Compositio Mathematica **137:** 275–292, 2003.

Slope Estimates of Artin–Schreier Curves

JASPER SCHOLTEN[1] and HUI JUNE ZHU[2]
[1]*ESAT/COSIC, KU Leuven, Kasteelpark Arenberg 10, 3001 Leuven-Heverlee, Belgium.*
e-mail: jasper.scholten@esat.kuleuven.ac.be
[2]*Department of Mathematics, University of California, Berkeley, CA 94720-3840. U.S.A.*
e-mail: zhu@alum.calberkeley.org

(Received: 21 August 2001; accepted in final form: 7 March 2002)

Abstract. Let $X/\overline{\mathbb{F}}_p$ be an Artin–Schreier curve defined by the affine equation $y^p - y = \tilde{f}(x)$ where $\tilde{f}(x) \in \overline{\mathbb{F}}_p[x]$ is monic of degree d. In this paper we develop a method for estimating the first slope of the Newton polygon of X. Denote this first slope by $\mathrm{NP}_1(X/\overline{\mathbb{F}}_p)$). We use our method to prove that if $p > d \geqslant 2$ then $\mathrm{NP}_1(X/\overline{\mathbb{F}}_p) \geqslant \lceil (p-1)/d \rceil/(p-1)$. If $p > 2d \geqslant 4$, we give a sufficient condition for the equality to hold.

Mathematics Subject Classifications (2000). 11Lxx, 14Hxx, 14Mxx.

Key words. Artin–Schreier curves, exponential sums, Hodge polygon, Newton polygon, zeta and L functions over finite fields.

1. Introduction

In this paper a curve is a smooth, projective and geometrically integral algebraic variety of dimension one. Let d be a positive integer. Let p be a prime coprime to d. Let $q = p^\nu$ for some positive integer ν. Let X be an *Artin–Schreier curve* over $\mathbb{F}_q$ defined by an affine equation $X\colon y^p - y = \tilde{f}(x)$, where $\tilde{f}(x) \in \mathbb{F}_q[x]$ is of degree d. Then X has genus $g := (p-1)(d-1)/2$ (see Section 3).

Write the L function of X over $\mathbb{F}_q$ as

$$\exp\left(\sum_{n=1}^{\infty}(q^n + 1 - \#X(\mathbb{F}_{q^n}))\frac{T^n}{n}\right) = \frac{1}{P(T)}. \tag{1}$$

The denominator $P(T)$ is a polynomial $1 + \sum_{\ell=1}^{2g} b_\ell T^\ell \in 1 + T\mathbb{Z}[T]$. Consider the sequence of points

$$(0,0), \quad \left(1, \frac{\mathrm{ord}_p b_1}{\nu}\right), \quad \left(2, \frac{\mathrm{ord}_p b_2}{\nu}\right), \ldots, \left(2g, \frac{\mathrm{ord}_p b_{2g}}{\nu}\right)$$

in $\mathbb{R}^2$. (If $b_\ell = 0$, define $\mathrm{ord}_p b_\ell = \infty$.) The *normalized p-adic Newton polygon* of $P(T)$ is defined to be the lower convex hull of this set of points. It is called the *Newton polygon* of $X/\mathbb{F}_q$, denoted by $\mathrm{NP}(X/\mathbb{F}_q)$. Let $\mathrm{NP}_1(X/\mathbb{F}_q)$ denote the first slope of $\mathrm{NP}(X/\mathbb{F}_q)$, which we call the *first slope* of $X/\mathbb{F}_q$.

In this paper we develop a technique for estimating $\mathrm{NP}_1(X/\mathbb{F}_q)$. We apply this technique in the case $p > d$. It can also be applied in other cases. See, for example, [13] for the case $p = 2$.

For any real number t let $\lceil t \rceil$ denote the least integer greater than or equal to t and let $\lfloor t \rfloor$ be the greatest integer less than or equal to t.

Let R be a commutative ring with unity. For any $f(x) \in R[x]$, any positive integers N and r, we use $[f(x)^N]_r$ to denote the x^r-coefficient of $f(x)^N$.

THEOREM 1.1. *Fix $d \geqslant 2$. Let $X/\mathbb{F}_q$ be an Artin–Schreier curve of genus $\geqslant 3$ whose affine equation is given by $y^p - y = \tilde{f}(x)$ where $\tilde{f}(x)$ is monic of degree d.*

(a) *If $p > d$ then* $\mathrm{NP}_1(X/\mathbb{F}_q) \geqslant \lceil (p-1)/d \rceil/(p-1)$.
(b) *If $p > 2d$ and* $[\tilde{f}(x)^{\lceil \frac{p-1}{d} \rceil}]_{p-1} \neq 0$ *then* $\mathrm{NP}_1(X/\mathbb{F}_q) = \lceil (p-1)/d \rceil/(p-1)$.

Remark 1.2. The Newton polygon of $X/\mathbb{F}_q$ has the same shape as that of the L function of exponential sums $\exp(\sum_{\ell=1}^{\infty} S_\ell(\tilde{f})\frac{T^\ell}{\ell})$ where

$$S_\ell(\tilde{f}) = \sum_{x \in \mathbb{F}_{q^\ell}} \exp\left(\frac{2\pi\sqrt{-1}}{p} \mathrm{Tr}_{\mathbb{F}_{q^\ell}/\mathbb{F}_p}(\tilde{f}(x))\right).$$

A proof of this known fact can be found in the Introduction of [19]. Using this, one observes that Theorem 1.1 is a generalization of Theorem 2 of [14], where q is assumed to be prime. See [13] and [14] for survey and further development.

If a curve is defined over a perfect field of characteristic p then its Newton polygon is defined by the 'formal types' of the p-divisible groups associated to the Jacobian of the curve (see [9] or [8]). Theorem 1.1 holds if $\mathbb{F}_q$ is replaced by any perfect field of characteristic p because its proof remains valid. It is known that the Newton polygons have integral bending points and are symmetric in the sense that any line segment of slope λ of length ℓ occurs in companion with a line segment of slope $1 - \lambda$ of the same length.

Artin–Schreier curves are precisely those degree p Abelian covers of the projective line with the point at infinity totally ramified, and no other ramification. So their p-ranks are zero by the Deuring–Shafarevich formula (see [3, Corollary 1.8] or [11]). The p-rank is exactly equal to the length of the slope zero segment of its Newton polygon (see [9]). Thus an Artin–Schreier curve has no zero slope. Suppose $g = 1$ or 2, then an Artin–Schreier curve X has its first slope equal to $1/2$.

When $f(x)$ is a monomial then the Frobenius and Verschiebung maps on the first crystalline cohomology of X have explicit interpretations (see [6] and [7]), which enable one to describe the entire Newton polygon of X explicitly. (Note that classical literature often refers to this special case as the definition of an Artin–Schreier curve.)

This paper is organized as follows: We recall relevant preliminaries in Section 2. Then we develop a method in Section 3 to estimate the first slopes of Artin–Schreier

curves. After some technical preparation in Sections 4 and 5, Section 6 proves a lower bound for the first slopes of Artin–Schreier curves, and gives a sufficient condition for the lower bound to be achieved. We prove Theorem 1.1 here.

2. Sharp Slope Estimates

This section provides fundamental ingredients for our slope estimates of curves over finite fields. Note that lemmas we need hold valid when the base field is perfect of characteristic p. However, for simplicity we constrain ourselves to finite fields in this paper. Firstly we establish a variation of Katz's sharp slope estimates in Theorem 2.2. Secondly we recall a method of computing the Verschiebung action on the first de Rham cohomology of a curve by taking power series expansions at a rational point. This section essentially follows [1, 2, 5, 6, 12]. Our approach is particularly inspired by Nygaard's paper [12].

Let W be the ring of Witt vectors over $\mathbb{F}_q$, and σ the absolute Frobenius automorphism of W. Throughout this section we assume that $X/\mathbb{F}_q$ is a curve of genus g with a rational point. Suppose there is a smooth and proper lifting X/W of X to W, together with a lifted rational point P. The Frobenius endomorphism F (resp., Verschiebung endomorphism V) are σ (resp., σ^{-1}) linear maps on the first crystalline cohomology $H^1_{\mathrm{crys}}(X/W)$ of X with $FV = VF = p$. It is known that $H^1_{\mathrm{crys}}(X/W)$ is canonically isomorphic to the first de Rham cohomology $H^1_{\mathrm{dR}}(X/W)$ of X, and one gets induced F and V actions on $H^1_{\mathrm{dR}}(X/W)$. Thus the pair $(H^1_{\mathrm{dR}}(X/W), F)$ can be considered as a σ-F-crystal, whereas the pair $(H^1_{\mathrm{dR}}(X/W), V)$ as a σ^{-1}-V-crystal. The Newton polygon of $X/\mathbb{F}_q$ is equal to the Newton polygon of the crystals $(H^1_{\mathrm{dR}}(X/W), F)$ and $(H^1_{\mathrm{dR}}(X/W), V)$ as defined in [5].

Below we will briefly describe some techniques to approximate slopes of these crystals. Let L be the image of $H^0(X, \Omega^1_{X/W})$ in $H^1_{\mathrm{dR}}(X/W)$, and let M be a complement of L such that $H^1_{\mathrm{dR}}(X/W) = L \oplus M$. The following lemma is for the proof of Theorem 2.2.

LEMMA 2.1. *Let notation be as above. Then* $L \subset V(L \oplus M) \subset L \oplus pM$. *If* p^{m-1} *divides* $V^a L$ *for some* $m > 0$ *and* $a \geqslant 0$, *then for all* $n > a$ *we have* $V^n L \subset p^{m-1}L + p^m M$.

Proof. Recall an equality due to Mazur and Ogus (see [10, Theorem 3]).

$$F^{-1}(p(L \oplus M)) \otimes \mathbb{F}_q = L \otimes \mathbb{F}_q.$$

One easily verifies the following inclusions

$$L \subset F^{-1}(p(L \oplus M)) + p(L \oplus M) \subset F^{-1}FV(L \oplus M) + VF(L \oplus M) \subset V(L \oplus M).$$

The rest follows from [12, Lemmas 1.4 and 1.5]. □

THEOREM 2.2. *Let* λ *be a rational number with* $0 \leqslant \lambda \leqslant \frac{1}{2}$. *Then* $\mathrm{NP}_1(X/\mathbb{F}_q) \geqslant \lambda$ *if and only if* $p^{\lceil n\lambda \rceil} \mid V^{n+g-1}L$ *for all integer* $n \geqslant 1$.

https://doi.org/10.1023/A:1024116216156 Published online by Cambridge University Press

Proof. The main ingredient of the proof is Katz's sharp slope estimate [5, Theorem (1.5)], which says that $\mathrm{NP}_1(X/\mathbb{F}_q) \geqslant \lambda$ if and only if $p^{\lceil n\lambda \rceil} \mid V^{n+g}$ for all $n \geqslant 1$.

Suppose $\mathrm{NP}_1(X/\mathbb{F}_q) \geqslant \lambda$. Then $p^{\lceil n\lambda \rceil} \mid V^{n+g}$ for all $n \geqslant 1$. By Lemma 2.1 we have

$$V^{n+g-1}(L) \subset V^{n+g-1}(\mathrm{Im}V) = V^{n+g}(L \oplus M) \subset p^{\lceil n\lambda \rceil}(L \oplus M).$$

Conversely, suppose that $p^{\lceil n\lambda \rceil} \mid V^{n+g-1}L$ for all $n \geqslant 1$. It suffices to show that $p^{\lceil n\lambda \rceil} \mid V^{n+g}$ for all $n \geqslant 0$. For $n = 0$ this statement is trivially true. We proceed by induction on n.

Assume that $p^{\lceil (n-1)\lambda \rceil} \mid V^{n+g-1}$. By Lemma 2.1 we have $V(L \oplus M) \subset L \oplus pM$. So

$$V^{n+g}(L \oplus M) = V^{n+g-1}V(L \oplus M) \subset V^{n+g-1}(L \oplus pM),$$

and $p^{\lceil n\lambda \rceil} \mid p^{\lceil (n-1)\lambda \rceil + 1} \mid V^{n+g-1}(pM)$. From the hypothesis $p^{\lceil n\lambda \rceil} \mid V^{n+g-1}L$, we have $p^{\lceil n\lambda \rceil} \mid V^{n+g}$. □

Remark 2.3. Let n and m be any positive integers. If p^{m-1} divides $V^a L$ for some nonnegative integer $a < n$, following Lemma 2.1, the composition of V^n/p^{m-1} and reduction to $\mathbb{F}_q$ gives a natural endomorphism of $L \otimes \mathbb{F}_q$. This endomorphism of $L \otimes \mathbb{F}_q$ is called a *higher Cartier operator*, denoted by $\mathcal{C}(m, n)$. The hypothesis in the theorem above is equivalent to that $\mathcal{C}(\lceil n\lambda \rceil, n + g - 1)$ is defined and vanishes for all integer $n \geqslant 1$. The underlying philosophy of our slope estimates is to replace the traditional Cartier operator by this higher Cartier operator. We will not explore this terminology further in this paper.

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

$$\begin{aligned} F\left(h(x)\frac{\mathrm{d}x}{x}\right) &= ph^{\sigma}(x^p)\frac{\mathrm{d}x}{x}, \\ V\left(h(x)\frac{\mathrm{d}x}{x}\right) &= h^{\sigma^{-1}}(x^{1/p})\frac{\mathrm{d}x}{x}, \quad \text{where } x^{m/p} = 0 \text{ if } p \not| m \end{aligned} \tag{2}$$

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

LEMMA 2.4. *The F and V actions on* $H^1_{\mathrm{dR}}(X/W)$ *and* $H^1_{\mathrm{dR}}(\hat{X}/W)$ *commute with the restriction map* res: $H^1_{\mathrm{dR}}(X/W) \longrightarrow H^1_{\mathrm{dR}}(\hat{X}/W)$. *Furthermore,* $\mathrm{res}^{-1}(pH^1_{\mathrm{dR}}(\hat{X}/W)) = F(H^1_{\mathrm{dR}}(X/W))$.

Proof. The first statement follows from [6, Lemma 5.8.2]. The second is precisely [12, Lemma 2.5]. □

This lemma will only be used in the proof of Theorem 3.4.

3. Slope Estimates of Artin–Schreier Curves

Assume that X is an Artin–Schreier curve over $\mathbb{F}_q$ defined by an affine equation $y^p - y = \tilde{f}(x)$ where $\tilde{f}(x) = x^d + \tilde{a}_{d-1}x^{d-1} + \cdots + \tilde{a}_1 x$ and $p \not| d$. It is easy to observe

https://doi.org/10.1023/A:1024116216156 Published online by Cambridge University Press

that every Artin–Schreier curve over $\overline{\mathbb{F}}_p$ can be written in this form (over some suitable $\mathbb{F}_q$). So $X/\mathbb{F}_q$ has a rational point at the origin. Assume that the genus g of X is $\geqslant 3$. Take a lifting X/W defined by $y^p - y = f(x)$ where $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x \in W[x]$ with $a_\ell \equiv \tilde{a}_\ell \bmod p$ for all ℓ. So X/W has a rational point at the origin with a local parameter x. The goal of this section is to prove Theorem 3.4. In particular, we shall prove a highly applicable version in Key-Lemma 3.5.

For any integer $N > 0$ and $0 \leqslant i \leqslant p-2$ let $C_r(i, N)$ be the x^r-coefficient of the power series expansion of the function $y^i(py^{p-1} - 1)^{p^N - 1}$ at the origin P:

$$y^i(py^{p-1} - 1)^{p^N-1} = \sum_{r=0}^{\infty} C_r(i, N)x^r. \tag{3}$$

We prepare three lemmas before we start to prove Theorem 3.4. We shall restrict the range of i and j as in Lemma 3.1.

LEMMA 3.1. *The curve X/W has genus $(d-1)(p-1)/2$, and for $p-2 \geqslant i \geqslant 0$, $j \geqslant 1$ and $di + pj \leqslant (p-1)(d-1) - 2 + p$ the differential forms*

$$\omega_{ij} := x^j y^i (py^{p-1} - 1)^{-1} \frac{\mathrm{d}x}{x}$$

form a basis for L.

Proof. For the special fibre $X/\mathbb{F}_q$ this follows immediately from Proposition VI.4.1 of [16]. Let $\mathbb{Q}W$ be the field of fractions of W. Consider the generic fibre $X/\mathbb{Q}W$. There are no points (x, y) in $X(\overline{\mathbb{Q}\mathbb{W}})$ with $py^{p-1} - 1 = f'(x) = 0$, since for such (x, y) one can easily show that $y^p - y$ is not integral over W, and $f(x)$ is integral over W. It follows that the affine part of $X/\mathbb{Q}W$ is nonsingular. The affine ramification points of the map $X \to \mathbb{P}^1$ defined by $(x, y) \mapsto x$ are those that satisfy $py^{p-1} - 1 = 0$. For each such y there are exactly d corresponding values of x, since $f'(x) \neq 0$ there. So there are $(p-1)d$ ramification points on the affine part. The function $y^p - y - f(x)$ in y and its first two derivatives have no common zeroes, so all affine ramification points are of index 2. Let e_∞ be the ramification index at ∞. Write g' for the genus of X/W. By Riemann–Hurwitz, we have $2g' - 2 = -2p + (p-1)d + e_\infty - 1$. It follows that $g' \leqslant (p-1)(d-1)/2$. But the genus of the special fibre $X/\mathbb{F}_q$ is $g = (p-1)(d-1)/2$, hence $g' = g = (p-1)(d-1)/2$, and $e_\infty = p$.

The differential form $\mathrm{d}x/(py^{p-1} - 1) = \mathrm{d}y/f'(x)$ has no affine poles. The form $\mathrm{d}x$ only has affine zeroes (of order 1) at points where the map $(x, y) \mapsto x$ ramifies. At these points, $py^{p-1} - 1 = 0$, so $\mathrm{d}x/(py^{p-1} - 1)$ has no affine zeroes. The degree of a canonical differential form is $2g - 2 = (p-1)(d-1) - 2$, hence $\mathrm{d}x/(py^{p-1} - 1)$ has a zero of order $(p-1)(d-1) - 2$ at ∞. The function x has degree p and no poles at the affine part. Hence it has a pole of order p at ∞. Similarly, y has a pole of order d at ∞. So for $p-2 \geqslant i \geqslant 0$, $j \geqslant 1$ and $di + pj \leqslant (p-1)(d-1) - 2 + p$ the form ω_{ij} is in L. From the assumption that d and p are coprime it follows that for i and j in this range the ω_{ij} have zeroes of different order at ∞, hence they are independent. From

https://doi.org/10.1023/A:1024116216156 Published online by Cambridge University Press

[16], Proposition VI.4.1 (h), it follows that the reduction of these differential forms modulo p form a basis for $H^0(\Omega^1_{X/\mathbb{F}_q})$, hence the ω_{ij} form a basis for L. □

LEMMA 3.2. *Let m be a positive integer. If $p \nmid m$ then $x^m(py^{p-1}-1)^{-1}\frac{dx}{x} \equiv 0 \bmod p$ in $H^1_{\mathrm{dR}}(\hat{X}/W)$.*

Proof. If $p \nmid m$ then $x^m(py^{p-1}-1)^{-1}dx/x \equiv -d(x^m/m) \bmod p$, which is cohomological to zero in $H^1_{\mathrm{dR}}(\hat{X}/W)$. □

LEMMA 3.3. *For all nonnegative integers a and r we have $C_r(i, N+a) \equiv C_r(i, N) \bmod p^{N+1}$.*

Proof. It is easy to see that $\binom{p^N}{\ell} \equiv 0 \bmod p^{N+1-\ell}$ if $N+1 \geqslant \ell \geqslant 1$. Thus

$$(1-py^{p-1})^{p^N} = \sum_{\ell=0}^{p^N}\binom{p^N}{\ell}(-py^{p-1})^{\ell} \equiv 1 \bmod p^{N+1}.$$

Therefore, we have

$$\begin{aligned} y^i(py^{p-1}-1)^{p^{N+a}-1} &= y^i(py^{p-1}-1)^{p^N-1}(1-py^{p-1})^{p^N(p^a-1)} \\ &\equiv y^i(py^{p-1}-1)^{p^N-1} \bmod p^{N+1}. \end{aligned}$$

This proves the lemma. □

THEOREM 3.4. *Let λ be a rational number with $0 \leqslant \lambda \leqslant \frac{1}{2}$. Suppose there exists an integer n_0 such that*

(i) *for all $m \geqslant 1$ and $1 \leqslant n < n_0$ we have $\mathrm{ord}_p(C_{mp^{n+g-1}-j}(i, n+g-2)) \geqslant \lceil n\lambda \rceil$;*
(ii) *for all $m \geqslant 2$ we have $\mathrm{ord}_p(C_{mp^{n_0+g-1}-j}(i, n_0+g-2)) \geqslant \lceil n_0\lambda \rceil$.*

Then

$$p^{\lceil n\lambda \rceil} \mid V^{n+g-1}(\omega_{ij}), \quad \text{if } n < n_0;$$
$$p^{\lceil n_0\lambda \rceil - 1} \mid V^{n_0+g-1}(\omega_{ij}), \quad \text{if } n = n_0.$$

Furthermore, we have

$$V^{n_0+g-1}(\omega_{ij}) \equiv C^{\sigma^{-(n_0+g-1)}}_{p^{n_0+g-1}-j}(i, n_0+g-2)(\omega_{0,1}) \bmod p^{\lceil n_0\lambda \rceil}.$$

Proof. We will prove the first part by induction. Suppose $1 \leqslant n \leqslant n_0$ and

$$p^{\lceil (n-1)\lambda \rceil} \mid V^{n+g-2}(\omega_{ij}). \tag{4}$$

Note that this is trivially true if $n = 1$.

Write $h(x) := (py^{p-1}-1)^{-1} \in W[[x]]$. By [12, Lemma 2.2], we have

$$h(x)^{p^{n+g-2}} = h^{\sigma^{n+g-2}}(x^{p^{n+g-2}}) + ph_1^{\sigma^{n+g-3}}(x^{p^{n+g-3}}) + \cdots + p^{n+g-2}h_{n+g-2}(x)$$

https://doi.org/10.1023/A:1024116216156 Published online by Cambridge University Press

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

$$\begin{aligned}
\operatorname{res}(\omega_{ij}) &= \operatorname{res}\left(x^j y^i (py^{p-1} - 1)^{-1} \frac{\mathrm{d}x}{x}\right) \\
&= \operatorname{res}\left(x^j y^i (py^{p-1} - 1)^{p^{n+g-2}-1} h(x)^{p^{n+g-2}} \frac{\mathrm{d}x}{x}\right) \\
&= \sum_{r=0}^{\infty} C_r(i, n+g-2) x^{r+j} h^{\sigma^{n+g-2}}(x^{p^{n+g-2}}) \frac{\mathrm{d}x}{x} + \\
&\quad + p \sum_{r=0}^{\infty} C_r(i, n+g-2) x^{r+j} h_1^{\sigma^{n+g-3}}(x^{p^{n+g-3}}) \frac{\mathrm{d}x}{x} + \\
&\quad + \cdots + p^{n+g-2} \sum_{r=0}^{\infty} C_r(i, n+g-2) x^{r+j} h_{n+g-2}(x) \frac{\mathrm{d}x}{x}.
\end{aligned}$$

Apply V^{g+n-2} to the first differential form above. Since the V-action commutes with the restriction map (by Lemma 2.4), we have

$$\begin{aligned}
&\operatorname{res}(V^{n+g-2}\omega_{ij}) \\
&= \sum_{m=1}^{\infty} C^{\sigma^{-(n+g-2)}}_{mp^{n+g-2}-j}(i, n+g-2) x^m h(x) \frac{\mathrm{d}x}{x} + \\
&\quad + p \sum_{m=1}^{\infty} C^{\sigma^{-(n+g-3)}}_{mp^{n+g-3}-j}(i, n+g-2) V\left(x^m h_1(x) \frac{\mathrm{d}x}{x}\right) + \\
&\quad + p^2 \sum_{m=1}^{\infty} C^{\sigma^{-(n+g-4)}}_{mp^{n+g-4}-j}(i, n+g-2) V^2\left(x^m h_2(x) \frac{\mathrm{d}x}{x}\right) + \\
&\quad + \cdots + p^{\lceil n\lambda \rceil - 1} \sum_{m=1}^{\infty} C^{\sigma^{-(n+g-1-\lceil n\lambda \rceil)}}_{i,mp^{n+g-1-\lceil n\lambda \rceil}-j}(n+g-2) V^{\lceil n\lambda \rceil - 1}\left(x^m h_{\lceil n\lambda \rceil - 1}(x) \frac{\mathrm{d}x}{x}\right) \\
&\quad + p^{\lceil n\lambda \rceil} \beta, \qquad (5)
\end{aligned}$$

for some $\beta \in H^1_{\mathrm{dR}}(\hat{X}/W)$.

By the hypothesis, $p^{\lceil n\lambda \rceil - 1}$ divides $C_{mp^{n+g-2}-j}(i, n+g-3)$. For all $m \geqslant 1$, by Lemma 3.3,

$$p^{\lceil n\lambda \rceil - 1} \mid C_{mp^{n+g-2}-j}(i, n+g-2). \qquad (6)$$

For m coprime to p it follows from Lemma 3.2 that p divides $x^m h(x)\,\mathrm{d}x/x$. Thus

$$p^{\lceil n\lambda \rceil} \mid C_{mp^{n+g-2}-j}(i, n+g-2) x^m h(x) \frac{\mathrm{d}x}{x}.$$

Otherwise, except possibly when $n = n_0$ and $m = p$, we have

$$p^{\lceil n\lambda \rceil} \mid C_{(\frac{m}{p})p^{n+g-1}-j}(i, n+g-2).$$

https://doi.org/10.1023/A:1024116216156 Published online by Cambridge University Press

Therefore,

$$\begin{aligned}
&\sum_{m=1}^{\infty} C^{\sigma^{-(n+g-2)}}_{mp^{n+g-2}-j}(i, n+g-2)x^m h(x)\frac{\mathrm{d}x}{x} \\
&\quad\equiv \sum_{m'=1}^{\infty} C^{\sigma^{-(n+g-2)}}_{m'p^{n+g-1}-j}(i, n+g-2)x^{pm'} h(x)\frac{\mathrm{d}x}{x} \\
&\quad\equiv \begin{cases} 0 \bmod p^{\lceil n\lambda\rceil}, & \text{if } n < n_0 \\ C^{\sigma^{-(n_0+g-2)}}_{p^{n_0+g-1}-j}(i, n_0+g-2)x^p h(x)\frac{\mathrm{d}x}{x} \bmod p^{\lceil n\lambda\rceil}, & \text{if } n = n_0. \end{cases} \qquad (7)
\end{aligned}$$

For all integer $\ell \geqslant 1$, by the hypothesis of the theorem, we obtain

$$\mathrm{ord}_p(C_{mp^{n+g-\ell-2}-j}(i, n+g-\ell-3)) \geqslant \lceil (n-\ell-1)\lambda\rceil \geqslant \lceil n\lambda\rceil - \ell.$$

So, by Lemma 3.3, we have $\mathrm{ord}_p(C_{mp^{n+g-\ell-2}-j}(i, n+g-2)) \geqslant \lceil n\lambda\rceil - \ell$. So $p^{\lceil n\lambda\rceil}$ divides every sum of (5) except possibly the one on the first line. Combining this information with (4), (6) and (7) yields for all $n < n_0$

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

Hence for such n Lemma 2.4 implies

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

so

$$\frac{V^{n+g-1}(\omega_{ij})}{p^{\lceil n\lambda\rceil-1}} \in VF(H^1_{\mathrm{dR}}(X/W)) = pH^1_{\mathrm{dR}}(X/W),$$

which proves the induction hypothesis. If $n = n_0$ then the above implies

$$\mathrm{res}\left(\frac{V^{n_0+g-2}(\omega_{ij})}{p^{\lceil n_0\lambda\rceil-1}}\right) - \frac{1}{p^{\lceil n_0\lambda\rceil-1}} C^{\sigma^{-(n_0+g-2)}}_{p^{n_0+g-1}-j}(i, n_0+g-2)x^p h(x)\frac{\mathrm{d}x}{x}$$

lies in $pH^1_{\mathrm{dR}}(\hat{X}/W)$. Lemma 2.4 implies

$$\frac{V^{n_0+g-2}(\omega_{ij})}{p^{\lceil n_0\lambda\rceil-1}} - \frac{1}{p^{\lceil n_0\lambda\rceil-1}} C^{\sigma^{-(n_0+g-2)}}_{p^{n_0+g-1}-j}(i, n_0+g-2)\omega_{0,p}$$

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

$$\frac{V^{n_0+g-1}(\omega_{ij})}{p^{\lceil n_0\lambda\rceil-1}} - \frac{1}{p^{\lceil n_0\lambda\rceil-1}} C^{\sigma^{-(n_0+g-1)}}_{p^{n_0+g-1}-j}(i, n_0+g-2)V(\omega_{0,p})$$

https://doi.org/10.1023/A:1024116216156 Published online by Cambridge University Press

lies in $VFH^1_{\mathrm{dR}}(X/W) = pH^1_{\mathrm{dR}}(X/W)$. Now the theorem follows from $V(\omega_{0,p}) \equiv \omega_{0,1} \bmod p$. □

We summarize everything we need in the key lemma below.

KEY-LEMMA 3.5. *Let* λ *be a rational number with* $0 \leqslant \lambda \leqslant \frac{1}{2}$.

(i) *If for all* i, j *within the range of Lemma* 3.1, *and for all* $m \geqslant 1$, $n \geqslant 1$ *we have*

$$\mathrm{ord}_p(C_{mp^{n+g-1}-j}(i, n+g-2)) \geqslant \lceil n\lambda \rceil \text{ then } \mathrm{NP}_1(X/\mathbb{F}_q) \geqslant \lambda.$$

(ii) *Let* i, j *be within the range.*

(a) *Let* $n_0 \geqslant 1$. *Suppose that for all* $m \geqslant 1$ *and* $1 \leqslant n$ *we have*

$$\mathrm{ord}_p(C_{mp^{n+g-1}-j}(i, n+g-2)) \geqslant \lceil n\lambda \rceil;$$

(b) *suppose that for all* $m \geqslant 2$ *we have* $\mathrm{ord}_p(C_{mp^{n_0+g-1}-j}(i, n_0+g-2)) \geqslant \lceil n_0\lambda \rceil$;

(c) *suppose* $\mathrm{ord}_p(C_{p^{n_0+g-1}-j}(i, n_0+g-2)) < \lceil n_0\lambda \rceil$; *Then* $\mathrm{NP}_1(X/\mathbb{F}_q) < \lambda$.

Proof. (i) The hypotheses in Theorem 3.4 are satisfied for all positive integers n_0 and for all possible i and j. Thus our statement follows from Theorem 2.2.

(ii) If $\mathrm{NP}_1(X/\mathbb{F}_q) \geqslant \lambda$ then $p^{\lceil n_0\lambda \rceil} | V^{n_0+g-1}(\omega_{ij})$ for all i, j in the range of Lemma 3.1 by Theorem 2.2. This implies that for the particular i, j satisfying the hypothesis of Theorem 3.4 we have $\mathrm{ord}_p(C_{p^{n_0+g-1}-j}(i, n_0+g-2)) \geqslant \lceil n_0\lambda \rceil$. This proves the Key-Lemma. □

4. *p*-Adic Behavior of Coefficients of Power Series

In this section we study the p-adic behavior of coefficients of two power series.

To make this paper as self-contained as possible, we recall the *Lagrange inversion formula* from mathematical analysis [4, IX, § 189]. Let z and y be two functions such that $y = z\mu(y)$ for some function $\mu(y)$ which can be developed into a power series in y. Then the power series expansion of any function $h(y)$ in z is

$$h(y) = \sum_{k_1=1}^{\infty} \frac{1}{k_1!} \left(\left(\mu(y)^{k_1} h'(y)\right)^{(k_1-1)} \Big|_{y=0} \right) z^{k_1}, \tag{8}$$

where the upper corner $^{(k_1-1)}$ denotes the (k_1-1)th derivative and $h'(y)$ denotes the first derivative of $h(y)$ in terms of y.

LEMMA 4.1. *Let* $a > 0$ *and let* $y \in W[[z]]$ *be a power series that satisfies* $y^p - y = z$ *and* $y(0) = 0$. *Then* $y^a = \sum_{k_1=1}^{\infty} D_{k_1}(a) z^{k_1}$ *where* $D_{k_1}(a) = 0$ *if* $k_1 \not\equiv a \bmod p-1$; *otherwise,*

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

https://doi.org/10.1023/A:1024116216156 Published online by Cambridge University Press

Proof. Note that $y = z(y^{p-1} - 1)^{-1}$. Apply (8) to this equation, we get

$$y^a = \sum_{k_1=1}^{\infty} \frac{a}{k_1!} \left(\left((y^{p-1} - 1)^{-k_1} y^{a-1} \right)^{(k_1-1)} \Big|_{y=0} \right) z^{k_1}. \tag{9}$$

We have

$$\left((y^{p-1} - 1)^{-k_1} y^{a-1} \right)^{(k_1-1)} \Big|_{y=0} = \left(\sum_{\ell=0}^{\infty} (-1)^{(p-1)\ell+k_1} \binom{-k_1}{\ell} y^{(p-1)\ell+a-1} \right)^{(k_1-1)} \Bigg|_{y=0}.$$

Clearly, this is 0 if $k_1 \not\equiv a \bmod p-1$; otherwise, it is equal to

$$(-1)^a (k_1 - 1)! \binom{-k_1}{\frac{k_1-a}{p-1}}.$$

Plugging this into (9) yields the desired value for $D_{k_1}(a)$. □

For any positive integers k_1 and a, we will keep the notation $D_{k_1}(a)$ as defined in Lemma 4.1. We also define $D_{k_1}(a) = 1$ if $a = k_1 = 0$ and $D_{k_1}(a) = 0$ if only one of k_1 and a is 0. For any integer $k \geqslant 0$ denote by $s_p(k)$ the sum of all digits in the 'base p' expansion of k.

LEMMA 4.2. *If $a > 0$ and $k_1 \equiv a \bmod p-1$, write $a = i + \ell(p-1)$ with integers ℓ and $1 \leqslant i \leqslant p-1$, then*

$$\operatorname{ord}_p(D_{k_1}(a)) = \frac{s_p(k_1) - i}{p-1}, \quad \text{if } \ell = 0;$$
$$\operatorname{ord}_p(D_{k_1}(a)) \geqslant \frac{s_p(k_1) - i}{p-1} - (\ell - 1), \quad \text{if } \ell \geqslant 1.$$

Proof. Let $k_1 \equiv a \bmod p-1$. Using the well-known identity $(p-1)\operatorname{ord}_p(k!) = k - s_p(k)$ for all positive integer k, one gets that

$$\operatorname{ord}_p(D_{k_1}(a)) = \operatorname{ord}_p(a) + \frac{1}{p-1} \left(s_p(k_1) + s_p\left(\frac{k_1-a}{p-1}\right) - 1 - s_p\left(a - 1 + \frac{k_1-a}{p-1} p\right) \right). \tag{10}$$

If $\ell = 0$, then

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

If $\ell = 1$, then

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

https://doi.org/10.1023/A:1024116216156 Published online by Cambridge University Press

If $\ell > 1$, then

$$\begin{aligned} & s_p\left(a-1+\frac{k_1-a}{p-1}p\right) \\ & \quad \leqslant i-1+s_p(\ell(p-1))+s_p\left(\frac{k_1-a}{p-1}\right) \\ & \quad \leqslant i-1+(\ell-1)(p-1)+s_p\left(\frac{k_1-a}{p-1}\right). \end{aligned}$$

Substitute these back in (10), we obtain the desired (in)equalities. □

Fix two integers $N > 0$ and $0 \leqslant i \leqslant p-2$. Let $y \in W[[z]]$ still be the power series satisfying $y^p - y = z$. Define coefficients $E_{k_1}(i, N)$ by

$$y^i(py^{p-1}-1)^{p^N-1} = \sum_{k_1=0}^{\infty} E_{k_1}(i,N)z^{k_1}.$$

For any integer $r \geqslant 0$ let $\mathbf{K}_r$ denote the set of transposes $\mathbf{k} = {}^t(k_1, \ldots, k_d)$ of d-tuple integers with $k_1 \geqslant k_2 \geqslant \cdots \geqslant k_d \geqslant 0$ and $\sum_{\ell=1}^{d} k_\ell = r$. (*Remark*: Transposes are used only to give an easy setup for the p-adic box analysis in [13] and [15].) We define

$$s_p(\mathbf{k}) := s_p(k_1 - k_2) + \cdots + s_p(k_{d-1} - k_d) + s_p(k_d).$$

Note that from the definition of the coefficients $C_r(i, N)$ in (3) we find

$$\sum_{r=0}^{\infty} C_r(i,N)x^r = \sum_{k_1=0}^{\infty} E_{k_1}(i,N)f(x)^{k_1}.$$

Expanding the powers of $f(x)$ yields

$$C_r(i,N) = \sum_{\mathbf{k}\in\mathbf{K}_r} E_{k_1}(i,N)\prod_{\ell=1}^{d-1}\binom{k_\ell}{k_{\ell+1}}a_\ell^{k_\ell-k_{\ell+1}}. \tag{11}$$

LEMMA 4.3. *Let* $\mathbf{k} = {}^t(k_1, \ldots, k_d) \in \mathbf{K}_r$. *If* $k_1 \not\equiv i \bmod p-1$ *then* $E_{k_1}(i, N) = 0$. *If* $k_1 \equiv i \bmod p-1$ *then*

$$\begin{aligned} & \operatorname{ord}_p(E_{k_1}(i,N)) = \frac{s_p(k_1)-i}{p-1}, \\ & \operatorname{ord}_p\left(E_{k_1}(i,N)\prod_{\ell=1}^{d-1}\binom{k_\ell}{k_{\ell+1}}\right) = \frac{s_p(\mathbf{k})-i}{p-1}. \end{aligned}$$

Proof. Take the identity

$$y^i(py^{p-1}-1)^{p^N-1} = \sum_{\ell=0}^{p^N-1}(-1)^{p^N-1-\ell}\binom{p^N-1}{\ell}p^\ell y^{i+\ell(p-1)}. \tag{12}$$

https://doi.org/10.1023/A:1024116216156 Published online by Cambridge University Press

Substitute the power series expansion of $y^{i+\ell(p-1)}$ in (12); we get

$$E_{k_1}(i,N)=\sum_{\ell=0}^{p^N-1}(-1)^{p^N-1-\ell}\binom{p^N-1}{\ell}D_{k_1}(i+\ell(p-1))p^{\ell}. \tag{13}$$

If $k_1 \not\equiv i \bmod p-1$ then $D_{k_1}(i+\ell(p-1))=0$ by Lemma 4.1; hence $E_{k_1}(i,N)=0$. This prove the first part of the lemma.

If $k_1=i=0$ then $E_{k_1}(i,N)=(-1)^{p-1}$ and $s_p(k_1)-i=0$. If $i=0$, $k_1>0$ and $i\equiv k_1 \bmod p-1$ then, by Lemma 4.2, the term with minimal valuation in (13) occurs at $\ell=1$. We have

$$\operatorname{ord}_p(E_{k_1}(i,N))=1+\operatorname{ord}_p(D_{k_1}(p-1))=1+\frac{s_p(k_1)-(p-1)}{p-1}.$$

If $i>0$ and $k_1\equiv i \bmod p-1$ then the term with minimal valuation in (13) occurs at $\ell=0$. We have

$$\operatorname{ord}_p(E_{k_1}(i,N))=\operatorname{ord}_p(D_{k_1}(i))=\frac{s_p(k_1)-i}{p-1}.$$

This implies the second assertion.

By $\operatorname{ord}_p(k!)=\big(k-s_p(k)\big)/(p-1)$ we have that

$$\operatorname{ord}_p\binom{k_\ell}{k_{\ell+1}}=\frac{s_p(k_{\ell+1})+s_p(k_\ell-k_{\ell+1})-s_p(k_\ell)}{p-1}.$$

Thus

$$\operatorname{ord}_p\left(\prod_{\ell=1}^{d-1}\binom{k_\ell}{k_{\ell+1}}\right)=\frac{s_p(\mathbf{k})-s_p(k_1)}{p-1}.$$

So the third assertion follows from this equality and the second assertion. □

5. *p*-Adic Behavior of $C_r(i,N)$

To apply Theorem 3.4 one needs to have at hand an efficient formula for the p-adic valuations of the coefficients in (3). This formula is in Lemma 5.3, which is prepared for Section 6.

Let $\mathbf{k}={}^t(k_1,\dots,k_d)\in\mathbf{K}_r$. For $1\leqslant\ell\leqslant d$, let $k_\ell=\sum_{v\geqslant 0}k_{\ell,v}p^v$ be the 'base p' expansion of k_ℓ, we introduce a *dot representation*

$$\dot{k}_\ell:=[\dots,\dot{k}_{\ell,2},\dot{k}_{\ell,1},\dot{k}_{\ell,0}]$$

in the following way: for $\ell=d$, let $\dot{k}_{d,v}=k_{d,v}$ for all $v\geqslant 0$; for $1\leqslant\ell<d$, it is defined inductively by

$$\dot{k}_{\ell-1,v}:=\dot{k}_{\ell,v}+p^v\text{-coefficient in the 'base } p\text{' expansion of } (k_{\ell-1}-k_\ell),$$

https://doi.org/10.1023/A:1024116216156 Published online by Cambridge University Press

for all $v \geqslant 0$. It can be verified that $k_\ell = \sum_{v \geqslant 0} \dot{k}_{\ell,v} p^v$ for $1 \leqslant \ell \leqslant d$. Since $k_\ell \geqslant k_{\ell+1}$ we have $\dot{k}_{\ell-1,v} \geqslant \dot{k}_{\ell,v}$ for all v. It is not hard to observe

$$s_p(\mathbf{k}) = \sum_{v \geqslant 0} \left(\sum_{\ell=1}^{d-1} (\dot{k}_{\ell,v} - \dot{k}_{\ell+1,v}) + \dot{k}_{d,v} \right) = \sum_{v \geqslant 0} \dot{k}_{1,v}.$$

For any positive integer a, define a subset of $\mathbf{K}_r$ as follows

$$\mathbf{K}_r^a := \{\mathbf{k} \in \mathbf{K}_r \mid \dot{k}_{\ell,v} = 0 \text{ for } v \geqslant a,\ 1 \leqslant \ell \leqslant d\}.$$

More explicitly $\mathbf{K}_r^a$ consists of all $\mathbf{k} \in \mathbf{K}_r$ with $\dot{k}_\ell = [\ldots, 0, \dot{k}_{\ell,a-1}, \ldots, \dot{k}_{\ell,1}, \dot{k}_{\ell,0}]$ for all $1 \leqslant \ell \leqslant d$. Then we have an obvious filtration $\mathbf{K}_r^1 \subset \cdots \subset \mathbf{K}_r^{a-1} \subset \mathbf{K}_r^a \subset \cdots \subset \mathbf{K}_r$.

LEMMA 5.1. *Let $p > d$. Let $1 \leqslant j \leqslant p-1$, let $a, m, n \geqslant 1$ and $r = mp^a - j$. If $\mathbf{k} \in \mathbf{K}_r^a$, then*

$$s_p(\mathbf{k}) \geqslant \left\lfloor \frac{(m-1)p}{d} \right\rfloor + (a-1)\left\lceil \frac{p-1}{d} \right\rceil + \left\lceil \frac{p-j}{d} \right\rceil.$$

If $p > 2d$, $m = 1$ and the equality holds, then

$$\dot{k}_1 = \left[\ldots, 0, \overbrace{\left\lceil \frac{p-1}{d} \right\rceil, \ldots, \left\lceil \frac{p-1}{d} \right\rceil}^{a}, \left\lceil \frac{p-j}{d} \right\rceil \right].$$

Proof. We will prove this lemma by induction on a. Let $\mathbf{k} \in \mathbf{K}_r^a$. Suppose $a = 1$. Note that all real numbers c_1 and c_2 satisfy $\lceil c_1 + c_2 \rceil \geqslant \lfloor c_1 \rfloor + \lceil c_2 \rceil$. So we have

$$s_p(\mathbf{k}) = \dot{k}_{1,0} \geqslant \left\lceil \frac{r}{d} \right\rceil \geqslant \left\lfloor \frac{(m-1)p}{d} \right\rfloor + \left\lceil \frac{p-j}{d} \right\rceil.$$

Suppose $m = 1$ and the equality holds. It reads $\dot{k}_{1,0} = \lceil (p-j)/d \rceil$.

Now suppose $a \geqslant 2$. Let $\mathbf{k} \in \mathbf{K}_r^a$. Let $k'_\ell := \sum_{v=0}^{a-2} \dot{k}_{\ell,v} p^v$ for all $1 \leqslant \ell \leqslant d$. One can find a positive integer m' such that $m'p^{a-1} - j = \sum_{\ell=1}^d k'_\ell$. Then $\mathbf{k}' := {}^t(k'_1, \ldots, k'_d) \in \mathbf{K}_{m'p^{a-1}-j}^{a-1}$. We have $(m-1)p + p - 1 = (m'-1) + \sum_{\ell=1}^d \dot{k}_{\ell,a-1} \leqslant (m'-1) + d\dot{k}_{1,a-1}$. So

$$\begin{aligned} \dot{k}_{1,a-1} &\geqslant \left\lceil \frac{(m-1)p - (m'-1) + p - 1}{d} \right\rceil \\ &\geqslant \left\lfloor \frac{(m-1)p}{d} \right\rfloor - \left\lceil \frac{m'-1}{d} \right\rceil + \left\lceil \frac{p-1}{d} \right\rceil. \end{aligned} \tag{14}$$

On the other hand, by induction hypothesis on $\mathbf{k}' \in \mathbf{K}_{m'p^{a-1}-j}^{a-1}$, one has

$$\sum_{v=0}^{a-2} \dot{k}_{1,v} \geqslant \left\lfloor \frac{(m'-1)p}{d} \right\rfloor + (a-2)\left\lceil \frac{p-1}{d} \right\rceil + \left\lceil \frac{p-j}{d} \right\rceil. \tag{15}$$

Combining (14) and (15), one gets

https://doi.org/10.1023/A:1024116216156 Published online by Cambridge University Press

$$s_p(\mathbf{k}) = \sum_{v=0}^{a-1} \dot{k}_{1,v} \geqslant \left\lfloor \frac{(m-1)p}{d} \right\rfloor + (a-1)\left\lceil \frac{p-1}{d} \right\rceil + \left\lceil \frac{p-j}{d} \right\rceil + A, \tag{16}$$

where

$$A := \left\lfloor \frac{(m'-1)p}{d} \right\rfloor - \left\lceil \frac{m'-1}{d} \right\rceil.$$

Using $p > d$ one easily observes that $A \geqslant 0$, and the first part of the lemma follows from (16).

Now suppose $p > 2d$, $m = 1$, the equality holds in (16) and $A = 0$. This can only happen if $m' = 1$. It follows by induction that $\dot{k}_{1,0} = \lceil (p-j)/d \rceil$ and $\dot{k}_{1,v} = \lceil (p-1)/d \rceil$ for $1 \leqslant v < a-1$. From the equality in (16) it follows that $\dot{k}_{1,a-1} = \lceil (p-1)/d \rceil$. □

LEMMA 5.2. *Let a be a positive integer and $p > d$. For a polynomial $f(x) \in W[x]$ of degree d we have*

$$\left[f(x)^{\sum_{v=0}^{a-1} \left\lceil \frac{p-1}{d} \right\rceil p^v} \right]_{p^a-1} \equiv \prod_{v=0}^{a-1} \left[(f(x))^{\left\lceil \frac{p-1}{d} \right\rceil} \right]_{p-1}^{\sigma^v} \bmod p.$$

Proof. Write

$$f(x)^{\sum_{v=0}^{a-1} \left\lceil \frac{p-1}{d} \right\rceil p^v} = \prod_{v=0}^{a-1} f(x)^{\left\lceil \frac{p-1}{d} \right\rceil p^v} \equiv \prod_{v=0}^{a-1} f^{\sigma^v}(x^{p^v})^{\left\lceil \frac{p-1}{d} \right\rceil} \bmod p. \tag{17}$$

Now we write

$$x^{p^a-1} = \prod_{v=0}^{a-1} x^{p^v(p-1)}. \tag{18}$$

Consider contributions of each factor of the product of (17) in the coefficient of (18). Each vth factor of (17) contributes to the coefficients of $x^{p^v m}$ for some m, where $1 \leqslant m \leqslant d\lceil p-1/d \rceil < 2p-1$. When $v = 0$ then it has to contribute to the coefficient of x^{p-1}. Inductively for each $v = 1, \ldots, a-1$ the vth factor contributes precisely to the coefficient of $x^{p^v(p-1)}$. It is easy to see that

$$[f^{\sigma^v}(x^{p^v})^{\lceil \frac{p-1}{d} \rceil}]_{p^v(p-1)} \equiv [f(x)^{\lceil \frac{p-1}{d} \rceil}]_{p-1}^{\sigma^v} \bmod p.$$

Thus our assertion follows. □

LEMMA 5.3. *Let $p > d$. Let a, m, N be positive integers. Let i, j be as in Lemma* 3.1. *Then*

$$\operatorname{ord}_p(C_{mp^a-j}(i, N)) \geqslant \left\lceil \frac{(a-1)\lceil \frac{p-1}{d} \rceil + \lceil \frac{p-j}{d} \rceil - i}{p-1} \right\rceil. \tag{19}$$

Moreover, for $p > 2d$ we have

https://doi.org/10.1023/A:1024116216156 Published online by Cambridge University Press

$$\operatorname{ord}_p(C_{mp^a-1}(i,N)) = \frac{a\left\lceil\frac{p-1}{d}\right\rceil - i}{p-1} \tag{20}$$

if and only if

$$m = 1;$$

$$a\left\lceil\frac{p-1}{d}\right\rceil \equiv i \bmod p-1;$$

$$\left[f(x)^{\left\lceil\frac{p-1}{d}\right\rceil}\right]_{p-1} \not\equiv 0 \bmod p.$$

Proof. Let $\mathbf{k} = {}^t(k_1,\dots,k_d) \in \mathbf{K}_{mp^a-j}$. Let $\mathbf{k}' := {}^t(k_1',\dots,k_d')$ where $k_\ell' = \sum_{v=0}^{a-1} \dot{k}_{\ell,v}p^v$, then $\mathbf{k}' \in \mathbf{K}_{r'}^a$. Let $r' := \sum_{\ell=1}^d k_\ell'$, write $r' = m'p^a - j$ for some m'. From Lemma 5.1, it follows that

$$s_p(\mathbf{k}) = \sum_{v\geqslant 0}\dot{k}_{1,v} \geqslant \sum_{v=0}^{a-1}\dot{k}_{1,v} = s_p(\mathbf{k}') \geqslant (a-1)\left\lceil\frac{p-1}{d}\right\rceil + \left\lceil\frac{p-j}{d}\right\rceil. \tag{21}$$

Then by (11) and Lemma 4.3 one easily verifies that (19) holds.

Assume (20) holds. Then there is a $\mathbf{k}$ such that the equality in (21) holds for $j=1$, which implies that $m=1$, $\dot{k}_{1,v}=0$ for $v\geqslant a$, $\dot{k}_{1,v} = \lceil (p-1)/d\rceil$ for $0\leqslant v\leqslant a-1$ by Lemma 5.1. Thus $k_1 = \sum_{v=0}^{a-1}\lceil (p-1)/d\rceil p^v$. So $s_p(k_1) = a\lceil (p-1)/d\rceil \equiv i \bmod p-1$. Those $\mathbf{k}\in\mathbf{K}_{mp^a-1}$ which contribute terms in the sum (11) with minimal valuation necessarily have $k_1 \equiv i \bmod p-1$. By the identity

$$C_{p^a-1}(i,N) = \sum_{k_1=0}^{\infty} E_{k_1}(i,N)\cdot [f(x)^{k_1}]_{p^a-1},$$

we have by Lemma 4.3

$$\begin{aligned}\operatorname{ord}_p(C_{p^a-1}(i,N)) &\geqslant \operatorname{ord}_p(E_{k_1}(i,N)) + \operatorname{ord}_p([f(x)^{k_1}]_{p^a-1})\\ &= \frac{s_p(k_1)-i}{p-1} + \operatorname{ord}_p([f(x)^{k_1}]_{p^a-1})\end{aligned}$$

This is equal to $(a\lceil\frac{p-1}{d}\rceil - i)/(p-1)$ if and only if $[f(x)^{k_1}]_{p^a-1}\not\equiv 0 \bmod p$. By Lemma 5.2 this is equivalent to $[f(x)^{\lceil\frac{p-1}{d}\rceil}]_{p-1}\not\equiv 0 \bmod p$.

Conversely, the conditions imply that the contribution of $\mathbf{k}\in\mathbf{K}_{p^a-1}$ with $k_1 = \sum_{v=0}^{a-1}\lceil (p-1)/d\rceil p^v$ to $\operatorname{ord}_p(C_{p^a-1}(i,N))$ in (11) has valuation $[(a\lceil\frac{(p-1)}{d}\rceil - i)/(p-1)]$. Any contribution from other $\mathbf{k}\in\mathbf{K}_{p^a-1}$ has higher valuation by the above arguments. Thus $\operatorname{ord}_p(C_{p^a-1}(i,N)) = (a\lceil\frac{p-1}{d}\rceil - i)/(p-1)$. This finishes the proof of this lemma. □

6. Proof of Theorem 1.1

Proof of Theorem 1.1. It suffices to prove the theorem for the case that $\tilde{f}(x)$ has constant coefficient $\tilde{a}_0 = 0$. In the binomal expansion of $\tilde{f}(x)^{\left\lceil\frac{p-1}{d}\right\rceil}$, any monomial of the form $c\tilde{a}_{i_1}\cdots\tilde{a}_{i_k}x^{p-1}$ (with some coefficient c) has

https://doi.org/10.1023/A:1024116216156 Published online by Cambridge University Press

$$0 \leqslant k \leqslant \left\lceil \frac{p-1}{d} \right\rceil, \quad 0 \leqslant i_1, \ldots, i_k \leqslant d.$$

Suppose $i_1 = 0$ say, then

$$i_1 + \cdots + i_k \leqslant (k-1)d \leqslant \left(\left\lceil \frac{p-1}{d} \right\rceil - 1 \right) d < p-1,$$

leading to a contradiction. Thus $[\tilde{f}(x)^{\lceil \frac{p-1}{d} \rceil}]_{p-1}$ is independent of $\tilde{a}_0$. On the other hand, the curves $y^p - y = \tilde{f}(x)$ and $y^p - y = \tilde{f}(x) + \tilde{a}_0$ are isomorphic over $\overline{\mathbb{F}}_p$ for any $\tilde{a}_0$, and hence have the same Newton polygon. With the assumption $\tilde{a}_0 = 0$ we can use the results of Section 3.

(a) Set $\lambda_0 := (\lceil \frac{p-1}{d} \rceil)/(p-1)$. By the hypothesis on d, p and g it is elementary to check that for i and j in the range of Lemma 3.1 we have $(g-2)\lceil (p-1)/d \rceil + \lceil (p-j)/d \rceil \geqslant i$, thus

$$\left\lceil (n+g-2)\lambda_0 + \left(\left\lceil \frac{p-j}{d} \right\rceil - i \right) \Big/ (p-1) \right\rceil \geqslant \lceil n\lambda_0 \rceil$$

for all $n \geqslant 1$. By Lemma 5.3, we have

$$\operatorname{ord}_p(C_{mp^{n+g-1}-j}(i, n+g-2)) \geqslant \left\lceil (n+g-2)\lambda_0 + \frac{\lceil \frac{p-j}{d} \rceil - i}{p-1} \right\rceil \geqslant \lceil n\lambda_0 \rceil.$$

Thus $\mathrm{NP}_1(X/\mathbb{F}_q) \geqslant \lambda_0$ by Lemma 3.5i.

(b) Choose a value of i in the range of Lemma 3.1 for $j = 1$ such that the following congruence has a solution for a,

$$a \left\lceil \frac{p-1}{d} \right\rceil \equiv i \bmod p-1.$$

For any integer $n > 1$ define

$$\lambda_n := \frac{(n+g-2)\lceil \frac{p-1}{d} \rceil - i}{(n-1)(p-1)}.$$

Note that λ_n is monotonically decreasing as a function in n, and it converges to λ_0 as n approaches ∞. Suppose $\mathrm{NP}_1(X/\mathbb{F}_q) > \lambda_0$, then there exists a positive integer n_0 large enough such that $\mathrm{NP}_1(X/\mathbb{F}_q) > \lambda_{n_0}$. Choose such an n_0, and such that $a = n_0 + g - 1$ is a solution to the congruence above and such that

$$\frac{(g-1)\lceil \frac{p-1}{d} \rceil - i}{(p-1)(n_0-1)} \leqslant 1.$$

For all $1 \leqslant n < n_0$ we have

$$\lambda_{n_0} \leqslant \lambda_{n+1} = \frac{(n+g-1)\lceil \frac{p-1}{d} \rceil - i}{n(p-1)}.$$

https://doi.org/10.1023/A:1024116216156 Published online by Cambridge University Press

Thus, for all $m \geqslant 1$ and $1 \leqslant n < n_0$ we have by Lemma 5.3 that

$$\begin{aligned}
&\mathrm{ord}_p(C_{mp^{n+g-1}-1}(i, n+g-2)) \\
&\quad \geqslant \left\lceil \frac{(n+g-1)\lceil \frac{p-1}{d} \rceil - i}{p-1} \right\rceil \\
&\quad \geqslant \lceil n\lambda_{n_0} \rceil.
\end{aligned}$$

On the other hand, since

$$0 < n_0\lambda_{n_0} - \frac{(n_0+g-1)\lceil \frac{p-1}{d} \rceil - i}{p-1} = \frac{(g-1)\lceil \frac{p-1}{d} \rceil - i}{(p-1)(n_0-1)} \leqslant 1,$$

by our assumption we have

$$\lceil n_0\lambda_{n_0} \rceil = \frac{(n_0+g-1)\lceil \frac{p-1}{d} \rceil - i}{p-1} + 1.$$

Hence, for all $m \geqslant 2$ one has by Lemma 5.3 that

$$\begin{aligned}
&\mathrm{ord}_p(C_{mp^{n_0+g-1}-1}(i, n_0+g-2)) \\
&\quad \geqslant \frac{(n_0+g-1)\lceil \frac{p-1}{d} \rceil - i}{p-1} + 1 \\
&\quad = \lceil n_0\lambda_{n_0} \rceil.
\end{aligned}$$

So the hypotheses of Lemma 3.5 iia and iib are satisfied. Again by Lemma 5.3,

$$\mathrm{ord}_p(C_{p^{n_0+g-1}-1}(i, n_0+g-2)) \quad \geqslant \quad \lceil n_0\lambda_{n_0} \rceil - 1,$$

where the equality holds if and only if $[f(x)^{\lceil \frac{p-1}{d} \rceil}]_{p-1} \not\equiv 0 \bmod p$. In this case Lemma 3.5 iic is satisfied, from which we conclude that $\mathrm{NP}_1(X/\mathbb{F}_q) < \lambda_{n_0}$. This contradicts our assumption that $\mathrm{NP}_1(X/\mathbb{F}_q) > \lambda_{n_0}$. Therefore, we have $\mathrm{NP}_1(X/\mathbb{F}_q) = \lambda_0$. □

Acknowledgements

We thank Daqing Wan for explaining his conjectures. We doubly thank him for numerous stimulating conversations and historical remarks. We also thank Bjorn Poonen for comments on an early version of this paper. Finally, we thank the referee for detailed comments. The research of Hui June Zhu was partially supported by a grant of Bjorn Poonen from the David and Lucile Packard Foundation.

References

1. Berthelot, P.: Slopes of Frobenius in crystalline cohomology, In: *Algebraic Geometry* (*Arcata 1974*), Proc. Sympos. Pure Math. 29, Amer. Math. Soc., Providence, 1974, pp. 315–328.
2. Berthelot, P. and Ogus, A.: *Notes on Crystalline Cohomology*, Math. Notes, Princeton Univ. Press, Princeton, New Jersey, 1978.

3. Crew, R.: Etale p-covers in characteristic *p*, *Compositio Math*. **52** (1984), 31–45.
4. Goursat, É.: *A Course in Mathematical Analysis*, Vol. 1, Ginn, 1904.
5. Katz, N.: Slope filtration of F-crystals, *Astérisque* **63** (1979), 113–164.
6. Katz, N.: Crystalline cohomology, Dieudonné modules, and Jacobi sums, In: *Automorphic Forms, Representation Theory and Arithmetic*, Tata Inst. Fundam. Res., Bombay, 1979, pp. 165–246.
7. Koblitz, N.: *p-adic analysis: A Short Course on Recent Work*, London Math. Soc. Lecture Note Ser. 46, Cambridge Univ. Press, 1980.
8. Lenstra, H. W., Jr. and Oort, F.: Simple abelian varieties having a prescribed formal isogeny type, *J. Pure Appl. Algebra* **4** (1974), 47–53.
9. Manin, Y.: The theory of commutative formal groups over fields of finite characteristic, *Russian Math. Surveys* **18** (1963), 1–84.
10. Mazur, B.: Frobenius and the Hodge filtration, *Ann. of Math*. **98** (1973), 58–95.
11. Nakajima, S.: Equivariant form of the Deuring-Shafarevich formula for Hasse–Witt invariants, *Math. Z*. **190** (1985), 559–566.
12. Nygaard, N.: On supersingular abelian varieties, In: *Algebraic Geometry* (*Ann Arbor, Mich., 1981*), Lecture Notes in Math. 1008, Springer, New York, 1983, pp. 83–101.
13. Scholten, J. and Zhu, H. J.: Hyperelliptic curves in characteristic 2, *Inter. Math. Res. Notices* **17** (2002), 905–917.
14. Scholten, J. and Hu, J. H.: The first slope case of Wan's conjecture, *Finite Fields Appl*. **8** (2002), 414–419.
15. Scholten, J. and Zhu, H. J.: Families of supersingular curves in characteristic 2, *Math. Res. Lett*. **9** (2002), 639–650.
16. Stichtenoth, H.: *Algebraic Function Fields and Codes*, Universitext, Springer-Verlag, Berlin.
17. van der Geer, G. and van der Vlugt, M.: Reed-Muller codes and supersingular curves. I, *Compositio Math*. **84** (1992), 333–367.
18. van der Geer, G. and van der Vlugt, M.: On the existence of supersingular curves of given genus, *J. Reine Angew. Math*. **458** (1995), 53–61.
19. Zhu, H. J.: *p*-adic variation of *L* functions of exponential sums, I, to appear in *Amer. J. Math*. **125** (2003).