RAMIFICATION OF WILD AUTOMORPHISMS OF LAURENT SERIES FIELDS

KENZ KALLAL AND HUDSON KIRKPATRICK

Abstract. Let $K$ be a complete discrete valuation field with residue class field $k$, where both are of positive characteristic $p$. Then the group of wild automorphisms of $K$ can be identified with the group under composition of formal power series over $k$ with no constant term and $X$-coefficient 1. Under the hypothesis that $p > b^2$, we compute the first nontrivial coefficient of the $p$th iterate of a power series over $k$ of the form $f = X + \sum_{i \geq 1} a_i X^{ki+1}$. As a result, we obtain a necessary and sufficient condition for an automorphism to be “$b$-ramified,” having lower ramification numbers of the form $\nu_n(f) = b(1 + \cdots + p^n)$. This is a vast generalization of Nordqvist’s 2017 theorem on 2-ramified power series, as well as the analogous result for minimally ramified power series which proved to be useful for arithmetic dynamics in a 2013 paper of Lindahl on linearization discs in $\mathbb{C}_p$ and a 2015 result of Lindahl–Rivera-Letelier on optimal cycles over nonarchimedean fields of positive residue characteristic. The success of our computation is also promising progress towards a generalization of Lindahl–Nordqvist’s 2018 theorem bounding the norm of periodic points of 2-ramified power series.

1. Introduction

Let $k$ be a field of characteristic $p > 0$, and consider the complete discrete valuation field $K = k((X))$ under the $X$-adic valuation. Any $k$-linear automorphism of $K$ is continuous, and therefore determined by a choice of the image of $X$ in the set of non-units of $k[[X]]$. The group of wild automorphisms, the subgroup of $\text{Aut}(K/k)$ consisting of all $\sigma$ such that $\nu_X(\sigma(X) - X) > 1$, can therefore be identified with the following group of formal power series over $k$.

Definition 1.1 ($\mathcal{N}(k)$). We write $\mathcal{N}(k)$ to denote the group under composition of formal power series of the form

$$f(X) = X + \sum_{i=2}^{\infty} a_i X^i$$

with coefficients $a_i \in k$.

Remark. In the case $k = \mathbb{F}_p$, the group $\mathcal{N}(k)$ is called the Nottingham group. It is an example of a pro-$p$ group, and is thus of general interest in both group theory and number theory (see [22, Ch. 1] and [3, Ch. 10]). It was first introduced by Jennings [6], Johnson [7] and York [23, 24]. Of particular importance to group theory are some results of Leedham-Green–Weiss and Camina [2, Theorems 3 and 5]; they state that every finite $p$-group can be embedded in $\mathcal{N}(\mathbb{F}_p)$, and every countably-based pro-$p$ group can be embedded as a closed subgroup of $\mathcal{N}(\mathbb{F}_p)$. Other important group-theoretic considerations about the Nottingham group are those about torsion: Klopsch [9] classified all elements of $\mathcal{N}(\mathbb{F}_p)$ of order $p$ up to conjugacy, and his result was generalized by Jean [5] and Lubin [18] to order $p^n$ (see also [1]).

In this paper we always use the notation $f^n$ to mean the $n$-th iterate of $f \in \mathcal{N}(k)$. By taking compositional inverses, this notation is well-defined for any $n \in \mathbb{Z}$. If $G \subseteq \text{Aut}(K/k)$ is the group of wild $k$-linear automorphisms, then the identification $\mathcal{N}(k) \overset{\sim}{\to} G$ is given by mapping $f(X)$ to the automorphism $g \mapsto g \circ f^{-1}$. In this way, composition and inverses of automorphisms correspond to the same operations for power series (where the inverses are compositional inverses). This gives a convenient explicit way to describe the higher ramification groups of $K/k$. For a given power series $f \in \mathcal{N}(k)$, we are interested in the ramification numbers with respect to the filtration of ramification groups of $\text{Aut}(K/k)$ of the $\sigma \in \text{Aut}(K/k)$ corresponding
to $f$ and its iterates. From the identification between $\mathcal{N}(k)$ and the group of wild automorphisms of $K$, the ramification number of $f$ should be a constant factor from $\nu_X(f^{-1}(X) - X)$. Since the ramification groups are groups, the ramification number of $f$ is the same as that of $f^{-1}$. Consistent with this, we can define the ramification numbers explicitly in terms of power series without worrying about taking inverses:

**Definition 1.2** (Ramification). The ramification number of $f \in \mathcal{N}(k)$ is

$$i(f) := \nu_X(f(X) - X) - 1.$$ 

Note that this normalizes the ramification number so that the least ramified $f \in \mathcal{N}(k)$ have $i(f) = 1$ instead of 2.

We will frequently mention the “$n^{th}$ ramification number” of $f$, that is, $i_n(f) := i(f^n)$. In fact, we are interested in power series with certain types of sequences of ramification numbers.

**Definition 1.3.** Let $f \in \mathcal{N}(k)$ and $b \geq 1$. We write that $f$ is $b$-ramified if it has ramification numbers of the form

$$i_n(f) = b(1 + p + \cdots + p^n)$$

for all $n \geq 0$.

We will justify the choice of ramification of this form with Theorem 2.5, a powerful result of Laubie and Saïne which restricts it to that form under certain conditions. We will also see that $b$-ramification is the minimal sequence of ramification numbers given $i(f) = b$. The main question that this paper is concerned with is the following:

**Question 1.4.** Let $b \in \mathbb{N}$ with $p \nmid b$. Given a sequence $\{a_i\}_{i \geq 1}$ of coefficients in $k$, is the formal power series

$$f(X) = X + \sum_{i=1}^{\infty} a_i X^{i+b} \in \mathcal{N}(k)$$

$b$-ramified?

We will call $a_1, \ldots, a_n$ as defined in Question 1.4 the “first $n$ nontrivial coefficients of $f$.” Nordqvist [19] solved Question 1.4 for $b = 2$ by giving a polynomial condition on finitely many of the $a_i$’s. This itself is a generalization of the characterization of minimally ramified power series (see [20, Exemple 3.19] or somewhat more generally [14, Theorem E]). The computations that lead to these results have been relevant to many important theorems in nonarchimedean dynamical systems [11, 16, 12, 14, 20, 15].

The main result of this paper generalizes the polynomial condition given by Nordvist to the following under certain hypotheses:

**Definition 1.5** ($P_b$). For $b \in \mathbb{N}$, define the polynomial in $\mathbb{Z}[x_1, \ldots, x_{b+1}]$

$$P_b(x_1, \ldots, x_{b+1}) := (b+1)x_1^{b+1} + 2 \sum_{(e_1, \ldots, e_{b+1})} (-1)^{e_2 + \cdots + e_{b+1}} \frac{(e_2 + \cdots + e_{b+1})!}{e_2! \cdots e_{b+1}!} x_1^{e_1} \cdots x_{b+1}^{e_{b+1}}$$

where the sum is taken over all tuples $(e_1, \ldots, e_{b+1}) \in \mathbb{Z}_{\geq 0}^{b+1}$ such that $\sum_{i=1}^{b+1} e_i = b$ and $\sum_{i=1}^{b+1} ie_i = 2b$.

This polynomial is what results from a computation of the first nontrivial coefficient of $f^p$ given those of $f$.

The main result of this paper is the following theorem\footnote{Since we posted on arXiv.org a draft of this paper containing this result, Jonas Nordqvist and Juan Rivera-Letelier informed us in a private communication that they have independently proved a version of it using the language of iterative residues.}, answering Question 1.4 in the case where $b^2 < p$.

**Theorem 1.6.** Fix an odd prime $p$ and $b \in \mathbb{N}$ such that $b^2 < p$, and let $k$ be an arbitrary field of characteristic $p$. Let $f(X) = X + \sum_{i=1}^{\infty} a_i X^{i+b} \in \mathcal{N}(k)$. Then $f$ is $b$-ramified if and only if $a_1 \neq 0$ and $P_b(a_1, \ldots, a_{b+1}) \neq 0$. 
Note that the resulting
\[
P_1 = 2x_1^2 - 2x_2 \\
P_2 = 3x_1^3 + 2x_2^2 - 2x_1x_3
\]
agree with the previous results of Rivera-Letelier [20, Exemple 3.19] and Nordqvist [19, Theorem 1] answering Question 1.4 in the cases \( b = 1, 2 \).

This paper is organized as follows. In Section 2, we describe the historical results on ramification numbers of power series which are necessary for our work. In Section 3, we give an explicit computation of the first nontrivial coefficient of the \( p \)-th iterate of a power series \( f \in \mathcal{N}(k) \) with \( i(f) = b \), which yields the desired necessary and sufficient condition for \( f \) being \( b \)-ramified. In Section 4, we describe the implications this computation has for a generalization of Lindahl–Nordqvist’s work in [13] on the locations of periodic points in the open unit disc of a nonarchimedean field of characteristic \( p \) under iteration of power series.

2. Ramification of Power Series

In this section and the next, \( k \) is taken, as usual, to be an arbitrary field of characteristic \( p > 0 \). It is useful to have strong restrictions on the possible sequences of ramification numbers of elements of \( \mathcal{N}(k) \).

The most important historical result with regard to this is due to Sen [21, Theorem 1]:

**Theorem 2.1** (Sen, 1969). Let \( f \in \mathcal{N}(k) \), where \( k \) is a field of characteristic \( p > 0 \). Then for all \( n \in \mathbb{N} \),
\[
i_n(f) \equiv i_{n-1}(f) \pmod{p^n}.
\]

Sen originally stated Theorem 2.1 under the hypothesis that \( k \) is also perfect, but it holds in the more general setting by an argument due to Lubin [17, pg. 64]. The following corollary immediately follows from power series computations and Sen’s Theorem.

**Corollary 2.2.** Let \( f \in \mathcal{N}(k) \). Then for all \( n \geq 0 \),
\[
i_n(f) \geq 1 + p + \cdots + p^n.
\]

Power series \( f \in \mathcal{N}(k) \) for which equality holds in (2.3) are called minimally ramified. Another useful result is a theorem of Keating [8, Theorem 7], which gives a general form for \( i_n(f) \) given the first two ramification numbers under certain conditions.

**Theorem 2.4** (Keating, 1992). Let \( f \in \mathcal{N}(k) \). If \( i_0(f) = 1 \) and \( i_1(f) = 1 + bp \) with \( 1 \leq b \leq p - 2 \), then
\[
i_n(f) = 1 + bp + \cdots + bp^n.
\]

We will use a powerful generalization of Theorem 2.4 from [10, Theorem 2].

**Theorem 2.5** (Laubie and Saïne, 1997). Let \( f \in \mathcal{N}(k) \). Then the following hold:

1. If \( p|\ell(f) \), then \( i_n(f) = p^\ell f(f) \) for all \( n \geq 0 \).
2. Otherwise, if \( i_1(f) < (p^2 - p + 1)i(f) \), then
\[
i_n(f) = i(f) + (1 + \cdots + p^{n-1})(i_1(f) - i(f))
\]
for all \( n \geq 1 \).

It follows from Theorem 2.5 that if \( f \in \mathcal{N}(k) \) with \( i(f) = b \), \( i_1(f) = b + bp \) and \( p \nmid b \), then \( f \) is \( b \)-ramified. Since \( b \)-ramified power series must have \( i(f) = b \), to answer Question 1.4 it suffices to determine the power series \( f = X + \sum_{i=1}^{\infty} a_i X^{i+b} \) with \( a_1 \neq 0 \) with the property that \( i(f^p) = b + bp \).

The special case \( b = 2 \) was solved using exactly this technique in [19, Theorem 1]:

**Theorem 2.6** (Nordqvist, 2017). A power series given by \( f(X) = X + \sum_{i=1}^{\infty} a_i X^{i+2} \in \mathcal{N}(k) \) is \( 2 \)-ramified if and only if \( 3a_3^2 + 2a_2^3 - 2a_2a_3 \neq 0 \) and \( a_1 \neq 0 \).

We will prove a similar result for the \( b \)-ramified power series in \( \mathcal{N}(k) \) when \( p > b^2 \).
3. Classification of $b$-Ramified Power Series

Let $b \in \mathbb{N}$, and suppose $p > b^2$. Let

$$f(X) = X + a_1X^{b+1} + a_2X^{b+2} + \cdots \in \mathcal{N}(k),$$

where $a_1 \neq 0$ so that $i_0(f) = b$. By Theorem 2.5, $f$ is $b$-ramified if and only if $i_1(f) = b + bp$. Therefore, it suffices to compute the coefficients on the terms of degree at most $b + bp + 1$ in $f^p$ in terms of the $a_i$'s. To do this, we rely on a technique established in [14, Lemma 3.6]. In particular, define the power series $\{\Delta_m\}_{m \geq 1}$ recursively by $\Delta_1 = f(X) - X$ and

$$\Delta_{m+1} = \Delta_m \circ f - \Delta_m.$$

It is straightforward to check the following lemma by induction:

**Lemma 3.1.** Suppose $m \in \mathbb{N}$. Then,

$$\Delta_m(X) = \sum_{i=0}^{m} (-1)^i \binom{m}{i} f^{m-i}(X).$$

The following corollary is immediate by elementary properties of binomial coefficients modulo $p$:

**Corollary 3.2.** $\Delta_p(X) = f^p(X) - X$.

Therefore, the desired quantity is

$$i(f^p) = \nu_X(\Delta_p) - 1,$$

so it suffices to compute the coefficients of $\Delta_p$. In particular, we wish to compute $\Delta_p$ modulo $X^{b+bp+2}$, since this will provide us with all the coefficients of $f$ on the terms of degree at most $b + bp + 1$, as desired.

To do this, we prove a simple lemma that allows us to set up the necessary computational infrastructure.

**Lemma 3.3.** $\nu_X(\Delta_m) \geq bm + 1$ for all $m \in \mathbb{N}$.

**Proof.** We proceed by induction. For the base case, we have already that

$$\Delta_1 = f(X) - X = a_1X^{b+1} + \cdots,$$

so $\nu_X(\Delta_1) = b + 1$ as desired. Now, assume the inductive hypothesis that $\nu_X(\Delta_m) \geq bm + 1$ for some $m \in \mathbb{N}$. This means that we can write

$$\Delta_m = A_1(m)X^{bm+1} + A_2(m)X^{bm+2} + \cdots$$

for some $A_1(m), \ldots \in \mathbb{F}_p$. From here it is clear (from the definition of $f$) that the term of least degree in

$$\Delta_{m+1}(X) = (A_1(m)f(X)^{bm+1} + A_2(m)f(X)^{bm+2} + \cdots) - (A_1(m)X^{bm+1} + A_2(m)X^{bm+2} + \cdots)$$

has degree at least $b(m+1) + 1$ [in particular the term of least degree that is not guaranteed to be cancelled by subtracting $\Delta_m$ is produced by the term of $A_1(m)f(X)^{bm+1}$ produced by choosing $bm$ copies of $X$ and one copy of $X^{b+1}$]. The desired result follows by induction.

**Corollary 3.4.** $i_1(f) \geq bp$.

**Corollary 3.5.** $i_1(f) \geq bp + b$.

**Proof.** By Sen’s Theorem, $i_1(f) \equiv i_0(f) = b \pmod{p}$, which means that $i_1(f) = b + np$ for some integer $n$. If $n < b$, then by the assumption that $p > b$ (recall we actually assumed the stronger bound $p > b^2$), we have

$$i_1(f) = b + np \leq b + (b-1)p = bp + (b-p) < bp,$$

which contradicts the previous corollary. 

\[ \square \]
Corollary 3.5 means that under the hypothesis that $p > b$, $b$-ramification is the minimal possible ramification type subject to the condition $i_0(f) = b$.

By Lemma 3.3, there are no terms of degree at most $bp$ in $\Delta_p$. Thus, we only need to consider the terms of degree $d$ for $bp + 1 \leq d \leq b + bp + 1$. In the language of the proof of the lemma, we need only to compute the coefficients $A_1(p), \ldots, A_{b+1}(p)$ in terms of the $a_i$’s. But Corollary 3.5 guarantees that $A_1(p), \ldots, A_b(p)$ are identically zero. It remains to compute $A_{b+1}(p)$ in terms of the $a_i$’s, which will in turn give us a criterion for $b$-ramification: by Theorem 2.5, $f$ is $b$-ramified if and only if $A_{b+1}(p) \neq 0$. To do this, we compute using the recursive definition of the $A_i(m)$’s. In particular, we can compute modulo $X^{b+b(m+1)+2}$ that since $f(X)^n$ for $n > b + bm + 1$ can contribute no term that isn’t cancelled by subtracting $\Delta_{m+1}(X)$,

$$\Delta_{m+1}(X) \equiv A_1(m)f(X)^{bm+1} + A_2(m)f(X)^{bm+2} + \cdots + A_b(m)f(X)^{bm+b} + A_{b+1}(m)f(X)^{bm+b+1} - \Delta_m(X)$$

Recalling from the definition of $\Delta_1$ that $A_1(1) = a_i$, this is equivalent to defining the $A_i(m)$’s by the recurrence

$$\begin{bmatrix} A_1(m+1) \\ A_2(m+1) \\ \vdots \\ A_b(m+1) \\ A_{b+1}(m+1) \end{bmatrix} = \begin{bmatrix} a_1(bm+1) \\ a_2(bm+1) \\ \vdots \\ a_b(bm+1) \\ a^2(bm+1) + a_{b+1}(bm+1) \end{bmatrix} \begin{bmatrix} A_1(m) \\ A_2(m) \\ \vdots \\ A_b(m) \\ A_{b+1}(m) \end{bmatrix}$$

with initial conditions

$$\begin{bmatrix} A_1(1) \\ A_2(1) \\ \vdots \\ A_b(1) \\ A_{b+1}(1) \end{bmatrix} = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_b \\ a_{b+1} \end{bmatrix}.$$
And for \( \ell = b + 1 \),
\[
A_{b+1}(m) = a_{b+1}a_1^{m-1}\frac{(bm + 1)!}{bm + 1} + a_1^{m+1} \frac{b}{2} \sum_{r=1}^{m-1} \frac{(bm + 1)!}{(br + b)!} \frac{(br + 1)!}{(br + 1)!} + a_0a_1^{m-1}\frac{1}{b} \sum_{r=1}^{m-1} \frac{(bm + 1)!}{(br + b)!} \cdot
\]
\[
+ \sum_{\substack{b \geq \alpha_1 \geq \ldots \geq \alpha_n > 0 \\ \{\alpha_i\} \neq \{b\}}} \left( a_1^{m-n-1}a_{b-\alpha_1 + 2}a_{\alpha_1} \prod_{i=1}^{n-1} a_{\alpha_i - \alpha_{i-1} + 1} \right).
\]

**Proof.** This is easily shown from the recursive descriptions of the \( A_i(m) \) and the following observation from [4, §1.2], described in a similar form by [19, Lemma 4]:

**Lemma 3.7.** Let \( f, g : \mathbb{N} \to k \). Then the difference equation
\[
A(n + 1) = f(n)A(n) + g(n)
\]
with initial condition \( A(1) = a \) is uniquely satisfied by
\[
A(m) = \left[ \prod_{j=1}^{m-1} f(j) \right] a + \sum_{r=1}^{m-1} \left[ \prod_{j=r+1}^{m-1} f(j) \right] g(r).
\]

Using the result for \( A_1, \ldots, A_{k-1} \) for \( g \) and applying the recursive definition above, we get the summation form for \( A_k \) as desired. \( \square \)

Recall that all equalities are stated in \( k \), and all the quantities in Proposition 3.6 other than the \( \alpha_i \)'s are just integers which are reduced modulo \( p \); they are in \( \mathbb{F}_p \subseteq k \), so we can compute them as elements of \( \mathbb{F}_p \). By taking an inverse of \( b \) modulo \( p \), we can simplify the expressions by making them include factorials instead of \( b \)-tuple factorials:

**Lemma 3.8.** Let \( y \in \{0, 1, \ldots, b - 1\} \) and \( x \geq 0 \). Then we have an equality of reductions modulo \( p \)
\[
(bx + y)^{t(b)} = b^x \frac{(x + yt)!}{(yt)!},
\]
where \( t \) is the smallest lift of \( b^{-1} \in \mathbb{F}_p \) to \( \mathbb{N} \).

**Proof.** In \( \mathbb{F}_p \) we can write
\[
(bx + y)^{t(b)} = (bx + y)(b(x - 1) + y) \cdots (b + y).
\]
Multiplying by \( t^x = (b^x)^{-1} \), we have
\[
(bx + y)^{t(b)} = b^x (x + yt)(x - 1 + yt) \cdots (1 + yt) = b^x \frac{(x + yt)!}{(yt)!}
\]
as desired. \( \square \)

Applying Lemma 3.8 to the last part of Proposition 3.6, we get

**Proposition 3.9.** The first nontrivial coefficient of \( f^p \) is
\[
A_{b+1}(p) = a_{b+1}a_1^{p-1}b^p \frac{(p + t)!}{t!(b + 1)!} + a_1^{p+1} \frac{b}{2} \sum_{r=1}^{p-1} \frac{(p + t)!}{(r + t)!} \frac{(r + t)!}{(r + 1 + t)!} + a_0a_1^{p-1}b^p \sum_{r=1}^{p-1} \frac{(p + t)!}{(r + 1 + t)!} + a_{b-1}a_{b-2}a_1^{p-2} \sum_{r=1}^{p-1} \frac{(p + t)!}{(r + 1 + t)!} \cdot
\]
\[
+ b^{p-1} \sum_{b > \alpha_1 > \ldots > \alpha_n > 0} \left( a_1^{p-n-1}a_{b-\alpha_1 + 2}a \prod_{i=1}^{n-1} a_{\alpha_i - \alpha_{i-1} + 1} \right).
\]
The goal of the rest of this section is to compute a more convenient form for these sums. We will frequently and without comment compute only residues mod $p$, passing to $\mathbb{Q}_p$ and moving factors of $p$ in denominators around whenever necessary.

**Proposition 3.10.**

\[
 b^p \frac{(p+t)!}{t!(b+1)!} = b^p \sum_{r=1}^{p-1} \frac{(p+t)!(r+1)!}{(r+1+t)!} = 0, \quad \frac{b}{2} \sum_{r=1}^{p-1} \frac{(p+t)!(r+1)!}{(r+1+t)!} b^{p-1} r = \frac{b+1}{2}.
\]

**Proof.** We start with the first expression. The fact that $b^p \frac{(p+t)!}{t!(b+1)!}$ vanishes in $\mathbb{F}_p$ is obvious from the fact that $b+1 < p$. For the second expression, Wilson’s Theorem gives us $(r+1)! = (-1)^r/(p-r-2)!$ for positive $r < p - 1$ and the $r = p-1$, $r < p - t - 1$ terms are obviously zero so we have

\[
 \sum_{r=1}^{p-1} \frac{(p+t)!(r+1)!}{(r+1+t)!} = \sum_{r=p-t-1}^{p-2} (-1)^r \frac{(p+t)!}{(r+1+t)!(p-r-2)!}
\]

\[
 = (p+t) \sum_{r=p-t-1}^{p-2} (-1)^r \binom{p+t-1}{r+t+1}
\]

\[
 = t \sum_{i=0}^{t-1} (-1)^i \binom{p+t-1}{p+i} \binom{t-1}{i}
\]

\[
 = 0
\]

by the binomial theorem, as desired. The congruence $(\binom{p+t-1}{i}) \equiv \binom{t-1}{i} \pmod{p}$ is evident either from writing them down as quotients and cancelling factors of $p$ or as a special case of Lucas’s Theorem.

Finally, the only nonzero term in the third sum $\sum_{r=1}^{p-1} \frac{(p+t)!(r+t)!}{(r+1+t)!} b^{p-1} r$ occurs when $r + 1 + t = p$, i.e. $r = p - t - 1$. Therefore,

\[
 \frac{b}{2} \sum_{r=1}^{p-1} \frac{(p+t)!(r+t)!}{(r+1+t)!} b^{p-1} r = \frac{b}{2} \frac{(p+t)!(p-1)!}{(p)!} b^{p-1}(p-t-1)
\]

\[
 = -\frac{b}{2} \frac{p!}{p!} b^{p-1}(p-t-1)
\]

\[
 = \frac{b}{2} \cdot (t+1)
\]

\[
 = \frac{b+1}{2}
\]

which proves the proposition. \(\square\)
For the remaining two terms, we proceed by induction. From the form that we have reduced them to, it suffices to compute the sum
\[
\varphi_\beta(\alpha_1, \ldots, \alpha_n) := \sum_{i=1}^{n-1} \sum_{i_n=1}^{i_n-1} \sum_{i_{n-1}=1}^{i_{n-1}-1} \frac{(p+t)!(i_1 + \alpha_1 t)\cdots (i_n + \alpha_n t + \beta)!}{(i_1 + t)! (i_2 + \alpha_2 t)\cdots (i_{n-1} + \alpha_{n-1} t)! (\alpha_n t)!} \in \mathbf{F}_p
\]
where $\beta < b$ is a nonnegative integer, and $\alpha_1 > \cdots > \alpha_n$ are positive integers at most $b$. In fact, we will show that this expression has a much simpler form in terms of the inputs:

**Proposition 3.11.** Let $\beta, \alpha_1, \ldots, \alpha_n$ be as above. Then
\[
\varphi_\beta(\alpha_1, \ldots, \alpha_n) = (-1)^n \delta(\alpha_1, 1) \delta(\beta, 0)
\]
where $\delta(\cdot, \cdot)$ denotes the Kronecker delta.

**Proof.** Let $n \geq 2$, $\beta < b$ and $b \geq \alpha_1 > \cdots > \alpha_n > 0$ be integers. We claim the result is true by induction on $n$.

Fix $i_{n-1} < p$. Then by cancelling factors of $p$ and analyzing the factors left over, we have that $\sum_{i_n=1}^{i_n-1} \frac{(i_n + \alpha_n t + \beta + (\alpha_n-1 - \alpha_n)p)!\left[\frac{i_n + \alpha_n t + \beta}{p}\right]}{(i_n + \alpha_n - 1)!((\alpha_n-1 - \alpha_n)p)!((\alpha_n-1 - \alpha_n + 1)\cdots (\alpha_n-1 + \alpha_n + \left[\frac{i_n + \alpha_n t + \beta}{p}\right])}
\]
reduces to
\[
\sum_{i_n=1}^{i_n-1} \frac{(i_n + \alpha_n t + \beta + (\alpha_n-1 - \alpha_n)p)!\left[\frac{i_n + \alpha_n t + \beta}{p}\right]}{(i_n + \alpha_n - 1)!((\alpha_n-1 - \alpha_n)p)!((\alpha_n-1 - \alpha_n + 1)\cdots (\alpha_n-1 + \alpha_n + \left[\frac{i_n + \alpha_n t + \beta}{p}\right])}
\]
\[
= \sum_{i_n=1}^{i_n-1} \frac{(i_n + \alpha_n t + \beta + (\alpha_n-1 - \alpha_n)p)!\left[\frac{i_n + \alpha_n t + \beta}{p}\right]}{(i_n + \alpha_n - 1)!((\alpha_n-1 - \alpha_n)p)!((\alpha_n-1 - \alpha_n + 1)\cdots (\alpha_n-1 + \alpha_n + \left[\frac{i_n + \alpha_n t + \beta}{p}\right])}
\]
\[
\frac{(i_n + \alpha_n t + \beta + (\alpha_n-1 - \alpha_n)p)!\left[\frac{i_n + \alpha_n t + \beta}{p}\right]}{(i_n + \alpha_n - 1)!((\alpha_n-1 - \alpha_n)p)!((\alpha_n-1 - \alpha_n + 1)\cdots (\alpha_n-1 + \alpha_n + \left[\frac{i_n + \alpha_n t + \beta}{p}\right])}
\]
\[
\frac{(i_n + \alpha_n t + \beta + (\alpha_n-1 - \alpha_n)p)!\left[\frac{i_n + \alpha_n t + \beta}{p}\right]}{(i_n + \alpha_n - 1)!((\alpha_n-1 - \alpha_n)p)!((\alpha_n-1 - \alpha_n + 1)\cdots (\alpha_n-1 + \alpha_n + \left[\frac{i_n + \alpha_n t + \beta}{p}\right])}
\]
\[
\frac{(i_n + \alpha_n t + \beta + (\alpha_n-1 - \alpha_n)p)!\left[\frac{i_n + \alpha_n t + \beta}{p}\right]}{(i_n + \alpha_n - 1)!((\alpha_n-1 - \alpha_n)p)!((\alpha_n-1 - \alpha_n + 1)\cdots (\alpha_n-1 + \alpha_n + \left[\frac{i_n + \alpha_n t + \beta}{p}\right])}
\]
Of course, $\left[\frac{i_n + \alpha_n t + \beta}{p}\right]$ can only take on the values $\left[\frac{\alpha_n t + \beta}{p}\right]$ and $\left[\frac{\alpha_n t + \beta}{p}\right] + 1$ depending on whether $i_n$ is sufficiently large (since we know a priori that $i_n < p$). In particular, the former value is taken on if and only if $i_n < [\alpha_n t + \beta]_p - (\alpha_n t + \beta)$ (here $[x]_p$ denotes the least multiple of $p$ which is greater than $x$; note that this means $[kp]_p = (k+1)p$). If $i_n-1 < [\alpha_n t + \beta]_p - (\alpha_n t + \beta)$, then $i_n \leq i_{n-1} - 1 < [\alpha_n t + \beta]_p - (\alpha_n t + \beta) - 1$, so we have $\left[\frac{i_n + \alpha_n t + \beta}{p}\right] = \left[\frac{\alpha_n t + \beta}{p}\right]$ (in particular it doesn’t depend on any of the indices in the sum). Therefore, in this case we have
\[
\sum_{i_n=1}^{i_n-1} \frac{(i_n + \alpha_n t + \beta)!}{(i_n + \alpha_n - 1)!} = \frac{(i_n + \alpha_n t + \beta)!}{(i_n + \alpha_n - 1)!} \frac{(\alpha_n-1 + \alpha_n + 1)\cdots (\alpha_n-1 + \alpha_n + \left[\frac{i_n + \alpha_n t + \beta}{p}\right])}{(\alpha_n-1 + \alpha_n + 1)\cdots (\alpha_n-1 + \alpha_n + \left[\frac{i_n + \alpha_n t + \beta}{p}\right])}
\]
By the hockey stick identity, the sum on the right hand side is
\[
\left(\frac{(i_n-1 + \alpha_n t + \beta + (\alpha_n-1 - \alpha_n)p)!}{(i_n-1 + \alpha_n t + \beta + (\alpha_n-1 - \alpha_n)p)!} - \frac{(i_n-1 + \alpha_n t + \beta + (\alpha_n-1 - \alpha_n)p)!}{(i_n-1 + \alpha_n t + \beta + (\alpha_n-1 - \alpha_n)p)!}\right)
\]
\[
= \frac{(i_n-1 + \alpha_n t + \beta + (\alpha_n-1 - \alpha_n)p)!}{(i_n-1 + \alpha_n t + \beta + (\alpha_n-1 - \alpha_n)p)!} - \frac{(i_n-1 + \alpha_n t + \beta + (\alpha_n-1 - \alpha_n)p)!}{(i_n-1 + \alpha_n t + \beta + (\alpha_n-1 - \alpha_n)p)!}
\]
\[
= \frac{(i_n-1 + \alpha_n t + \beta + (\alpha_n-1 - \alpha_n)p)!}{(i_n-1 + \alpha_n t + \beta + (\alpha_n-1 - \alpha_n)p)!} - \frac{(i_n-1 + \alpha_n t + \beta + (\alpha_n-1 - \alpha_n)p)!}{(i_n-1 + \alpha_n t + \beta + (\alpha_n-1 - \alpha_n)p)!}
\]
\[
= \frac{(i_n-1 + \alpha_n t + \beta + (\alpha_n-1 - \alpha_n)p)!}{(i_n-1 + \alpha_n t + \beta + (\alpha_n-1 - \alpha_n)p)!} - \frac{(i_n-1 + \alpha_n t + \beta + (\alpha_n-1 - \alpha_n)p)!}{(i_n-1 + \alpha_n t + \beta + (\alpha_n-1 - \alpha_n)p)!}
\]
\[
= \frac{(i_n-1 + \alpha_n t + \beta + (\alpha_n-1 - \alpha_n)p)!}{(i_n-1 + \alpha_n t + \beta + (\alpha_n-1 - \alpha_n)p)!} - \frac{(i_n-1 + \alpha_n t + \beta + (\alpha_n-1 - \alpha_n)p)!}{(i_n-1 + \alpha_n t + \beta + (\alpha_n-1 - \alpha_n)p)!}
\]
\[
= \frac{(i_n-1 + \alpha_n t + \beta + (\alpha_n-1 - \alpha_n)p)!}{(i_n-1 + \alpha_n t + \beta + (\alpha_n-1 - \alpha_n)p)!} - \frac{(i_n-1 + \alpha_n t + \beta + (\alpha_n-1 - \alpha_n)p)!}{(i_n-1 + \alpha_n t + \beta + (\alpha_n-1 - \alpha_n)p)!}
\]
\[
= \frac{(i_n-1 + \alpha_n t + \beta + (\alpha_n-1 - \alpha_n)p)!}{(i_n-1 + \alpha_n t + \beta + (\alpha_n-1 - \alpha_n)p)!} - \frac{(i_n-1 + \alpha_n t + \beta + (\alpha_n-1 - \alpha_n)p)!}{(i_n-1 + \alpha_n t + \beta + (\alpha_n-1 - \alpha_n)p)!}
\]
Recall the assumption that $i_{n-1} < [\alpha_n t + \beta] - (\alpha_n t + \beta)$, from which it follows that $\left\lceil \frac{i_{n-1} + \alpha_n t + \beta}{p} \right\rceil = \left\lceil \frac{\alpha_n t + \beta}{p} \right\rceil$ and thus

\begin{equation}
\sum_{i_n=1}^{i_{n-1}-1} \frac{(i_n + \alpha_n t + \beta)!}{(i_n + \alpha_{n-1} t)!} = \frac{(i_{n-1} + \alpha_n t + \beta)!}{(i_{n-1} + \alpha_{n-1} t - 1)!(\beta + 1 - (\alpha_{n-1} - \alpha_n)t)} - \frac{(\alpha_n t + \beta + 1)!\ell(\alpha_{n-1}, \alpha_n)}{(\alpha_{n-1} t)!((\beta + 1 - (\alpha_{n-1} - \alpha_n)t))}
\end{equation}

where $\ell(\alpha_{n-1}, \alpha_n)$ is defined to be $1$ if $\left\lceil \frac{1 + \alpha_n t + \beta}{p} \right\rceil = \left\lceil \frac{\alpha_n t + \beta}{p} \right\rceil$ (i.e., if $\alpha_n t + \beta \equiv -1 \mod p$) and otherwise

$$
\ell(\alpha_{n-1}, \alpha_n) := \frac{\alpha_{n-1} - \alpha_n + \left\lceil \frac{\alpha_n t + \beta}{p} \right\rceil + 1}{\frac{\alpha_{n-1} + \left\lceil \frac{\alpha_n t + \beta}{p} \right\rceil}{\alpha_{n-1} - \alpha_n + \left\lceil \frac{\alpha_n t + \beta}{p} \right\rceil + 1}}.
$$

In the remaining case, $i_{n-1} \geq [\alpha_n t + \beta] - (\alpha_n t + \beta)$, so $\sum_{i_n=1}^{i_{n-1}-1} \frac{(i_n + \alpha_n t + \beta)!}{(i_n + \alpha_{n-1} t)!}$ reduces to

\begin{equation}
\sum_{i_n=1}^{[\alpha_n t + \beta] - (\alpha_n t + \beta) - 1} \frac{(i_n + \alpha_n t + \beta)!}{(i_n + \alpha_{n-1} t)!} + \sum_{i_n = [\alpha_n t + \beta] - (\alpha_n t + \beta)}^{i_{n-1}-1} \frac{(i_n + \alpha_n t + \beta)!}{(i_n + \alpha_{n-1} t)!} = \frac{(\alpha_{n-1} - \alpha_n)(p - t + \beta)!\left\lceil \frac{\alpha_n t + \beta}{p} \right\rceil)!}{((\alpha_{n-1} - \alpha_n)p)!((\alpha_{n-1} - \alpha_n + 1) \cdots (\alpha_{n-1} - \alpha_n + \left\lceil \frac{\alpha_n t + \beta}{p} \right\rceil)!}
\end{equation}

$$
= \left\lceil \frac{\alpha_n t + \beta}{p} \right\rceil \sum_{i_n=1}^{[\alpha_n t + \beta] - (\alpha_n t + \beta) - 1} \frac{(i_n + \alpha_n t + \beta + (\alpha_{n-1} - \alpha_n)t)}{i_n + \alpha_{n-1} t} \sum_{i_n = [\alpha_n t + \beta] - (\alpha_n t + \beta)}^{i_{n-1}-1} \frac{(i_n + \alpha_n t + \beta + (\alpha_{n-1} - \alpha_n)t)}{i_n + \alpha_{n-1} t}.
$$

Using the hockey stick identity,

\begin{equation}
\sum_{i_n=1}^{[\alpha_n t + \beta] - (\alpha_n t + \beta) - 1} \frac{(i_n + \alpha_n t + \beta + (\alpha_{n-1} - \alpha_n)p)}{i_n + \alpha_{n-1} t} = \left(\frac{[\alpha_n t + \beta] + (\alpha_{n-1} - \alpha_n)p}{[\alpha_n t + \beta] + (\alpha_{n-1} - \alpha_n)p} - \frac{\alpha_n t + \beta + 1 + (\alpha_{n-1} - \alpha_n)p}{\alpha_{n-1} t}\right)
\end{equation}

while

\begin{equation}
\sum_{i_n = [\alpha_n t + \beta] - (\alpha_n t + \beta)}^{i_{n-1}-1} \frac{(i_n + \alpha_n t + \beta + (\alpha_{n-1} - \alpha_n)p)}{i_n + \alpha_{n-1} t} = \left(\frac{[\alpha_n t + \beta] + (\alpha_{n-1} - \alpha_n)p}{[\alpha_n t + \beta] + (\alpha_{n-1} - \alpha_n)p} - \frac{[\alpha_n t + \beta] + (\alpha_{n-1} - \alpha_n)p}{[\alpha_n t + \beta] + (\alpha_{n-1} - \alpha_n)p}\right).
\end{equation}

Therefore, it suffices to compute these four binomial coefficients modulo $p$; note that the second one may be written as a specialization of the third to $i_{n-1} = 1$. As before, we can write that

\begin{equation}
\left(\frac{i_{n-1} + \alpha_n t + \beta + (\alpha_{n-1} - \alpha_n)p}{i_{n-1} + \alpha_{n-1} t - 1}\right)
\end{equation}

reduces to

\begin{equation}
\frac{(i_{n-1} + \alpha_n t + \beta)!((\alpha_{n-1} - \alpha_n)p)!((\alpha_{n-1} - \alpha_n + 1) \cdots (\alpha_{n-1} - \alpha_n + \left\lceil \frac{i_{n-1} + \alpha_n t + \beta}{p} \right\rceil)!}{(i_{n-1} + \alpha_{n-1} t - 1)!(\alpha_{n-1} - \alpha_n)!((\alpha_{n-1} - \alpha_n)(p + t + \beta + 1)!(\left\lceil \frac{i_{n-1} + \alpha_n t + \beta}{p} \right\rceil)!\cdot)
\end{equation}

Since $b^2 < p$, the smallest lift of the inverse of $b$ modulo $p$ must be greater than $b$. Hence,

$$
\beta < b < t \leq (\alpha_{n-1} - \alpha_n)t
$$
so we can write $\beta + 1 \leq (\alpha_{n-1} - \alpha_n)t$. Using the same manipulations as before,

$$\left[\alpha_nt + \beta\right]_p + (\alpha_{n-1} - \alpha_n)p$$

$$\left[\alpha_nt + \beta\right]_p + (\alpha_{n-1} - \alpha_n)t - \beta - 1$$

therefore reduces to

$$\frac{((\alpha_{n-1} - \alpha_n)p)![(\alpha_n t + \beta)_p](\alpha_{n-1} - \alpha_n + 1) \cdots (\alpha_{n-1} - \alpha_n + \left\lfloor \frac{\alpha_{n-1} - \alpha_n}{p} \right\rfloor + 1)(\alpha_{n-1} - \alpha_n + 1 - \beta - 1)}{((\alpha_{n-1} - \alpha_n)p)![(\alpha_n t + \beta)_p](\alpha_{n-1} - \alpha_n + 1) \cdots (\alpha_{n-1} - \alpha_n + \left\lfloor \frac{\alpha_{n-1} - \alpha_n}{p} \right\rfloor + 2) \cdots ((\alpha_{n-1} - \alpha_n)t - \beta - 1))((\alpha_{n-1} - \alpha_n)(p - t) + \beta + 1)!}$$

Finally,

$$\left(\alpha_nt + \beta + 1 + (\alpha_{n-1} - \alpha_n)p\right)$$

reduces to

$$\frac{(\alpha_{n-1} - \alpha_n)p)!((\alpha_{n-1} - \alpha_n)p)!(\alpha_{n-1} - \alpha_n + 1 \cdots (\alpha_{n-1} - \alpha_n + \left\lfloor \frac{\alpha_{n-1} - \alpha_n}{p} \right\rfloor)!}{(\alpha_{n-1}t)!((\alpha_{n-1} - \alpha_n)(p - t) + \beta + 1)!\left\lfloor \frac{\alpha_{n-1} - \alpha_n}{p} \right\rfloor!}$$

so we can write in this case by substituting our computations into (3.13),

$$\sum_{i_{n-1}=1}^{\left\lfloor \frac{\alpha_{n-1} - \alpha_n}{p} \right\rfloor} (i_{n-1} + \alpha_{n-1}t + \beta)! - \frac{(\alpha_{n-1} - \alpha_n)(p - t) + \beta + 1)\left\lfloor \frac{\alpha_{n-1} - \alpha_n}{p} \right\rfloor!}{(\alpha_{n-1} - \alpha_n)!((\alpha_{n-1} - \alpha_n)(p - t) + \beta + 1)\left\lfloor \frac{\alpha_{n-1} - \alpha_n}{p} \right\rfloor!}$$

Recall that $\phi(\alpha_1, \ldots, \alpha_n)$ is defined by

$$\phi(\alpha_1, \ldots, \alpha_n) := \sum_{i=1}^{p-1} \cdots \sum_{i_{n-1}=1}^{i_{n-2} - 1} \frac{(p+t)(i_1 + \alpha_1 t) \cdots (i_n + \alpha_n t + \beta)!}{(i_1 + 1 + t)!(i_2 + \alpha_2 t) \cdots (i_n + \alpha_n t - \beta - 1)!}(\alpha_{n-1} - \alpha_n t + \beta - 1)!$$

and that when $\beta = 0$ this is the last kind of coefficient we want to compute (see Proposition 3.9). Since the last two terms in our expression for $\sum_{i_{n-1}=1}^{i_{n-2} - 1} (i_{n-1} + \alpha_n t + \beta)!$ are the same modulo $p$ as entire expression in the case $i_{n-1} < [\alpha_n t + \beta]_p - (\alpha_n t + \beta)$ (see (3.12)), we can conclude that

$$\phi(\alpha_1, \ldots, \alpha_n) = c_1 \sum_{i_{n-1}=1}^{i_{n-2} - 1} \frac{(p+t)(i_1 + \alpha_1 t) \cdots (i_n + \alpha_n t + \beta)!}{(i_1 + 1 + t)!(i_2 + \alpha_2 t) \cdots (i_n + \alpha_n t - \beta - 1)!}(\alpha_{n-1} - \alpha_n t + \beta - 1)!$$

$$+ c_2 \sum_{i_{n-1}=1}^{i_{n-2} - 1} \frac{(p+t)(i_1 + \alpha_1 t) \cdots (i_n + \alpha_n t + \beta)!}{(i_1 + 1 + t)!(i_2 + \alpha_2 t) \cdots (i_n + \alpha_n t - \beta - 1)!}(\alpha_{n-1} - \alpha_n t + \beta - 1)!$$

$$+ \frac{1}{1 + \beta - (\alpha_{n-1} - \alpha_n)t}.$$
It follows by induction that 
\[ (p + t)!(i_1 + 1 + t) ![i_2 + a_1 t] ![i_{n-1} + a_n t + \beta] ![i_{n-1} + a_n t + 1 + t - 1]! \]
where \( c_1, c_2 \in \mathbb{F}_p^* \) (i.e. they have no factors of \( p \) in numerator or denominator) and they depend only on the \( a_i \)'s. Note that the terms of the first sum are of the form 
\[ \sum_{i_1=1}^{p-1} \cdots \sum_{i_{n-1} = 1}^{i_n - 2} \frac{(p + t)!(i_1 + a_1 t) ![i_2 + a_1 t] ![i_{n-1} + a_n t + \beta] ![i_{n-1} + a_n t + 1 + t - 1]!}{(i_1 + 1 + t) ![i_2 + a_1 t] ![i_{n-1} + a_n t + 1 + t - 1]!} \]
and from the fact that \( i_{n-1} + a_n t + \beta \geq [a_n t + \beta]_p \) it is immediate that this is zero modulo \( p \). Therefore, each term of the first sum is zero, and we can ignore it altogether. The second sum is equal to 
\[ c_2 \frac{(a_\alpha t + \beta + 1)!}{(a_n !)} \sum_{i_1=1}^{p-1} \cdots \sum_{i_{n-1} = 1}^{i_n - 2} \frac{(p + t)!(i_1 + 1 + t) ![i_2 + a_1 t] ![i_{n-1} + a_n t + 1 + t - 1]!}{(i_1 + 1 + t) ![i_2 + a_1 t] ![i_{n-1} + a_n t + 1 + t - 1]!} \]
which is 
\[ c_2 \frac{(a_\alpha t + \beta + 1)!}{(a_n !)} \phi_0 (a_1, \ldots, a_{n-1}) = 0 \]
by induction (since \( a_{n-1} > a_n \geq 1 \)). Therefore, \( \varphi_\beta (a_1, \ldots, a_n) \) is
\[ \frac{1}{1 - (a_n - 1 - a_n t)!} \sum_{i_1=1}^{p-1} \cdots \sum_{i_{n-1} = 1}^{i_n - 2} \frac{(p + t)!(i_1 + 1 + t) ![i_2 + a_1 t] ![i_{n-1} + a_n t + 1 + t - 1]!}{(i_1 + 1 + t) ![i_2 + a_1 t] ![i_{n-1} + a_n t + 1 + t - 1]!} \]
\[ = \frac{1}{1 - (a_n - 1 - a_n t)!} \varphi_{\beta + 1} (a_1, \ldots, a_{n-2}, a_n) - \varphi_{\beta} (a_1, \ldots, a_{n-2}, a_n) \]
by induction since \( \beta + 1 > 0 \).

The base case \((n = 1)\) also lends itself well to our methods: if \( \alpha > 1 \) or if \( \beta > 0 \), then \( i_1 + a_1 t + \beta \geq i_1 + 1 + t \)
and we can write 
\[ \varphi_\beta (a_1) = \sum_{i_1=1}^{p-1} \frac{(p + t)!(i_1 + a_1 t + \beta)!}{(i_1 + 1 + t) ![a_1 t] !} = \frac{(p + t)!(a_1 - 1)! + \beta)!}{(a_1 t) ![1 + \beta)!} \sum_{i_1=1}^{p-1} \frac{1}{(i_1 + 1 + t) ![a_1 t] !} \]
\[ = \frac{(p + t)!(a_1 - 1)! + \beta)!}{(a_1 t) ![1 + \beta)!} \left( \frac{p + \alpha t + \beta}{p + t} - \frac{1 + \alpha t + \beta}{1 + t} \right) \]
\[ = 0. \]

On the other hand, if \( \alpha = 1 \) and \( \beta = 0 \), we find that 
\[ \varphi_\beta (a_1) = \sum_{i_1=1}^{p-1} \frac{(p + t)!(i_1 + 1 + t) ![t] !}{(i_1 + 1 + t) ![t] !} \]
and the only nonzero term in this sum occurs when \( i_1 + 1 + t = p \). Thus, 
\[ \varphi_\beta (a_1) = \frac{(p + t)!(p - 1)!}{p ![1) !} = -1. \]
It follows by induction that \( \varphi_\beta (a_1, \ldots, a_n) = 0 \) if \( \alpha > 1 \) or \( \beta > 0 \), and otherwise it is \((-1)^n \).

Applying Proposition 3.10 and Proposition 3.11 to the sums achieved in Proposition 3.9, we obtain
\[ (3.14) \quad A_{b+1} (p) = \frac{b + 1}{2} a_1 a_{b+1} + \sum_{n=1}^{b} (-1)^n a_1^{p - n} \sum_{b_{\alpha_1} > \ldots > \alpha_n} a_{b_{\alpha_1} + 2} \prod_{i=1}^{n-1} a_{\alpha_i - \alpha_i + 1}. \]
A careful analysis of the terms in this sum yields the main theorem of this paper.
Proof of Theorem 1.6. Recall from Corollary 3.5 that \( A_{b+1}(p) \) is the first nonzero coefficient of \( \Delta_p \), and that \( A_{b+1}(p) \) is the \( X^{bp+b+1} \)-coefficient of \( \Delta_p \). By Corollary 3.2, it follows that \( i_1(f) = bp + b \) if and only if \( A_{b+1}(p) \neq 0 \). By Theorem 2.5, \( f \) is \( b \)-ramified if and only if \( i_1(f) = bp + b \), so in fact \( f \) is \( b \)-ramified if and only if \( A_{b+1}(p) \neq 0 \).

Since \( a_1 \neq 0 \), we can multiply (3.14) by \( 2a_1^{-bp} \) to get that \( f \) is \( b \)-ramified if and only if

\[(b + 1)a_1^{b+1} + 2 \sum_{n=1}^{b} (-1)^n a_1^{b-n} \sum_{b \geq \alpha_1 > \cdots > \alpha_n = 1} a_{b-\alpha_1 + 2}^{b-\alpha_1} \prod_{i=1}^{n-1} a_{\alpha_i - \alpha_{i+1} + 1}^{b-\alpha_1} \neq 0.

Fixing \( n \), the term \( a_2^{e_2} \cdots a_{b+1}^{e_{b+1}} \) appears exactly \( \binom{e_2 + \cdots + e_{b+1}}{e_2, \ldots, e_{b+1}} \) times. Since \( n = e_2 + \cdots + e_{b+1} \) (in particular it is determined by the \( e_i \)'s), any monomial can only appear for at most one value of \( n \). In fact, \( a_2^{e_2} \cdots a_{b+1}^{e_{b+1}} \) shows up if and only if \( e_2 + 2e_3 + \cdots + be_{b+1} = b \). In this case,

\[e_1 = b - n = b - (e_2 + \cdots + e_{b+1})
\]

so this condition is equivalent to \( a_1^{e_1} \cdots a_{b+1}^{e_{b+1}} \) appearing in the entire sum if and only if

\[e_1 + 2e_2 + \cdots + (b+1)e_{b+1} = 2b
\]

and

\[e_1 + e_2 + \cdots + e_{b+1} = b.
\]

It follows that \( f \) is \( b \)-ramified if and only if

\[(b + 1)a_1^{b+1} + \sum_{e_1 + \cdots + e_{b+1} = 2b \atop e_1 + 2e_2 + \cdots + (b+1)e_{b+1} = 2b} 2(-1)^{e_2 + \cdots + e_{b+1}} \binom{e_2 + \cdots + e_{b+1}}{e_2, \ldots, e_{b+1}} a_1^{e_1} \cdots a_{b+1}^{e_{b+1}} \neq 0.
\]

We have finally recovered the polynomial (see Definition 1.5) \( P_b(a_1, \ldots, a_{b+1}) \) as the criterion for \( f \) being \( b \)-ramified. Adding in the assumption that \( a_1 \neq 0 \) from the beginning of this section (which is implied by \( i(f) = b \)), the desired result is established. \( \square \)

4. Further Work and Applications to Nonarchimedean Dynamics

The case where \( k \) is perfect, so that \( \mathcal{N}(k) \) is the group of wild automorphisms of the local field \( k((X)) \), is a natural application of Theorem 1.6. Our results are also of interest for their application to the case where \( k \) is equipped with a nonarchimedean valuation, and the power series over \( k \) are considered as acting on the open unit disc in \( k \). In this section, \( k \) is taken to be a nonarchimedean field of characteristic \( p \) with absolute value \( | \cdot | \).

The ramification numbers of a power series, as we have defined them in Definition 1.2, are only originally defined as being naturally an invariant of the corresponding automorphism of \( k((X)) \). However, in [14] and [15], Lindahl and Rivera-Letelier found a deep connection between the ramification numbers of a power series over an arbitrary nonarchimedean field of characteristic \( p \) and the location of its periodic points. In particular, if \( k \) is a nonarchimedean field of characteristic \( p \), then the power series

\[f(z) \in z(1 + zO_k[[z]])
\]

converge on the open unit disc \( m_k \), and all of their periodic points have minimal period of the form \( p^n \) (see [14, Lemma 2.1]). The relevant general lemma is from [15, Lemma 2.4]:

**Lemma 4.1.** Suppose \( f(z) \in \mathcal{N}(k) \) with \( i_n(f) < \infty \) for all \( n \geq 0 \), and let \( z_0 \in m_k \) be a periodic point under the action of \( f \) of minimal period \( p^n \). Then

\[|z_0| \geq \left| \frac{\delta_n(f)}{\delta_{n-1}(f)} \right|^{\frac{1}{p^n}},
\]

where \( \delta_n(f) \) denotes the \( X^{i_n(f)+1} \)-coefficient of \( fp^n \).
Using this fact and a computation of the relevant coefficient of \( f^p \), Lindahl and Nordqvist (see [13, Theorem A]) proved a lower bound on the norm of periodic points under the action of 2-ramified power series:

**Theorem 4.2** (Lindahl and Nordqvist, 2018). Suppose \( p \geq 5 \) and let

\[
f(z) = z + \sum_{i=1}^{\infty} a_i z^{i+2} \in \mathcal{O}_k[[z]].
\]

If \( z_0 \in \mathfrak{m}_k \) is a periodic point of period \( p^n \) under the action of \( f \), then

\[
|z_0| \geq \left| a_1^{p-3} \left( \frac{3}{2} a_1^3 + a_2^2 - a_1 a_3 \right) \right|^{\frac{1}{p}}.
\]

The bound for \( |z_0| \) comes from the computation of the first nontrivial coefficient of \( f^p \), and it turns out to not depend on \( n \) at all. Since the bound is a nonzero scalar multiple of the absolute value of \( P_2 \), it is only nontrivial so long as \( f \) is 2-ramified. Based on the the independence on \( n \) in that case, we conjecture that the analogous bound is true for \( b \)-ramified power series.

**Conjecture 4.3.** Let \( b \in \mathbb{N} \) and suppose that \( p > b^2 \) is a prime. Moreover, let

\[
f = z + \sum_{i=1}^{\infty} a_i z^{i+b}
\]

be a formal power series with coefficients in \( \mathcal{O}_k \), where \( a_1 \neq 0 \). If \( z_0 \in \mathfrak{m}_k \) is a periodic point of period \( p^n \) under the action of \( f \), then

\[
|z_0| \geq \left| a_1^{p-b-1} \left( \frac{2}{P_b(a_1, \ldots, a_{b+1})} \right) \right|^{\frac{1}{p}}.
\]

Our computation of the relevant coefficient of \( f^p \) in (3.14), combined with Lemma 4.1 gives a proof of Conjecture 4.3 in the case \( n = 1 \). For the general case, the appropriate coefficient of \( f^p \) must be computed as well\(^2\). After conjugating by a translation, scaling, and taking iterates if necessary (see the remarks in [15, p. 2]), this conjecture implies via the invariance of ramification under conjugation that any periodic point of a \( b \)-ramified power series over a nonarchimedean field of characteristic \( p > b^2 \) is isolated. That would add additional cases under which the main theorem of [15] holds, which represents progress towards [14, Conjecture 1.2].

**Acknowledgments**

The results in this paper originated from a project at PROMYS 2016. We are deeply grateful to Laurent Berger and Sandra Rozensztajn for proposing this problem, and for their mentoring. We also thank our PROMYS research lab counselor Alyosha Latynstsev for his support, as well as Krishanu Sankar, David Fried, Glenn Stevens, the PROMYS Foundation, and the Clay Mathematics Institute for making this research possible. In their most general form, many of the computations in this paper were completed at the University of Chicago REU during the summer of 2018. Therefore, the first author thanks his mentor Drew Moore for the encouragement he gave, as well as J.P. May for making the REU possible. Finally, we would like to thank Jonas Nordqvist and Juan Rivera-Letelier for their helpful correspondence with us regarding the hypotheses and implications of Conjecture 4.3.

---

\(^2\)Since we posted on arXiv.org a draft of this paper containing this conjecture, Jonas Nordqvist and Juan Rivera-Letelier informed us in a private communication that they have developed the required computation and therefore proved Conjecture 4.3.
References

[1] Frauke M Bleher, Ted Chinburg, Bjorn Poonen, and Peter Symonds. Automorphisms of Harbater–Katz–Gabber curves. Mathematische Annalen, 368(1-2):811–836, 2017.

[2] Rachel Camina. Subgroups of the Nottingham group. Journal of Algebra, 196(1):101–113, 1997.

[3] Marcus du Sautoy, Dan Segal, and Aner Shalev. New Horizons in pro-p Groups. New Horizons in Pro-p Groups. Birkhäuser Boston, 2000.

[4] Saber Elaydi. An Introduction to Difference Equations. Springer Science & Business Media, 2005.

[5] Sandrine Jean. Conjugacy classes of series in positive characteristic and Witt vectors. Journal de Théorie des Nombres de Bordeaux, 21(2):263–284, 2009.

[6] S.A. Jennings. Substitution groups of formal power series under substitution. Canadian Journal of Mathematics, 6:325 – 340, 1954.

[7] D. L. Johnson. The group of formal power series under substitution. Journal of the Australian Mathematical Society. Series A – Pure Mathematics and Statistics, 45(3):296–302, 04 2009.

[8] Kevin Keating. Automorphisms and extensions of k((t)). Journal of Number Theory, 41(3):314 – 321, 1992.

[9] Benjamin Klopsch. Automorphisms of the Nottingham group. Journal of Algebra, 223(1):37 – 56, 2000.

[10] F Laubie and M Saïne. Ramification of automorphisms of k((t)). Journal of Number Theory, 63(1):143 – 145, 1997.

[11] François Laubie, Abbas Movahhedi, and Alain Salinier. Systèmes dynamiques non archimédiens et corps des norms (non-archimedean dynamic systems and fields of norms). Compositio Mathematica, 132(1):57–98, 2002.

[12] Karl-Olof Lindahl. The size of quadratic p-adic linearization disks. Advances in Mathematics, 248:872 – 894, 2013.

[13] Karl-Olof Lindahl and Jonas Nordqvist. Geometric location of periodic points of 2-ramified power series. Journal of Mathematical Analysis and Applications, 2018.

[14] Karl-Olof Lindahl and Juan Rivera-Letelier. Optimal cycles in ultrametric dynamics and minimally ramified power series. Compositio Mathematica, 152(1):187–222, 009 2015.

[15] Karl-Olof Lindahl and Juan Rivera-Letelier. Generic parabolic points are isolated in positive characteristic. Nonlinearity, 29(5):1596, 2016.

[16] Jonathan Lubin. Nonarchimedean dynamical systems. Compositio Mathematica, 94(3):321–346, 1994.

[17] Jonathan Lubin. Sen’s theorem on iteration of power series. Proceedings of the American Mathematical Society, 123(1):63–66, 1995.

[18] Jonathan Lubin. Torsion in the Nottingham group. Bulletin of the London Mathematical Society, 43(3), 2011.

[19] Jonas Nordqvist. Characterization of 2-ramified power series. Journal of Number Theory, 174:258–273, 2017.

[20] J. Rivera-Letelier. Dynamique des fonctions rationelles sur des corps locaux. PhD thesis, Université de Paris XI, 2000.

[21] Shankar Sen. On automorphisms of local fields. Annals of Mathematics, 90(1):33–46, 1969.

[22] Jean-Pierre Serre. Galois cohomology. Springer Science & Business Media, 2013.

[23] I.O. York. The exponent of certain p-groups. Proceedings of the Edinburgh Mathematical Society, 33:483–490, 1990.

[24] I.O. York. The group of formal power series under substitution. PhD thesis, Nottingham University, 1990.

Department of Mathematics, Harvard University, Cambridge, MA 02138
E-mail address: kenzkallal@college.harvard.edu

Department of Mathematics, Princeton University, Princeton, NJ 08544-1000
E-mail address: Hbk@princeton.edu