PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 130, Number 2, Pages 379–386
S 0002-9939(01)06166-4
Article electronically published on July 25, 2001

ON HEIGHTS OF p-ADIC DYNAMICAL SYSTEMS

HUA-CHIEH LI

(Communicated by David E. Rohrlich)

Abstract. When we consider the properties of the iterates of a noninvertible endomorphism of a formal group, all the roots of iterates of the endomorphism are simple and the full commuting family contains both invertible and noninvertible series. Experimental evidence seems to suggest that for an invertible series to commute with a noninvertible series with only simple roots of iterates, two such commuting power series must be endomorphisms of a single formal group. Lubin proposed four conjectures to support this conjecture. In this paper, we provide answers to these four conjectures.

1. Introduction

In this paper, we consider analytic transformations of the p-adic open unit disk with a fixed point at 0. When such a transformation is an endomorphism of a formal group, the field generated by all roots or fixed points of its iterates is well known due to the efforts of Lubin and Tate [6] and Serre [10]. In general, when a transformation does not belong to any formal group, very little is known and so it is a very interesting area for exploration.

Let K be an algebraic extension of $\mathbb{Q}_p$ and let $\mathcal{O}$ be its integer ring with maximal ideal $\mathcal{M}$. If $\overline{K}$ is an algebraic closure of K, we denote by $\overline{\mathcal{O}}$ and $\overline{\mathcal{M}}$ the integral closure of $\mathcal{O}$ in $\overline{K}$ and the maximal ideal of $\overline{\mathcal{O}}$, respectively. Recall that K is a field which is complete with respect to a valuation, v. We normalize the valuation v such that $v(p) = 1$.

We say that a series $g(x) \in \mathcal{O}[[x]]$ is *stable* if $g(0) = 0$ and $g'(0)$ is not 0 nor a root of 1. When $g(x) \in \mathcal{O}[[x]]$, but not all coefficients of $g(x)$ are in $\mathcal{M}$, then the lowest degree in which a unit coefficient appears will be called the *Weierstrass degree* of $g(x)$, denoted $\operatorname{wideg}(g)$. If all coefficients are in $\mathcal{M}$, we will say that the Weierstrass degree is infinite. If $\operatorname{wideg}(g) = d < \infty$, then according to the Weierstrass Preparation Theorem, counting multiplicity, there are d roots of $g(x)$ that are in $\overline{\mathcal{M}}$.

We can split the study of stable series into two parts: one is $\operatorname{wideg}(g) > 1$ and the other one is $\operatorname{wideg}(g) = 1$.

The first kind of series are called *noninvertible stable series*. Let $f(x)$ be a noninvertible stable series. Because $f'(0) \in \mathcal{M}$, it has 0 as an attracting fixed point and has no other fixed point in $\overline{\mathcal{M}}$. When a noninvertible series $g(x)$ commutes with $f(x)$ (in the sense of composition), the set of roots of iterates of $f(x)$ in $\overline{\mathcal{M}}$

Received by the editors July 18, 2000.
2000 *Mathematics Subject Classification.* Primary 11S99; Secondary 11S31, 14S05.

is equal to the set of roots of iterates of $g(x)$ in $\overline{\mathcal{M}}$ (Lubin [7, Proposition 2.1]). Therefore, the roots of iterates are of serious interest. It is important to know that if $\operatorname{wideg}(f) < \infty$, then there are infinitely many elements of $\overline{\mathcal{M}}$ that are roots of iterates of $f(x)$ (Lubin [7]).

The other type of series is called *invertible stable series*, because if $u(x) \in \mathcal{O}[[x]]$ with $u'(0) \in \mathcal{O}^*$, then there exists a series $w(x) \in \mathcal{O}[[x]]$ such that $u \circ w(x) = x$. Let $u(x)$ be an invertible stable series in $\mathcal{O}[[x]]$. Since $u(x)$ is invertible, it and its iterates can have no other roots than 0. We denote $u^{\circ n}(x)$ the n-fold iteration of $u(x)$ with itself. The point $\alpha \in \overline{\mathcal{M}}$ is a *fixed point* for $u(x)$ if $u(\alpha) = \alpha$. The point α is a *periodic point* of period n if $u^{\circ n}(\alpha) = \alpha$. The periodic points of $u(x)$ now play a role parallel to the roots of iterates of a noninvertible series. We assume that the series $u(x)$ always satisfies $u'(0) \in 1 + \mathcal{M}$; finiteness of the residue field guarantees that any invertible series has an iterate with this property. Let $p \nmid m$. It is important to know that if α is a periodic point of period $p^n m$, then it is a periodic point of period p^n (Li [2, Corollary 2.3.2]). Therefore, we only have to study periodic points whose periods are powers of p.

The studies of these two kinds of series become no longer disjoint in case an invertible stable series $u(x)$ commutes with a noninvertible stable series $f(x)$. In fact, in this case the set of periodic points of $u(x)$ in $\overline{\mathcal{M}}$ is the same as the set of roots of iterates of $f(x)$ in $\overline{\mathcal{M}}$ (Lubin [7, Proposition 3.2]).

When we consider the properties of the iterates of an noninvertible endomorphism $f(x)$ of a formal group defined over $\mathcal{O}$, it is easy to show that all the roots of iterates of $f(x)$ are simple and the full commuting family contains both invertible and noninvertible stable series. Experimental evidence seems to suggest that for an invertible stable series to commute with a noninvertible stable series with only simple roots of iterates, two such commuting power series must be endomorphisms of a single formal group. Lubin's Main Theorem 6.3 in [7] supports this conjecture, in that it says that the only possible finite Weierstrass degree for such a noninvertible series is a power of p.

Definition 1.1. Let $f(x) \in \mathcal{O}[[x]]$ be a noninvertible stable series with $\operatorname{wideg}(f) < \infty$. We define the *height* of $f(x)$ equal to

$$\operatorname{height}(f) = \frac{\log_p(\operatorname{wideg}(f))}{v(f'(0))}.$$

We remark that if $f(x)$ is an endomorphism of a formal group, then $\operatorname{height}(f)$ would be the height of the formal group.

Let $u(x) \in \mathcal{O}[[x]]$ be an invertible stable series with $u'(0) \equiv 1 \pmod{\mathcal{M}}$. Denote $i_n(u) = \operatorname{wideg}(u^{\circ p^n}(x) - x)$. Notice that if $i_n(u) < \infty$, then $i_n(u)$ is the number of periodic points of $u(x)$ of period p^n, counting multiplicity. Sen's theorem [9] shows that when $i_n(u) < \infty$ then $i_{n-1}(u) \equiv i_n(u) \pmod{p^n}$. Keating [1], using local class field theory, says that under certain circumstance we have $i_n(u) = 2 + bp + \cdots + bp^n$, for some $0 < b < p$. When $u(x)$ commutes with a noninvertible stable series $f(x)$ with $\operatorname{wideg}(f) < \infty$, it is important to know that $i_n(u) < \infty$ for all n and $i_n(u) \to \infty$ as $n \to \infty$. In fact, according to Lubin [7], Corollary 4.3.1, we have that if $i_n(u) = \infty$ for some n, then $u(x)$ has only finitely many periodic points in $\overline{\mathcal{M}}$. However, $u(x)$ must have infinitely many periodic points in $\overline{\mathcal{M}}$, because the set of periodic points of $u(x)$ in $\overline{\mathcal{M}}$ is the same as the set of roots of iterates of $f(x)$ in $\overline{\mathcal{M}}$ and there are infinitely many roots of iterates of $f(x)$ in $\overline{\mathcal{M}}$, since $\operatorname{wideg}(f) < \infty$.

In this case, we have an effective method to compute $i_n(u)$. Theorem 3.9 in [3] says that there exist M and a positive integer λ such that when $n > M$,

$$\frac{i_{n+1}(u) - i_n(u)}{i_n(u) - i_{n-1}(u)} = p^\lambda.$$

Definition 1.2. Let $u(x) \in \mathcal{O}[[x]]$ be an invertible stable series with $u'(0) \equiv 1 \pmod{\mathcal{M}}$. We say that the *Height* of $u(x)$ exists if the value of

$$\log_p\left(\frac{\operatorname{wideg}(u^{\circ p^r}(x) - x)}{\operatorname{wideg}(u^{\circ p^{r-1}}(x) - x)}\right)$$

stabilizes as $r \to \infty$ and denote by $\operatorname{Height}(u)$ the stable value.

We remark that if $u(x)$ is an automorphism of a formal group, then $\operatorname{Height}(u)$ would be the height of the formal group.

Throughout this paper the power series $f(x)$ and $u(x)$ always satisfy the following assumptions:

- $f(x) \in \mathcal{O}[[x]]$ is a noninvertible stable series with finite Weierstrass degree,
- all roots of iterates of $f(x)$ are simple,
- $u(x) \in \mathcal{O}[[x]]$ is an invertible stable series with $u'(0) \equiv 1 \pmod{\mathcal{M}}$, and
- $u(x)$ and $f(x)$ commute.

Motivated by the general properties of formal groups, Lubin [8] made the following four conjectures.

Conjecture 1. $\operatorname{height}(f)$ *is an integer.*

We remark that if the roots of iterates of $f(x)$ are not always simple, then this conjecture is not true. For instance, for $p = 2$, $f(x) = 4x + x^2$ commutes with $u(x) = 9x + 6x^2 + x^3$, but we have $\operatorname{height}(f)$ equal to $1/2$.

Conjecture 2. $\operatorname{Height}(u)$ *exists.*

Note that even in the formal group case, $\operatorname{wideg}(u^{\circ p^r}(x) - x)/\operatorname{wideg}(u^{\circ p^{r-1}}(x) - x)$ is not constant until r gets large enough.

Conjecture 3. $\operatorname{height}(f) = \operatorname{Height}(u)$.

Conjecture 4. $\operatorname{wideg}(u^{\circ p^r}(x) - x)$ *is always a power of* p.

We remark that these conjectures are automatically true if $f(x)$ and $u(x)$ are endomorphisms of a formal group. In this paper, we will show that Conjectures 1, 2 and 3 are always true and Conjecture 4 is true when K is unramified over $\mathbb{Q}_p$.

2. Proof of Conjecture 2

Lubin's fourth conjecture says that if an invertible series $u(x)$ commutes with a noninvertible series, then $\operatorname{wideg}(u^{\circ p^n}(x) - x)$ is a power of p for all n. In section 4, we will prove that this is always true if $u(x)$ is a power series over the ring of integers of an unramified extension of $\mathbb{Q}_p$. In the general case, we have the following result which says that $\operatorname{wideg}(u^{\circ p^n}(x) - x)$ is a power of p for n sufficiently large.

Lemma 2.1. *There exists a constant C (depending only on $f(x)$) such that if $v(u'(0) - 1) > C$, then* $\operatorname{wideg}(u^{\circ p^n}(x) - x)$ *is a power of p for all n. Furthermore, if $v(f'(0)) = v(u'(0) - 1)$, then* $\operatorname{wideg}(f) = \operatorname{wideg}(u(x) - x)$.

Proof. See Li [4], Theorem 4.1 and Corollary 4.1.1. □

In fact, given any invertible series $u(x)$ with $u'(0)-1 \in \mathcal{M}$ and $u'(0)$ not a root of 1, since $(u^{\circ p^n})'(0) = (u'(0))^{p^n}$, we have that $v((u^{\circ p^n})'(0)-1) \to \infty$ as $n \to \infty$. Hence, Lemma 2.1 says that $\mathrm{wideg}(u^{\circ p^n}(x)-x)$ is a power of p for n sufficiently large.

Theorem 2.2 (Conjecture 2)**.** *There exists an integer λ such that*

$$\mathrm{wideg}(u^{\circ p^n}(x)-x) = p^\lambda \cdot \mathrm{wideg}(u^{\circ p^{n-1}}(x)-x),$$

for all n sufficiently large. In particular, $\mathrm{Height}(u)$ *exists and equals λ.*

Proof. Let $i_n = \mathrm{wideg}(u^{\circ p^n}(x)-x)$. Recall that since $u(x)$ commutes with a noninvertible series, there exists an integer λ such that $(i_{n+1}-i_n)/(i_n-i_{n-1}) = p^\lambda$ for all n sufficiently large. By Lemma 2.1, for n large enough, i_{n+1}, i_n and i_{n-1} are all powers of p. This implies that $i_n = p^\lambda i_{n-1}$, for all n large enough. Thus,

$$\mathrm{wideg}(u^{\circ p^n}(x)-x)/\mathrm{wideg}(u^{\circ p^{n-1}}(x)-x) = i_n/i_{n-1} = p^\lambda,$$

for n large enough. Hence, $\mathrm{wideg}(u^{\circ p^n}(x)-x)/\mathrm{wideg}(u^{\circ p^{n-1}}(x)-x)$ stabilizes as $n \to \infty$ and $\mathrm{Height}(u) = \lambda$. □

3. Proof of Conjectures 1 and 3

We first show that the definition of the height of a noninvertible series is well defined. Because we are mainly interested in the roots of iterates and periodic points of stable series, it is natural to say that two series $g(x)$ and $h(x)$ in $\mathcal{O}[[x]]$ are in the same dynamical system if $h \circ g = g \circ h$. The following result shows that if two noninvertible series are in the same dynamical system, then they have the same height.

Lemma 3.1. *Let $h(x)$, $g(x) \in \mathcal{O}[[x]]$ be noninvertible stable series such that $h \circ g = g \circ h$. Then* $\mathrm{height}(h) = \mathrm{height}(g)$.

Proof. Since $h \circ g = g \circ h$, by [5, Corollary 3.2.1], we have that

$$\mathrm{wideg}(g)^{v(h'(0))} = \mathrm{wideg}(h)^{v(g'(0))}.$$

Taking $\log_p$ on both sides, we have that

$$\mathrm{height}(h) = \log_p(\mathrm{wideg}(h))/v(h'(0)) = \log_p(\mathrm{wideg}(g))/v(g'(0)) = \mathrm{height}(g).$$

□

Theorem 3.2 (Conjectures 1 and 3)**.** $\mathrm{height}(f)$ *is an integer and* $\mathrm{height}(f) = \mathrm{Height}(u)$.

Proof. Suppose that $a \in \mathcal{M}$ and $v(a) > v(p)/(p-1) = 1/(p-1)$. Then it is easy to show that $v((1+a)^p - 1) = v(pa) = v(a)+1$. By induction, we have that $v((1+a)^{p^n}-1) = v(a)+n$. Hence, if n is large enough and $m > n$, then

$$v((u^{\circ p^m})'(0)-1) = v((u^{\circ p^n})'(0)-1) + (m-n).$$

Choose n large enough and $m > n$ such that $r \cdot v(f'(0)) = v((f^{\circ r})'(0)) = v((u^{\circ p^n})'(0)-1)$ and $s \cdot v(f'(0)) = v((f^{\circ s})'(0)) = v((u^{\circ p^m})'(0)-1)$ for some r and s. Since both $f^{\circ r}(x)$ and $f^{\circ s}(x)$ commute with $u(x)$, by Lemma 2.1, we have that $\mathrm{wideg}(f^{\circ r}(x)) = i_n$ and $\mathrm{wideg}(f^{\circ s}(x)) = i_m$. Also because both $f^{\circ r}(x)$ and

$f^{\circ s}(x)$ commute with $f(x)$, by Lemma 3.1, we have that height$(f) = $ height$(f^{\circ r}) = $ height$(f^{\circ s})$. Hence,

$$\frac{\log_p(i_n)}{v((u^{\circ p^n})'(0)-1)} = \text{height}(f^{\circ r}) = \text{height}(f^{\circ s}) = \frac{\log_p(i_m)}{v((u^{\circ p^m})'(0)-1)}.$$

Substitute $i_m = p^{\lambda(m-n)} i_n$ and $v((u^{\circ p^m})'(0)-1) = v((u^{\circ p^n})'(0)-1) + (m-n)$ into the equality. We have that

$$\lambda = \frac{\log_p(i_n)}{v((u^{\circ p^n})'(0)-1)} = \text{height}(f^{\circ r}) = \text{height}(f).$$

This shows that height(f) is an integer and height$(f) = \lambda = $ Height(u). □

4. Proof of Conjecture 4: The unramified case

In this section, we will show that Lubin's fourth conjecture is true when $u(x)$ is a power series over the ring of integers of an unramified extension of $\mathbb{Q}_p$.

Let K be an unramified extension of $\mathbb{Q}_p$ and let $\mathcal{A}$ be the residue ring $\mathcal{O}/\mathcal{M}^2$. Let $\tilde{u}(x)$ and $\tilde{f}(x)$ be the corresponding series of $u(x)$ and $f(x)$ over the residue ring $\mathcal{A}$, respectively.

We begin with some necessary notation:

- Let i_n and j_n be the lowest degree of the terms of $u^{\circ p^n}(x) - x$ with coefficient in $\mathcal{O}^*$ and $\mathcal{M} \setminus \mathcal{M}^2$, respectively.
- Let S_0 be the set of degrees of terms of $f(x)$ whose coefficients are in $\mathcal{O}^*$ and let S_1 be the set of degrees of terms of $f(x)$ whose coefficients are in $\mathcal{M} \setminus \mathcal{M}^2$. Thus, writing $f(x) = \sum_{i=1}^{\infty} a_i x^i$, then $i \in S_0$ if $v(a_i) = 0$ and $i \in S_1$ if $v(a_i) = 1$.
- Given a positive integer n, we denote $o(n)$ the highest exponent of the power of p dividing n, *i.e.* $n = tp^{o(n)}$ where $p \nmid t$.
- Let s_0 be the smallest number in S_0 with $o(s_0) = \inf\{o(s) \mid s \in S_0\}$ and let s_1 be the smallest number in S_1 with $o(s_1) = \inf\{o(s) \mid s \in S_1\}$ or let $s_1 = \infty$ if S_1 is empty.

We remark that Lubin's main theorem in [7] says that wideg$(f(x)) = s_0 = p^{o(s_0)}$.

Lemma 4.1. *If $v(u'(0)-1) \geq 2$, then $j_n = i_{n-1}$ and $j_n < i_n$, for all $n \geq 1$. If $v(u'(0)-1) = 1$, then $j_n = i_{n-1}$ and $j_n < i_n$, for all $n \geq 2$.*

Proof. Suppose $u'(0) - 1 \in \mathcal{M}^2$. Then we can write $u(x) \equiv x + pg(x) + bx^i \pmod{\mathcal{M}^2, x^{i+1}}$, where $i = $ wideg$(u(x)-x)$, $b \in \mathcal{O}^*$ and $g(x) \in \mathcal{O}[x]$ with lowest degree at least 2. By a simple calculation, we have that $u^{\circ 2}(x) \equiv x + 2pg(x) + 2bx^i \pmod{\mathcal{M}^2, x^{i+1}}$. By induction, $u^{\circ p}(x) \equiv x + pbx^i \pmod{\mathcal{M}^2, x^{i+1}}$. Hence, $j_n = i_{n-1}$ and $j_n < i_n$ for all $n \geq 1$. If $v(u'(0)-1) = 1$, because $(u^{\circ p})'(0) - 1 = u'(0)^p - 1 \in \mathcal{M}^2$, we have that $j_n = i_{n-1}$ and $j_n < i_n$ for all $n \geq 2$. □

Lemma 4.2. *If $v(u'(0)-1) \geq 2$, then the lowest degree of $\tilde{u}^{\circ p^n} \circ \tilde{f} - \tilde{f}$ is $p^{o(s_0)} j_n$, for all $n \geq 1$. If $v(u'(0)-1) = 1$, then the lowest degree of $\tilde{u}^{\circ p^n} \circ \tilde{f} - \tilde{f}$ is $p^{o(s_0)} j_n$, for all $n \geq 2$.*

Proof. Consider $(p\,h(x) + cx^t)^r$ where $h(x) \in \mathcal{O}[[x]]$, $h(0) = 0$, $c \in \mathcal{O}^*$ and $t \geq 2$. The lowest degree of $(p\,h(x) + cx^t)^r \bmod \mathcal{M}$ is tr and the lowest degree of $(p\,h(x) + cx^t)^r \bmod \mathcal{M}^2$ is greater than $t(r-1)$. Therefore the term $b_j x^j$ of $u^{\circ p^n}(x) - x$ with $v(b_j) = 1$ contributes a power series of lowest degree $p^{o(s_0)} j$ in $\tilde{u}^{\circ p^n} \circ \tilde{f} - \tilde{f}$

and the term $b_i x^i$ of $u^{\circ p^n}(x) - x$ with $v(b_i) = 0$ contributes a power series of lowest degree greater than $p^{o(s_0)}(i-1)$ in $\tilde{u}^{\circ p^n} \circ \tilde{f} - \tilde{f}$. By the definitions of i_n and j_n and by Lemma 4.1, the lemma follows. $\square$

We remark that after taking iterates of $f(x)$, we can always suppose that $o(s_1) > 0$. In fact, suppose that $f(x) = \sum_{i=1}^{\infty} a_i x^i$. Consider $f \circ f$. If $v(a_i) = 1$, then every non-zero term of $a_i(\sum_{i'} a_{i'} x^{i'})^i \bmod \mathcal{M}^2$ is contributed by some $a_{i'} x^{i'}$ with $i' \in S_0$. Since $o(i') \geq o(s_0) > 0$ for every $i' \in S_0$, every non-zero term of $a_i(\sum_{i'} a_{i'} x^{i'})^i \bmod \mathcal{M}^2$ has degree m which satisfies $o(m) > 0$. If $v(a_i) = 0$, then every non-zero term of $a_i(\sum_{i'} a_{i'} x^{i'})^i \bmod \mathcal{M}^2$ is also contributed by some $a_{i'} x^{i'}$ with $i' \in S_0$. The terms $a_j x^j$ with $v(a_j) \geq 1$ cannot happen, because $o(i) \geq o(s_0) > 0$. Therefore, the degrees of terms of $f \circ f$ whose coefficients are in $\mathcal{M} \setminus \mathcal{M}^2$ are all divisible by p.

Lemma 4.3. *Suppose that $o(s_1) > 0$. Then for n large enough, the lowest degree of $\tilde{f} \circ \tilde{u}^{\circ p^n}(x) - \tilde{f}(x)$ is*

$$\begin{cases} s_0 + (i_n - 1)p^{o(s_0)-1} & \textit{if } o(s_1) > o(s_0) - 1 \textit{ or} \\ & \textit{if } o(s_1) = o(s_0) - 1 \textit{ and } s_1 > s_0, \\ s_1 + (i_n - 1)p^{o(s_1)} & \textit{otherwise.} \end{cases}$$

Proof. For $r > 0$, consider $(x + pg(x) + bx^i)^{tp^r}$ where $g(x) \in \mathcal{O}[[x]]$, $b \in \mathcal{O}^*$, $i > 1$ and $p \nmid t$. We have

$$(x + pg(x) + bx^i)^{tp^r} \equiv x^{tp^r} + tb^{p^r} x^{p^r(t-1)+ip^r} \text{ (mod } \mathcal{M}\text{, higher degree).}$$

Therefore, if $s \in S_1$, then the term $a_s x^s$ of $f(x)$ contributes a power series of lowest degree $s + (i_n - 1)p^{o(s)}$ in $\tilde{f} \circ \tilde{u}^{\circ p^n}(x) - \tilde{f}(x)$. Notice that for $s_1 \neq s \in S_1$, we always have $o(s) \geq o(s_1)$ and if $o(s) = o(s_1)$, then $s > s_1$. Because $i_n \to \infty$ as $n \to \infty$, if $o(s) > o(s_1)$, then $s + (i_n - 1)p^{o(s)} > s_1 + (i_n - 1)p^{o(s_1)}$ for n large enough. Therefore, the lowest degree of $\tilde{f} \circ \tilde{u}^{\circ p^n}(x) - \tilde{f}(x)$ contributed by all terms $a_s x^s$ of $f(x)$ with $s \in S_1$ is equal to $s_1 + (i_n - 1)p^{o(s_1)}$ when n is large enough.

For $s \in S_0$, because $s_0 = p^{o(s_0)}$ and $o(s_0) > 0$, we always have that $o(s) \geq o(s_0)$ and $s > s_0$. Therefore, for the lowest degree contributed by $a_s x^s$ with $s \in S_0$, we only have to consider for $r > 0$,

$$(x + pg(x) + bx^i)^{p^r} \equiv x^{p^r} + \binom{p^r}{p^{r-1}} b^{p^{r-1}} x^{p^{r-1}(p-1)+ip^{r-1}} \text{ (mod } \mathcal{M}^2\text{, higher degree).}$$

Notice that $\binom{p^r}{p^{r-1}} \equiv p \pmod{p^2}$. Hence, the lowest degree of $\tilde{f} \circ \tilde{u}^{\circ p^n}(x) - \tilde{f}(x)$ contributed by all terms $a_s x^s$ of $f(x)$ with $s \in S_0$ is equal to $s_0 + (i_n - 1)p^{o(s_0)-1}$.

Notice that for n large enough, $s_1 + (i_n - 1)p^{o(s_1)}$ equals $s_0 + (i_n - 1)p^{o(s_0)-1}$ only if $o(s_1) = o(s_0) - 1$. This implies $s_1 = s_0$, which is absurd. Therefore, the lowest degree of $\tilde{f} \circ \tilde{u}^{\circ p^n}(x) - \tilde{f}(x)$ is $\min\{s_0 + (i_n - 1)p^{o(s_0)-1}, s_1 + (i_n - 1)p^{o(s_1)}\}$, when n is large enough. Our lemma follows. $\square$

Lemma 4.4. *Suppose that $s_1 = p^{o(s_1)}$ and $0 < o(s_1) < o(s_0)$. Then the lowest degree of $\tilde{f} \circ \tilde{u}^{\circ p^n}(x) - \tilde{f}(x)$ is $p^{o(s_1)} i_n$, for all $n \geq 0$.*

Proof. Because $s_1 = p^{o(s_1)}$, by the definition of s_1, we always have $o(s) \geq s_1$ and $s > s_1$, for every $s \in S_1$ which is not equal to s_1. This implies that $s + (i_n - 1)p^{o(s)} > s_1 + (i_n - 1)p^{o(s_1)}$ for all n. Therefore, the lowest degree of $\tilde{f} \circ \tilde{u}^{\circ p^n}(x) - \tilde{f}(x)$ contributed by all terms $a_s x^s$ of $f(x)$ with $s \in S_1$ is equal to $s_1 + (i_n - 1)p^{o(s_1)}$, for all

n. From the proof of Lemma 4.3, we know that the lowest degree of $\tilde{f}\circ\tilde{u}^{\circ p^n}(x)-\tilde{f}(x)$ contributed by all terms $a_s x^s$ of $f(x)$ with $s \in S_0$ is equal to $s_0 + (i_n - 1)p^{o(s_0)-1}$, for all n. Because $o(s_1) \leq o(s_0) - 1$, we have that $s_1 = p^{o(s_1)} < p^{o(s_0)} = s_0$. This implies that $s_1 + (i_n - 1)p^{o(s_1)} < s_0 + (i_n - 1)p^{o(s_0)-1}$, for all n, and so the lowest degree of $\tilde{f} \circ \tilde{u}^{\circ p^n}(x) - \tilde{f}(x)$ equals $s_1 + (i_n - 1)p^{o(s_1)} = p^{o(s_1)} i_n$, for all n. □

Theorem 4.5. *Let K be an unramified extension of $\mathbb{Q}_p$ and let $\mathcal{O}$ be its integer ring with maximal ideal $\mathcal{M}$. Let $u(x)$ be an invertible stable series in $\mathcal{O}[[x]]$ with $u'(0) \equiv 1 \pmod{\mathcal{M}}$. Suppose that $u(x)$ commutes with a noninvertible stable series which has finite Weierstrass degree and has only simple roots of iterates. Then $\operatorname{wideg}(u^{\circ p^n}(x) - x)$ is a power of p for all $n \geq 0$.*

Proof. Without loss of generality, we assume that $f(x)$ with $o(s_1) > 0$ commutes with $u(x)$. Because $\tilde{u}^{\circ p^n} \circ \tilde{f} - \tilde{f} = \tilde{f} \circ \tilde{u}^{\circ p^n} - \tilde{f}$ for all n, by Lemma 4.2 and Lemma 4.3, we know that when n is large enough,

$$p^{o(s_0)} j_n = \begin{cases} s_0 + (i_n - 1)p^{o(s_0)-1} & \text{if } o(s_1) > o(s_0) - 1 \text{ or} \\ & \text{if } o(s_1) = o(s_0) - 1 \text{ and } s_1 > s_0, \\ s_1 + (i_n - 1)p^{o(s_1)} & \text{otherwise.} \end{cases}$$

Since $s_0 = \operatorname{wideg}(f(x)) = p^{o(s_0)}$ and both i_n and $j_n = i_{n-1}$ are powers of p when n is large enough, we must have $p^{o(s_0)} j_n = s_1 + (i_n - 1)p^{o(s_1)}$ and this implies that $o(s_1) \leq o(s_0) - 1$. This also implies that $s_1 = p^{o(s_1)}$, because j_n and i_n are powers of p for all n large enough and s_1 is independent of n.

Now, suppose that $u'(0) - 1 \in \mathcal{M}^2$. By Lemma 4.1, we have that $j_n = i_{n-1}$ and $j_n < i_n$ for all $n \geq 1$. Because $o(s_1) \leq o(s_0) - 1$ and $s_1 = p^{o(s_1)}$, by Lemma 4.2 and Lemma 4.4, we have that $p^{o(s_0)} i_{n-1} = p^{o(s_1)} i_n$ for all $n \geq 1$. Because i_n is a power of p for n large enough, this implies that i_n is a power of p for all $n \geq 0$.

For the case $v(u'(0) - 1) = 1$, the lowest degree of $\tilde{f} \circ \tilde{u} - \tilde{f}$ is $i_0 p^{o(s_1)}$ and the lowest degree of $\tilde{u} \circ \tilde{f} - \tilde{f}$ is $p^{o(s_0)}$. Hence, we have that i_0 is a power of p. Because $(u^{\circ p})'(0) - 1 = u'(0)^p - 1 \in \mathcal{M}^2$, by the argument above, we have that i_n is a power of p for $n \geq 1$. □

Remark 4.6. In the ramified case, by similar argument, we can show that i_n is a power of p for all $n \geq 0$, if $v(u'(0) - 1) \geq v(p) = 1$.

References

[1] K. Keating, Automorphisms and Extensions of $k((t))$, *J. Number Theory* 41 (1992), no.3, pp. 314–321. MR **93d:**13015

[2] H-C. Li, p-adic Periodic Points and Sen's Theorem, *J. Number Theory*, 56 (1996), no.2, pp. 309–318. MR **96m:**11102

[3] H-C. Li, Counting Periodic Points of p-adic Power Series, *Compositio Math.*, 100 (1996), pp. 351–364. MR **97c:**11109

[4] H-C. Li, p-adic Dynamical Systems and Formal Groups, *Compositio Math.*, 104 (1996), pp. 41–54. MR **98a:**11163

[5] H-C. Li, p-adic Power Series which Commute under Composition, *Trans. Amer. Math. Soc.*, 349 (1997), pp. 1437–1446. MR **97h:**11147

[6] J. Lubin & J. Tate, Formal Complex Multiplication in Local Field, *Ann. of Math.* (2) 81 (1965), pp. 380–387. MR **30:**3094

[7] J. Lubin, Nonarchimedean Dynamical Systems, *Compositio Math.* 94 (1994), pp. 321–346. MR **96g:**11140

[8] J. Lubin, personal communication.

[9] S. Sen, On Automorphisms of Local Fields, *Ann. of Math.* (2) 90 (1969), pp. 33–46. MR **39:**5531

[10] J.-P. Serre, Sur les groupes de Galois attachés aux groupes p-divisibles, *Proceedings of a Conference on Local Fields held at Driebergen*, Springer-Verlag, Berlin and New York, 1967. MR **39:**4166

Department of Mathematics, National Tsing Hua University, Hsin Chu, Taiwan, Republic of China

E-mail address: `li@math.nthu.edu.tw`

Current address: Department of Mathematics, National Taiwan Normal University, Taipei, Taiwan, Republic of China