COMPOSITIO MATHEMATICA

Optimal cycles in ultrametric dynamics and minimally ramified power series

Karl-Olof Lindahl and Juan Rivera-Letelier

Compositio Math. **152** (2016), 187–222.

doi:10.1112/S0010437X15007575

FOUNDATION
COMPOSITIO
MATHEMATICA

LONDON
MATHEMATICAL
SOCIETY
EST. 1865

https://doi.org/10.1112/S0010437X15007575 Published online by Cambridge University Press

Compositio Math. 152 (2016) 187–222
doi:10.1112/S0010437X15007575

Optimal cycles in ultrametric dynamics and minimally ramified power series

Karl-Olof Lindahl and Juan Rivera-Letelier

Abstract

We study ultrametric germs in one variable having an irrationally indifferent fixed point at the origin with a prescribed multiplier. We show that for many values of the multiplier, the cycles in the unit disk of the corresponding monic quadratic polynomial are 'optimal' in the following sense: they minimize the distance to the origin among cycles of the same minimal period of normalized germs having an irrationally indifferent fixed point at the origin with the same multiplier. We also give examples of multipliers for which the corresponding quadratic polynomial does not have optimal cycles. In those cases we exhibit a higher-degree polynomial such that all of its cycles are optimal. The proof of these results reveals a connection between the geometric location of periodic points of ultrametric power series and the lower ramification numbers of wildly ramified field automorphisms. We also give an extension of Sen's theorem on wildly ramified field automorphisms, and a characterization of minimally ramified power series in terms of the iterative residue.

1. Introduction

In proving the optimality of the Bruno condition for the local linearization of fixed points of holomorphic germs, Yoccoz showed the following dichotomy for quadratic polynomials of the form

$$P_\lambda(z) := \lambda z + z^2, \tag{1.1}$$

where the complex number λ satisfies $|\lambda| = 1$ and is not a root of unity: either P_λ is locally linearizable at $z = 0$, or every neighborhood of $z = 0$ contains a periodic cycle different than $z = 0$; see [Yoc95]. This last property is usually known as the *small cycles property*, and it is clearly an obstruction for local linearization. In fact, in the case where P_λ is not locally linearizable at $z = 0$, Yoccoz proved more: the distance of a small cycle of P_λ to $z = 0$ is essentially the smallest possible among cycles of the same minimal period of normalized holomorphic germs of the form

$$f(z) = \lambda z + \cdots ; \tag{1.2}$$

see [Yoc95, § 6.6].

In this paper we prove an analogous result over an arbitrary ultrametric field. When the residue characteristic of the ground field is odd and $0 < |\lambda - 1| < 1$, we show that every cycle

Received 9 November 2013, accepted in final form 16 May 2015, published online 7 September 2015.
2010 Mathematics Subject Classification 37P05, 11S15, 37F50 (primary).
Keywords: non-Archimedean dynamical systems, periodic points, rotation domains, ramification theory.
The first author's research was supported by the Swedish Research and Education in Mathematics Foundation SVeFUM and by MECESUP2 (PUC-0711) and DICYT (U. de Santiago de Chile). The second author's research was partially supported by FONDECYT grant 1100922, Chile.

of the quadratic polynomial (1.1) that is in the open unit disk and that has minimal period at least 2 is 'optimal' in the following sense: it minimizes the distance to $z = 0$ among cycles of the same minimal period of normalized germs of the form (1.2); see Theorem C in § 1.3 and the remarks that follow. When either the residue characteristic of the field is 2, or $|\lambda - 1| = 1$, the quadratic polynomial (1.1) does not necessarily have this property. In this case we find a higher-degree polynomial such that all of its cycles in the open unit disk are optimal; see Theorem A in § 1.3. A consequence of these results is that irrationally indifferent periodic points are isolated (Corollary 1.1 in § 2.3). This is new in positive characteristic (in characteristic zero it follows from the local linearization result of Herman and Yoccoz [HY83]).

The proof of these results reveals a connection between the geometric location of periodic points of ultrametric power series and the lower ramification numbers of wildly ramified field automorphisms, as studied by Sen [Sen69], Keating [Kea92], Laubie and Saïne [LS98], Wintenberger [Win04], and others. In fact, we show that for a generic power series of the form $f(z) = \lambda z + \cdots$, normalized so that it has integer coefficients, the existence of an optimal cycle is equivalent to the reduction of f having the least possible lower ramification numbers; see Theorem B in § 1.4. Such 'minimally ramified' power series were previously considered by Laubie *et al.* [LMS02] in their study of Lubin's conjecture [Lub94].

In proving our main results, we give an extension of the main theorem of Sen in [Sen69] (Theorem D in § 3.1), and give a characterization of minimally ramified power series in terms of the iterative residue, which is a conjugacy invariant introduced by Écalle in the complex setting (Theorem E in § 4).

We now proceed to describe our main results in more detail.

1.1 Periodic points of normalized power series

Let $(K, |\cdot|)$ be an ultrametric field and denote by $\mathcal{O}_K$ the ring of integers of K, by $\mathfrak{m}_K$ the maximal ideal of $\mathcal{O}_K$, and by $\widetilde{K} := \mathcal{O}_K/\mathfrak{m}_K$ the residue field of K.

Let λ in K be such that $|\lambda| = 1$, and let

$$f(z) = \lambda z + \cdots \tag{1.3}$$

be a power series in $K[[z]]$ converging on a neighborhood of $z = 0$. Through a scale change, we can assume that f has coefficients in $\mathcal{O}_K$. We say that a power series f as in (1.3) is *normalized* if it has coefficients in $\mathcal{O}_K$. When the ground field K is algebraically closed, the power f is normalized if and only if it converges and is univalent on the open unit disk $\mathfrak{m}_K$; see, for example, [Riv03, § 1.3]. So this normalization is the same as the one used in the complex setting by Yoccoz in [Yoc95]. In what follows we only consider normalized power series.

A normalized power series of the form (1.3) maps $\mathfrak{m}_K$ to itself isometrically; see, for example, [Riv03, § 1.3]. If either the residue characteristic of K is zero or the reduction $\widetilde{\lambda}$ of λ has infinite order in $\widetilde{K}^*$, then a normalized power series as in (1.3) has at most a finite number of periodic points; see Lemma 2.1. Thus, to simplify the exposition, in the rest of this introduction we assume that the residue characteristic p of K is positive and that the order q of $\widetilde{\lambda}$ in $\widetilde{K}^*$ is finite. Then q is not divisible by p, and the minimal period of each periodic point in $\mathfrak{m}_K \backslash \{0\}$ is of the form qp^n, for some integer $n \geqslant 0$; see Lemma 2.1.

1.2 Periodic points lower bound

The main theme of this paper is the optimality of the following lower bound.

Periodic points lower bound. Let p be a prime number, and $(K, |\cdot|)$ an ultrametric field of residue characteristic p. Moreover, let λ in K be such that $|\lambda| = 1$, and such that the order q of $\widetilde{\lambda}$ in $\widetilde{K}^*$

https://doi.org/10.1112/S0010437X15007575 Published online by Cambridge University Press

is finite. Then, for every power series

$$f(z) = \lambda z + \cdots \quad \text{in } \mathcal{O}_K[[z]]$$

and every integer $n \geqslant 1$ such that $\lambda^{qp^n} \neq 1$, the following property holds: for every periodic point z_0 of f of minimal period qp^n,

$$|z_0| \geqslant \left| \frac{\lambda^{qp^n} - 1}{\lambda^{qp^{n-1}} - 1} \right|^{1/qp^n}. \tag{1.4}$$

See Lemma 2.3 for a more detailed statement, which includes a lower bound for periodic points of minimal period q.

Although the statement of the periodic points lower bound is new, similar estimates were shown in [EEW04a, EEW04b] in the case where K is of characteristic zero. The idea of the proof can be traced back, at least, to Cremer's example of a complex polynomial having an irrationally indifferent fixed point that is not locally linearizable; see, for example, [Mil06, § 11]. It boils down to the observation that the product of the norms of all the fixed points of f^{qp^n} in $\mathfrak{m}_K \setminus \{0\}$ is equal to $|\lambda^{qp^n} - 1|$.

Suppose that the characteristic of K is equal to p and that $\lambda^q \neq 1$. Then the lower bound in (1.4) is equal to $|\lambda^q - 1|^{(p-1)/qp}$, which is independent of n. Thus, the following corollary is a direct consequence of the periodic points lower bound.

Corollary 1.1. *Every irrationally indifferent periodic point is isolated in positive characteristic.*

Combined with the fact that the quadratic polynomial $\lambda z + z^2$ in $K[z]$ is not locally linearizable at $z = 0$ when p is odd and $|\lambda - 1| < 1$ (see [Lin04, Theorem 2.3]),[1] the corollary above shows that in odd characteristic the existence of small cycles is not an obstruction to local linearization[2] (see [Lin13, Corollary C] for a somewhat analogous phenomenon in the p-adic setting). This is in contrast to the complex field case: Yoccoz showed that if λ in $\mathbb{C}^*$ is not a root of unity and the quadratic polynomial $\lambda z + z^2$ in $\mathbb{C}[z]$ is not locally linearizable at $z = 0$, then every neighborhood of $z = 0$ contains a periodic cycle; see [Yoc95, § 6.6].

In view of Corollary 1.1, we propose the following conjecture.

Conjecture 1.2. *In positive characteristic, every periodic point whose multiplier is a root of unity is either isolated as a periodic point, or has a neighborhood on which an iterate of the map is the identity.*

In [LR15] we solve this conjecture in the affirmative, in the case of generic parabolic points. For an ultrametric ground field of characteristic zero, the assertion of the conjecture does hold: when the residue characteristic is zero it follows from Lemma 2.1, and when the residue characteristic is positive it follows from the fact that periodic points are the zeros of the iterative logarithm; see [Riv03, Proposition 3.6] and also [Lub94] for the case where K is discretely valued.

Suppose now that K is of characteristic zero and that λ is not a root of unity. Then a direct computation shows that the lower bound in (1.4) converges to 1 as $n \to +\infty$. So, the

[1] According to Herman's conjecture [Her87, Conjecture 2], in positive characteristic a typical indifferent periodic point is not locally linearizable; yet, it is isolated as a periodic point by Corollary 1.1. Pérez-Marco showed that in the complex setting there are maps with similar properties; see [Pér97, Theorem I.3.1].

[2] In a field of characteristic 2, the quadratic polynomial $\lambda z + z^2$ is locally linearizable at $z = 0$ when $|\lambda - 1| < 1$; see [Lin04, Theorem 2.3]. We can consider instead the polynomial $\lambda z + z^3$, which is not locally linearizable at $z = 0$ when $|\lambda - 1| < 1$; see [Lin10, Theorem 1.1]. Thus, Corollary 1.1 also proves that in characteristic 2 the existence of small cycles is not an obstruction to local linearization.

https://doi.org/10.1112/S0010437X15007575 Published online by Cambridge University Press

periodic points lower bound implies that for every r in $(0,1)$ the number of periodic points of f in $\{z \in K : |z| \leqslant r\}$ is finite.[3] In fact, the periodic points lower bound gives a quantitative estimate of the speed at which periodic points separate from $z=0$ as the period increases: just observe that there is $n_0 \geqslant 1$ that only depends on λ^q, such that for every integer $n \geqslant n_0$,

$$\left| \frac{\lambda^{qp^n} - 1}{\lambda^{qp^{n-1}} - 1} \right| = |p|;$$

see also [EEW04a, Remark 3.6] and [EEW04b, Theorem 1].

1.3 Optimal cycles

Let p, K, λ, and q be as in the periodic points lower bound. Then we say that a power series $f(z) = \lambda z + \cdots$ in $\mathcal{O}_K[[z]]$ *has an optimal cycle of period* qp^n, if f has a periodic point z_0 of minimal period qp^n such that (1.4) holds with equality. If f has an optimal cycle of period qp^n, then this is in fact the only cycle of minimal period qp^n of f; see Theorem B below.

Theorem A. *Let p be a prime number, and $(K, |\cdot|)$ an algebraically closed ultrametric field of residue characteristic p. Moreover, let λ in K be such that $|\lambda| = 1$, such that the order q of $\widetilde{\lambda}$ in $\widetilde{K}^*$ is finite, and such that $\lambda^q \neq 1$. If K is of characteristic zero, assume in addition that λ is transcendental over the prime field of K. Then there is a polynomial $P(z) = \lambda z + \cdots$ in $\mathcal{O}_K[z]$ of degree at most $2q+1$, having for each integer $n \geqslant 1$ an optimal cycle of period qp^n.*

We use some explicit polynomials to prove this theorem; see Propositions 5.3 and 5.6 in § 5.2 for details. For example, in the case where p is odd and $q=1$, we prove that the polynomial $\lambda z + z^2$ satisfies the conclusions of Theorem A, in agreement with the situation in the complex setting; see [Yoc95, § 6.6]. However, not every quadratic polynomial has this property: if $p = 11$ and $\widetilde{\lambda} = -1$, then there is no integer $n \geqslant 1$ for which the quadratic polynomial $\lambda z + z^2$ has an optimal cycle of period $2p^n$; see § 1.5.

Suppose that K is of characteristic p, and let P be a polynomial satisfying the conclusions of Theorem A. Then all the periodic points of P of minimal period at least qp are in fact concentrated in the sphere[4]

$$\{z \in K : |z| = |\lambda^q - 1|^{(p-1)/qp}\}.$$

It is not clear to us how the periodic points are distributed in this sphere. For concreteness, we propose the following problem.

Problem 1.3. Let p be an odd prime number, $(K, |\cdot|)$ an algebraically closed and complete ultrametric field of characteristic p, and λ in K such that $0 < |\lambda - 1| < 1$. Moreover, for each integer $n \geqslant 1$ let Π_n be the set of cardinality p^n of all periodic points of $P_\lambda(z) = \lambda z + z^2$ in $\mathfrak{m}_K$ of minimal period p^n. Is the sequence of measures

$$\left\{ \frac{1}{p^n} \sum_{z \in \Pi_n} \delta_z \right\}_{n=1}^{+\infty}$$

convergent?

[3] This also follows from the fact that the periodic points of f are the zeros of the iterative logarithm of f, which is given by an analytic power series that converges on $\mathfrak{m}_K$; see [Riv03, Proposition 3.16] and also [Lub94] for the case where K is discretely valued.

[4] As pointed out in § 1.2, such a concentration of periodic points cannot occur in the case where the characteristic of K is zero.

https://doi.org/10.1112/S0010437X15007575 Published online by Cambridge University Press

It would be natural to consider the measures above as measures on the Berkovich projective line of K, since they would accumulate on at least one measure with respect to the corresponding weak* topology; see [Ber90]. Furthermore, every accumulation measure would be invariant by the action of P_λ on the Berkovich projective line of K.

1.4 Minimally ramified power series

One of the main ingredients in the proof of Theorem A is (an extension of) the concept of 'minimally ramified' power series introduced by Laubie *et al.* [LMS02] in their study of Lubin's conjecture in [Lub94]. To introduce this concept, let p be a prime number, and k a field of characteristic p. Denote by $\operatorname{ord}(\cdot)$ the valuation on $k[[\zeta]]$ defined for a non-zero power series as the lowest degree of its non-zero terms, and for the zero power series 0 by $\operatorname{ord}(0) = +\infty$. For a power series of the form $g(\zeta) = \zeta + \cdots$ in $k[[\zeta]]$, define for each integer $n \geqslant 0$ the number

$$i_n(g) := \operatorname{ord}\left(\frac{g^{p^n}(\zeta) - \zeta}{\zeta}\right).$$

As observed in [LMS02], the results of Sen in [Sen69] imply that for every integer $n \geqslant 0$ we have $i_n(g) \geqslant (p^{n+1} - 1)/(p - 1)$; following [LMS02], the power series g is called *minimally ramified* if the equality holds for every n.[5]

To prove Theorem A, we need to deal with a more general class of power series, allowing $g'(0)$ to be an arbitrary root of unity. For this, we prove a higher-order version of the main theorem of Sen in [Sen69]; see Theorem D in § 3.1. We use it to show that for every integer $q \geqslant 1$ not divisible by p, every root of unity γ in k of order q, and every power series of the form

$$g(\zeta) = \gamma\zeta + \cdots \text{ in } k[[\zeta]],$$

we have, for every integer $n \geqslant 0$,

$$i_n(g^q) \geqslant q\frac{p^{n+1} - 1}{p - 1}; \tag{1.5}$$

see Proposition 3.2 in § 3.2. We say that g is *minimally ramified* if equality holds for every n; see Definition 3.2. We give a characterization of minimally ramified power series in terms of the iterative residue; see Theorem E in § 4.

The following theorem links the existence of optimal cycles to minimally ramified maps. To simplify the exposition we have restricted to ground fields of odd residue characteristic. An analogous statement holds for ground fields of residue characteristic 2; see Theorem B′ in § 5.1.

Theorem B. *Let p be an odd prime number, $(K, |\cdot|)$ an algebraically closed field of residue characteristic p, and $q \geqslant 1$ an integer that is not divisible by p. Then the following properties hold.*

(1) *Let λ in K be such that $|\lambda| = 1$ and such that the order of $\widetilde{\lambda}$ in $\widetilde{K}^*$ is q. Moreover, let $n \geqslant 1$ be an integer and $P(z) = \lambda z + \cdots$ a polynomial in $\mathcal{O}_K[z]$ having an optimal cycle of period qp^n. Then this is the only cycle of minimal period qp^n of P, and the reduction of P is minimally ramified.*

[5] We note that in the case $p = 2$, a minimally ramified power series in the sense of [LMS02] is what we call here an 'almost minimally ramified' power series; see § 3.3 for more details.

https://doi.org/10.1112/S0010437X15007575 Published online by Cambridge University Press

(2) *Let γ be a root of unity in $\widetilde{K}$ of order q, and $g(\zeta) = \gamma\zeta + \cdots$ a polynomial in $\widetilde{K}[\zeta]$ that is minimally ramified. Given an integer $d \geqslant \max\{\deg(g), p\}$, let $a_1, \ldots, a_d$ in $\mathcal{O}_K$ be algebraically independent over the prime field of K, and such that the reduction of the polynomial $P(z) := a_1 z + \cdots + a_d z^d$ is g. Then for every integer $n \geqslant 1$, the polynomial P has a unique cycle of minimal period qp^n, and this cycle is an optimal cycle of period qp^n of P.*

See Proposition 5.1 for a related result that holds under a weaker form of the genericity condition in part (2). This genericity condition is necessary to prevent the concentration of periodic points, as occurs, for example, for the polynomials studied in the Appendix.

1.5 Optimal cycles of quadratic polynomials

The following is a more precise version of Theorem B for quadratic polynomials.

Theorem C. *Let p be an odd prime number, and $(K, |\cdot|)$ an algebraically closed ultrametric field of residue characteristic p. Moreover, let λ in K be such that $|\lambda| = 1$, such that the order q of $\widetilde{\lambda}$ in $\widetilde{K}^*$ is finite, and such that $\lambda^q \neq 1$. If K is of characteristic zero, assume in addition that λ is transcendental over the prime field of K. Then the following dichotomy holds for the polynomial $P_\lambda(z) := \lambda z + z^2$.*

(1) *If the reduction of P_λ is minimally ramified, then for each integer $n \geqslant 1$ the polynomial P_λ has a unique cycle of minimal period qp^n, and this cycle is an optimal cycle of period qp^n of P_λ.*

(2) *If the reduction of P_λ is not minimally ramified, then there is no integer $n \geqslant 1$ for which the polynomial P_λ has an optimal cycle of period qp^n.*

The first alternative of the theorem always holds when $q = 1$, because the polynomial $\zeta + \zeta^2$ in $\widetilde{K}[\zeta]$ is minimally ramified; see [Riv03, *Exemple* 3.19] or Proposition 4.4 in § 4.2. For an example where the second alternative holds, suppose that $p = 11$ and consider the quadratic polynomial

$$g_0(\zeta) := -\zeta + \zeta^2 \text{ in } \widetilde{K}[\zeta];$$

a direct computation shows that $i_0(g_0^2) = 2$ and $i_1(g_0^2) > 24$, so g_0 is not minimally ramified. So, when $p = 11$ and $\widetilde{\lambda} = -1$, the second alternative of Theorem C holds.

Problem 1.4. Let p be an odd prime number, $\mathbb{F}_p$ a field of p elements, and $\overline{\mathbb{F}}_p$ an algebraic closure of $\mathbb{F}_p$. Determine all those γ in $\overline{\mathbb{F}}_p^*$ for which the quadratic polynomial $\gamma\zeta + \zeta^2$ in $\overline{\mathbb{F}}_p[\zeta]$ is minimally ramified.

To prove that for γ in $\overline{\mathbb{F}}_p^*$ the polynomial $\gamma\zeta + \zeta^2$ is minimally ramified, it is enough to show that (1.5) holds with equality with $g(\zeta) = \gamma\zeta + \zeta^2$ and $n = 1$; see Proposition 3.2 in § 3.2.

We note that for γ in $\overline{\mathbb{F}}_p$, the property of $\gamma\zeta + \zeta^2$ being minimally ramified does not depend on the order of γ alone. For example, when $p = 7$, the orders of 2 and 4 in $\overline{\mathbb{F}}_7^*$ are both equal to 3, but $2\zeta + \zeta^2$ is not minimally ramified, and $4\zeta + \zeta^2$ is.

1.6 Organization

In § 2 we give general properties of normalized power series. After some preliminaries in § 2.1, in § 2.2 we describe the minimal periods of cycles of a normalized power series (Lemma 2.1). In § 2.3 we prove a more general version of the periodic points lower bound (Lemma 2.3).

In § 3 we introduce and study minimally ramified power series. We start by proving a higher-order version of Sen's theorem in § 3.1. In § 3.2 we use this result to define and characterize minimally ramified power series. In § 3.3 we study a variant of this concept for fields of

https://doi.org/10.1112/S0010437X15007575 Published online by Cambridge University Press

characteristic 2. In our characterization of minimally ramified power series we use an extension of Laubie and Saïne [LS98] of a result of Keating [Kea92].

In § 4 we characterize, for each integer q not divisible by p and each root of unity γ of order q, those power series of the form $g(\zeta) = \gamma\zeta + \cdots$ that are minimally ramified in terms of the iterative residue of g (Theorem E). A direct consequence is that there is a minimally ramified polynomial g as above of degree $q + 1$ or $2q + 1$.

In § 5 we prove Theorems A–C. In § 5.1 we prove a general version of Theorem B which we state as Theorem B′. In § 5.2 we exhibit concrete polynomials that satisfy the conclusions of Theorem A (see Propositions 5.3 and 5.6). In the Appendix we study a concentration of periodic points phenomenon showing that a very natural candidate to have optimal cycles in characteristic 2 has none. The proof of Theorem C is given at the end of § 5.2.

2. Periodic points lower bound

The purpose of this section is to prove general facts about periodic points of normalized power series. After some preliminaries in § 2.1, in § 2.2 we describe the minimal periods of periodic points of normalized power series. In § 2.3 we prove a general version of the periodic points lower bound, stated in § 1.2, which we state as Lemma 2.3.

2.1 Preliminaries

Given a ring R and an element a of R, we denote by $\langle a \rangle$ the ideal of R generated by a.

Given a field k, denote by $k^* := k\backslash\{0\}$ the multiplicative subgroup of k. A non-zero element γ of k^* has *infinite order in* k^*, if for every integer $q \geqslant 1$ we have $\gamma^q \neq 1$. If γ is not of infinite order in k^*, then the *order of* γ in k^* is the least integer $q \geqslant 1$ such that $\gamma^q = 1$. When k is of positive characteristic, in this last case the order γ is not divisible by the characteristic of k.

Let p be a prime number, and k a field of characteristic p. The *order* of a non-zero power series $g(\zeta)$ in $k[[\zeta]]$ is the lowest degree of a non-zero term in $g(\zeta)$. The order of the zero power series in $k[[\zeta]]$ is $+\infty$. For $g(\zeta)$ in $k[[\zeta]]$, denote by $\operatorname{ord}(g)$ the order of g. The function ord so defined is a valuation on $k[[\zeta]]$.

Let $(K, |\cdot|)$ be an ultrametric field. Denote by $\mathcal{O}_K$ the ring of integers of K, by $\mathfrak{m}_K$ the maximal ideal of $\mathcal{O}_K$, and by $\widetilde{K} := \mathcal{O}_K/\mathfrak{m}_K$ the residue field of K. Moreover, denote the projection in $\widetilde{K}$ of an element a of $\mathcal{O}_K$ by $\widetilde{a}$; it is the *reduction of* a. The *reduction* of a power series $f(z)$ in $\mathcal{O}_K[[z]]$ is the power series in $\widetilde{K}[[\zeta]]$ whose coefficients are the reductions of the corresponding coefficients of f.

For such a power series $f(z)$ in $\mathcal{O}_K[[z]]$, the *Weierstrass degree* $\operatorname{wideg}(f)$ *of* f is the order in $\widetilde{K}[[\zeta]]$ of the reduction $\widetilde{f}(\zeta)$ of $f(z)$. When K is algebraically closed and $\operatorname{wideg}(f)$ is finite, $\operatorname{wideg}(f)$ is equal to the number of zeros of f in $\mathfrak{m}_K$, counted with multiplicity; see for example [Lan02, § VI, Theorem 9.2].

Notice that a power series $f(z)$ in $\mathcal{O}_K[[z]]$ converges in $\mathfrak{m}_K$. If in addition $|f(0)| < 1$, then by the ultrametric inequality f maps $\mathfrak{m}_K$ to itself. In this case, a point z_0 in $\mathfrak{m}_K$ is *periodic for* f, if there is an integer $n \geqslant 1$ such that $f^n(z_0) = z_0$. In this case z_0 *is of period* n, and n is a *period of* z_0. If in addition n is the least integer with this property, then n is the *minimal period of* z_0 and $(f^n)'(z_0)$ is the *multiplier of* z_0. Note that an integer $n \geqslant 1$ is a period of z_0 if and only if it is divisible by the minimal period of z_0. Given a periodic point z_0 of f of multiplier λ, we say that z_0 is *attracting* if $|\lambda| < 1$, *indifferent* if $|\lambda| = 1$, and *repelling* if $|\lambda| > 1$. In the case where z_0 is indifferent, z_0 is *rationally indifferent* or *parabolic* if λ is a root of unity, and it is *irrationally indifferent* otherwise.

https://doi.org/10.1112/S0010437X15007575 Published online by Cambridge University Press

2.2 Minimal periods of normalized power series

The purpose of this section is to prove the following lemma, where we gather well-known results on periodic points of a normalized power series.

Lemma 2.1. *Let $(K, |\cdot|)$ be an ultrametric field and λ in K such that $|\lambda| = 1$. Then for every power series $f(z) = \lambda z + \cdots$ in $\mathcal{O}_K[[z]]$, the following properties hold.*

(1) *If $r \geqslant 1$ is an integer such that $|\lambda^r - 1| = 1$, then f has no periodic point of period r, other than $z = 0$. In particular, if $\widetilde{\lambda}$ has infinite order in $\widetilde{K}^*$, then f has no periodic point other than $z = 0$.*

(2) *Suppose that the order q of $\widetilde{\lambda}$ in $\widetilde{K}^*$ is finite.*

(a) *If the residue characteristic of K is zero, then the minimal period of each periodic point of f in $\mathfrak{m}_K \setminus \{0\}$ is equal to q.*

(b) *If the residue characteristic p of K is positive, then p does not divide q and the minimal period of each periodic point of f in $\mathfrak{m}_K \setminus \{0\}$ is of the form qp^n, for some integer $n \geqslant 0$.*

Before proving this lemma, we state and prove the following result.

Lemma 2.2. *Let $(K, |\cdot|)$ be a complete ultrametric field and $g(z)$ a power series in $\mathcal{O}_K[[z]]$ such that $|g(0)| < 1$. Then for each integer $m \geqslant 1$ the power series $g(z) - z$ divides $g^m(z) - z$ in $\mathcal{O}_K[[z]]$.*

Proof. We proceed by induction on m, the case $m = 1$ being trivial. Let $m \geqslant 1$ be an integer for which the lemma holds. Note that it is enough to show that $g(z) - z$ divides $g^{m+1}(z) - g^m(z)$ in $\mathcal{O}_K[[z]]$. Writing $g^m(z) = \sum_{n=0}^{+\infty} a_n z^n$ and using $|g(0)| < 1$, we have that $\sum_{n=0}^{+\infty} a_n (g(z)^n - z^n)$ converges to a power series in $\mathcal{O}_K[[z]]$ and that

$$\sum_{n=0}^{+\infty} a_n (g(z)^n - z^n) = g^{m+1}(z) - g^m(z). \tag{2.1}$$

On the other hand, again using $|g(0)| < 1$, we have that the series

$$\sum_{n=0}^{+\infty} a_n \sum_{j=0}^{n-1} z^j g(z)^{n-1-j}$$

converges to a power series $h(z)$ in $\mathcal{O}_K[[z]]$, and that $h(z)(g(z) - z)$ is equal to (2.1). This completes the proof of the lemma. □

Proof of Lemma 2.1. To prove part (1), let $r \geqslant 1$ be an integer such that $|\lambda^r - 1| = 1$, and note that the constant term of the power series $(f^r(z) - z)/z$ is equal to $\lambda^r - 1$. Thus, by the ultrametric inequality, for each z_0 in $\mathfrak{m}_K \setminus \{0\}$ we have

$$|f^r(z_0) - z_0| = |\lambda^r - 1| \cdot |z_0| = |z_0| \neq 0.$$

Thus $f^r(z_0) \neq z_0$ and therefore z_0 is not a periodic point of period r of f. This proves part (1).

To prove part (2), suppose first the residue characteristic p of K is positive. We prove first that q is not divisible by p. Suppose by contradiction that q is divisible by p, and put $m = q/p$. By the minimality of q we have $\widetilde{\lambda}^m \neq \widetilde{1}$. On the other hand, $(\widetilde{\lambda}^m)^p = \widetilde{\lambda}^q = \widetilde{1}$. Since the characteristic of $\widetilde{K}$ is equal to p, this implies that $\widetilde{\lambda}^m = \widetilde{1}$. This contradiction proves that q is not divisible by p.

https://doi.org/10.1112/S0010437X15007575 Published online by Cambridge University Press

To complete the proof of part (2), we prove simultaneously part (2)(a) and the second assertion of part (2)(b). To do this, let $\ell \geqslant 1$ be an integer and z_0 a periodic point of f in $\mathfrak{m}_K \setminus \{0\}$ of minimal period ℓ. By part (1) we must have $|\lambda^\ell - 1| < 1$, or equivalently $\widetilde{\lambda}^\ell = \widetilde{1}$. Thus q divides ℓ. If the residue characteristic of K is zero, put $q_0 := q$. If the residue characteristic p of K is positive, let $n \geqslant 0$ be the largest integer such that p^n divides ℓ and put $q_0 := qp^n$. In both cases we have that q_0 divides ℓ. To complete the proof of part (2), it is enough to prove that $\ell = q_0$. Suppose by contradiction that ℓ is not equal to q_0, so that $m := \ell / q_0 \geqslant 2$. Then, by Lemma 2.2 with $g = f^{q_0}$, the power series $f^{q_0}(z) - z$ divides $f^\ell(z) - z$ in $\mathcal{O}_K[[z]]$. Note that z_0 is a zero of the power series $(f^\ell(z) - z)/(f^{q_0}(z) - z)$. However, if $\lambda^{q_0} \neq 1$, then the constant term of this power series is equal to

$$\frac{\lambda^\ell - 1}{\lambda^{q_0} - 1} = 1 + \lambda^{q_0} + \cdots + \lambda^{(m-1)q_0},$$

whose norm equal to 1; so the power series $(f^\ell(z) - z)/(f^{q_0}(z) - z)$ does not have zeros in $\mathfrak{m}_K$. We thus obtain a contradiction that completes the proof of part (2) when $\lambda^q \neq 1$. It remains to consider the case where $\lambda^q = 1$. In this case the order of $f^{q_0}(z) - z$ in $K[[z]]$ is at least 2. If the order of this power series is infinite, then $f^{q_0}(z) = z$ and therefore every point of $\mathfrak{m}_K$ would be periodic of period q_0; but this is not possible because z_0 is periodic of minimal period ℓ, and by assumption $\ell > q_0$. This proves that the order t of the power series $f^{q_0}(z) - z$ is finite and at least 2. If we denote by a the coefficient of z^t in $f^{q_0}(z)$, then a straightforward induction argument shows that for every integer $s \geqslant 1$ we have

$$f^{sq_0}(z) = z + saz^t + \cdots .$$

When $s = m$, we obtain

$$f^\ell(z) = z + maz^t + \cdots .$$

This implies that the constant term of the power series $(f^\ell(z) - z)/(f^{q_0}(z) - z)$ is equal to m, which has norm 1. As before, this implies that this power series has no zeros in $\mathfrak{m}_K$, and we obtain a contradiction that completes the proof of the lemma. □

2.3 Periodic points lower bound

The purpose of this section is to give, for a normalized power series with an irrationally indifferent fixed point at $z = 0$, a lower bound for the norms of periodic points different from $z = 0$. The bound depends only on the multiplier of the fixed point $z = 0$, and on the minimal period of the periodic point.

Lemma 2.3. *Let p be a prime number, and $(K, |\cdot|)$ an ultrametric field of residue characteristic p. Let λ in K be such that $|\lambda| = 1$, and such that the order q of $\widetilde{\lambda}$ in $\widetilde{K}^*$ is finite. Then for every power series $f(z) = \lambda z + \cdots$ in $\mathcal{O}_K[[z]]$, the following properties hold.*

(1) *Suppose that $\lambda^q \neq 1$, and let w_0 be a periodic point of f of minimal period q. In the case $q = 1$, assume that $w_0 \neq 0$. Then*

$$|w_0| \geqslant |\lambda^q - 1|^{1/q}, \tag{2.2}$$

with equality if and only if $\operatorname{wideg}(f^q(z) - z) = q + 1$. *Moreover, if equality holds, then the cycle containing w_0 is the only cycle of minimal period q of f in $\mathfrak{m}_K \setminus \{0\}$, and for every point w_0' in this cycle the inequality above holds with equality with w_0 replaced by w_0'.*

https://doi.org/10.1112/S0010437X15007575 Published online by Cambridge University Press

(2) *Let $n \geqslant 1$ be an integer such that $\lambda^{qp^n} \neq 1$, and z_0 a periodic point of f of minimal period qp^n. Then*

$$|z_0| \geqslant \left| \frac{\lambda^{qp^n} - 1}{\lambda^{qp^{n-1}} - 1} \right|^{1/qp^n}, \tag{2.3}$$

with equality if and only if

$$\operatorname{wideg}\left(\frac{f^{qp^n}(z) - z}{f^{qp^{n-1}}(z) - z} \right) = qp^n. \tag{2.4}$$

Moreover, if equality holds, then the cycle containing z_0 is the only cycle of minimal period qp^n of f, and for every point z_0' in this cycle the inequality above holds with equality with z_0 replaced by z_0'.

Note that in (2.4) above we use the fact that $f^{qp^{n-1}}(z) - z$ divides $f^{qp^n}(z) - z$ in $\mathcal{O}_K[[z]]$, given by Lemma 2.2 with $g = f^{qp^{n-1}}$ and $m = p$.

Before proving this lemma, we state and prove the following result.

Lemma 2.4. *Let K be a complete ultrametric field and let $h(z)$ be a power series in $\mathcal{O}_K[[z]]$. If ξ is a zero of h in $\mathfrak{m}_K$, then $z - \xi$ divides $h(z)$ in $\mathcal{O}_K[[z]]$.*

Proof. Put $T(z) = z + \xi$ and note that $h \circ T(z)$ vanishes at $z = 0$ and is in $\mathcal{O}_K[[z]]$. This implies that z divides $h \circ T(z)$ in $\mathcal{O}_K[[z]]$. Letting $g(z) := h \circ T(z)/z$, it follows that the power series $g \circ T^{-1}(z) = h(z)/(z - \xi)$ is in $\mathcal{O}_K[[z]]$, as desired. □

Proof of Lemma 2.3. Replacing K by one of its completions if necessary, assume K complete.

We use the fact that, since $|f'(0)| = 1$, the power series f maps $\mathfrak{m}_K$ to itself isometrically; see, for example, [Riv03, § 1.3].

(1) To prove (2.2), let w_0 in $\mathfrak{m}_K \backslash \{0\}$ be a periodic point of f of minimal period q. Note that every point in the forward orbit $\mathcal{O}$ of w_0 under f is a zero of the power series $(f^q(z) - z)/z$, and that the constant term of this power series is $\lambda^q - 1$. On the other hand, $\mathcal{O}$ consists of q points, and, since f maps $\mathfrak{m}_K$ to itself isometrically, all the points in $\mathcal{O}$ have the same norm. Applying Lemma 2.4 inductively with ξ replaced by each element of $\mathcal{O}$, it follows that $\prod_{w_0' \in \mathcal{O}}(z - w_0')$ divides $(f^q(z) - z)/z$ in $\mathcal{O}_K[[z]]$. In particular, the constant term

$$\frac{\lambda^q - 1}{\prod_{w_0' \in \mathcal{O}}(-w_0')} \tag{2.5}$$

of the power series $((f^q(z) - z)/z)/\prod_{w_0' \in \mathcal{O}}(z - w_0')$ is in $\mathcal{O}_K$. We thus have

$$|w_0|^q = \prod_{w_0' \in \mathcal{O}} |w_0'| \geqslant |\lambda^q - 1|, \tag{2.6}$$

and therefore (2.2). Moreover, equality holds precisely when the constant term (2.5) of $((f^q(z) - z)/z)/\prod_{w_0' \in \mathcal{O}}(z - w_0')$ has norm equal to 1. Equivalently, equality in (2.6) holds if and only if $\operatorname{wideg}(f^q(z) - z) = q + 1$. Finally, when this last equality holds, the set $\mathcal{O}$ is the set of all zeros of $(f^q(z) - z)/z$ in $\mathfrak{m}_K$, so $\mathcal{O}$ is the only cycle of minimal period q of f. This completes the proof of part (1).

(2) To prove (2.3), let $n \geqslant 1$ be an integer such that $\lambda^{qp^n} \neq 1$, and z_0 a periodic point of f of minimal period qp^n. By Lemma 2.2 with $g = f^{qp^{n-1}}$ and $m = p$, the power series $f^{qp^{n-1}}(z) - z$

https://doi.org/10.1112/S0010437X15007575 Published online by Cambridge University Press

divides $f^{qp^n}(z) - z$ in $\mathcal{O}_K[[z]]$. Note that every point in the forward orbit $\mathcal{O}$ of z_0 under f is a zero of the power series

$$h(z) := \frac{f^{qp^n}(z) - z}{f^{qp^{n-1}}(z) - z},$$

and that the constant term of this power series is

$$\frac{\lambda^{qp^n} - 1}{\lambda^{qp^{n-1}} - 1}.$$

On the other hand, $\mathcal{O}$ consists of qp^n points, and, since f maps $\mathfrak{m}_K$ to itself isometrically, all the points in $\mathcal{O}$ have the same norm. Applying Lemma 2.4 inductively with ξ replaced by each element of $\mathcal{O}$, it follows that $\prod_{z_0' \in \mathcal{O}} (z - z_0')$ divides $h(z)$ in $\mathcal{O}_K[[z]]$. In particular, the constant term

$$\left(\frac{\lambda^{qp^n} - 1}{\lambda^{qp^{n-1}} - 1} \right) \Big/ \prod_{z_0' \in \mathcal{O}} (-z_0') \tag{2.7}$$

of the power series $h(z) / \prod_{z_0' \in \mathcal{O}} (z - z_0')$ is in $\mathcal{O}_K$. We thus have

$$|z_0|^{qp^n} = \prod_{z_0' \in \mathcal{O}} |z_0'| \geqslant \left| \frac{\lambda^{qp^n} - 1}{\lambda^{qp^{n-1}} - 1} \right|, \tag{2.8}$$

and therefore (2.3). Note that equality holds if and only if the constant term (2.7) of the power series $h(z) / \prod_{z_0' \in \mathcal{O}} (z - z_0')$ has norm equal to 1. Equivalently, equality holds if and only if $\operatorname{wideg}(h(z) / \prod_{z_0' \in \mathcal{O}} (z - z_0')) = 0$. Using

$$\operatorname{wideg}\left(\frac{h(z)}{\prod_{z_0' \in \mathcal{O}} (z - z_0')} \right) = \operatorname{wideg}\left(\frac{f^{qp^n}(z) - z}{f^{qp^{n-1}}(z) - z} \right) - qp^n,$$

we conclude that equality holds if and only if $\operatorname{wideg}((f^{qp^n}(z) - z)/(f^{qp^{n-1}}(z) - z)) = qp^n$. Finally, note that if this last equality holds, then $\mathcal{O}$ is the set of all zeros of $(f^{qp^n}(z) - z)/(f^{qp^{n-1}}(z) - z)$ in $\mathfrak{m}_K$, so $\mathcal{O}$ is the only cycle of minimal period qp^n of f. This completes the proof of part (2). □

3. Minimally ramified power series

Our main goal in this section is study condition (2.4) appearing in the optimality part of Lemma 2.3. To do this, for a given prime number p and a field k of characteristic p, define, for each power series $g_0(\zeta) = \zeta + \cdots$ in $k[[\zeta]]$ and each integer $n \geqslant 0$, the order

$$i_n(g_0) := \operatorname{ord}\left(\frac{g_0^{p^n}(\zeta) - \zeta}{\zeta} \right).$$

Note that if K, q, λ, and f are as in Lemma 2.3 and $k = \widetilde{K}$, then $\widetilde{\lambda}$ is a root of unity of order q in k, and for each integer $n \geqslant 1$ such that

$$\operatorname{wideg}(f^{qp^{n-1}}(z) - z) = i_{n-1}(\widetilde{f}^q) + 1$$

is finite, we have

$$\operatorname{wideg}\left(\frac{f^{qp^n}(\zeta) - \zeta}{f^{qp^{n-1}}(\zeta) - \zeta} \right) = i_n(\widetilde{f}^q) - i_{n-1}(\widetilde{f}^q).$$

https://doi.org/10.1112/S0010437X15007575 Published online by Cambridge University Press

Thus, (2.4) naturally leads us to consider, for a root of unity γ of order q in k and a power series $g(\zeta) = \gamma\zeta + \cdots$ in $k[[\zeta]]$, the sequence $\{i_n(g^q)\}_{n=0}^{+\infty}$. When p is odd, we show that for an integer $n \geqslant 1$ such that $i_{n-1}(g^q)$ is finite, the equality

$$i_n(g^q) - i_{n-1}(g^q) = qp^n \tag{3.1}$$

can only hold if g is 'minimally ramified', in the sense that the sequence $\{i_n(g^q)\}_{n=0}^{+\infty}$ is the smallest possible; see Corollary 3.10 in § 3.3, which also includes a characterization in the case $p = 2$. Thus, in the case where p is odd and $f(z) = \lambda z + \cdots$ is a polynomial in $\mathcal{O}_K[z]$ with non-linear reduction, the existence of an optimal cycle of period qp^n implies that $\widetilde{f}$ is minimally ramified; see Corollary 3.11.

The structure of this section is as follows. In § 3.1 we establish a 'higher-order' version of the main theorem of Sen in [Sen69]. In § 3.2 we combine this result with a result of Laubie and Saïne in [LS98], extending a previous result of Keating in [Kea92], to characterize minimally ramified power series. In § 3.3 introduce the notion of 'almost minimally ramified' power series, and we use it to handle the case $p = 2$.

3.1 A higher-order version of Sen's theorem

The purpose of this section is to prove the following theorem.

Theorem D. *Let p be a prime number, and k a field of characteristic p. Moreover, let γ be a root of unity in k, $q \geqslant 1$ the order of γ, and*

$$g(\zeta) = \gamma\zeta + a_2\zeta^2 + \cdots$$

a power series in $k[[\zeta]]$. Then $i_0(g^q)$ is divisible by q when finite. Furthermore, for every integer $n \geqslant 1$ such that $i_n(g^q)$ is finite, $i_{n-1}(g^q)$ is also finite and

$$i_n(g^q) \equiv i_{n-1}(g^q) \mod qp^n.$$

In particular, for every $n \geqslant 0$ such that $i_n(g^q)$ is finite, $i_n(g^q)$ is divisible by q.

When restricted to $q = 1$, the theorem above is [Sen69, Theorem 1]. Sen's original proof in [Sen69] is based on a careful analysis of the orders of cocycles of power series in $k[[\zeta]]$. Lubin gave a conceptual proof of this result in [Lub95] that is even shorter than Sen's original proof; Lubin interprets $i_n(g) - i_{n-1}(g)$ as the number of periodic points of minimal period p^n of a certain 'lift' of g. See also [Li96, Theorem 3.1] for a variant of Lubin's proof.

To prove Theorem D, we follow Lubin's strategy. The main difficulty is to find, for a given n, a lift g such that the zeros of $g^{qp^n}(z) - z$ are simple. Lubin achieved this through an inductive perturbative procedure. We use the fact that a generic polynomial has no parabolic periodic point.

Lemma 3.1. *Let K be a field of characteristic zero, $d \geqslant 2$ an integer, and $a_1, \ldots, a_d$ in K algebraically independent over the prime field of K. Then the polynomial*

$$a_1 z + \cdots + a_d z^d$$

in $K[z]$ has no parabolic periodic point.

https://doi.org/10.1112/S0010437X15007575 Published online by Cambridge University Press

Proof. Denote by $\mathbb{Q}$ the prime field of K, and by $|\cdot|$ the usual absolute value in $\mathbb{C}$.

Suppose by contradiction there is an integer $n \geqslant 1$ and a periodic point z_0 of period n of the polynomial $P(z) := a_1 z + \cdots + a_d z^d$ in $K[z]$, such that $(P^n)'(z_0)$ is a root of unity. Let $\sigma : \mathbb{Q}[z_0, a_1, \ldots, a_d] \to \mathbb{C}$ be a ring homomorphism such that $\sigma(a_d) = 1$, and such that for each j in $\{1, \ldots, d-1\}$ we have $\sigma(a_j) = 0$. Then $\sigma(P)(z) = z^d$, $\sigma(z_0)$ is a periodic point of period n of $\sigma(P)$, and $(\sigma(P)^n)'(\sigma(z_0)) = \sigma((P^n)'(z_0))$ is a root of unity. This implies that $\sigma(z_0) \neq 0$, and therefore that $|\sigma(z_0)| = 1$. Thus,

$$|(\sigma(P)^n)'(\sigma(z_0))| = |d^n \sigma(z_0)^{d^n - 1}| = d^n.$$

This contradicts our hypothesis that $\sigma((P^n)'(z_0))$ is a root of unity, and proves the lemma. □

Proof of Theorem D. Replacing k by one of its algebraic closures if necessary, assume that k is algebraically closed. Then k is perfect and therefore there is an algebraically closed field K of characteristic zero that is complete with respect to a non-trivial ultrametric norm and whose residue field $\widetilde{K}$ is isomorphic to k; see, for example, [Ser68, II, Théorème 3]. Identify k with $\widetilde{K}$. Then K is uncountable and therefore we can choose for each j in $\{1, \ldots, i_n(g^q)+1\}$ an element a_j of K, such that the $a_1, \ldots, a_{i_n(g^q)+1}$ are algebraically independent over the prime field of K and such that the reduction $\widetilde{P}$ of the polynomial

$$P(z) = a_1 z + \cdots + a_{i_n(g^q)+1} z^{i_n(g^q)+1}$$

in $K[z]$ satisfies $\widetilde{P}(\zeta) \equiv g(\zeta) \bmod \langle \zeta^{i_n(g^q)+2} \rangle$ in $k[\zeta]$. Then

$$\operatorname{wideg}(P^{qp^n}(z) - z) = i_n(g^q) + 1,$$

and by Lemma 3.1 the polynomial P has no parabolic periodic points.

Suppose that $n = 0$. From $a_1^q \neq 1$, it follows that $P^q(z) - z$ has precisely $i_0(g^q)$ zeros in $\mathfrak{m}_K \backslash \{0\}$, counted with multiplicity. Note that if $P^q(z) - z$ had a double zero of z_0 in $\mathfrak{m}_K \backslash \{0\}$, then z_0 would also be a zero of $(P^q)'(z) - 1$, and therefore z_0 would be a parabolic periodic point of P. We conclude that all zeros of $P^q(z) - z$ in $\mathfrak{m}_K \backslash \{0\}$ are simple, and therefore that $P^q(z) - z$ has precisely $i_0(g^q)$ zeros in $\mathfrak{m}_K \backslash \{0\}$. By part (2) of Lemma 2.1, every zero of $P^q(z) - z$ in $\mathfrak{m}_K \backslash \{0\}$ is a periodic point of minimal period q of P. Combined with $P(\mathfrak{m}_K) = \mathfrak{m}_K$, it follows that the set Z_0 of zeros of $P^q(z) - z$ in $\mathfrak{m}_K \backslash \{0\}$ is a union of periodic orbits of minimal period q. We conclude that $\# Z_0 = i_0(g^q)$ is divisible by q. This completes the proof of the theorem in the case $n = 0$.

Suppose that $n \geqslant 1$. Our assumption that $i_n(g^q)$ is finite, together with the straightforward inequality $i_{n-1}(g^q) \leqslant i_n(g^q)$, implies that $i_{n-1}(g^q)$ is also finite. So, by our choice of P, we have

$$\operatorname{wideg}(P^{qp^{n-1}}(z) - z) = i_{n-1}(g^q) + 1,$$

and therefore $h(z) := (P^{qp^n}(z) - z)/(P^{qp^{n-1}}(z) - z)$ has precisely $i_n(g^q) - i_{n-1}(g^q)$ zeros in $\mathfrak{m}_K$, counted with multiplicity. As in the previous case, if $P^{qp^n}(z) - z$ had a double zero z_0, then z_0 would also be a zero of $(P^{qp^n})'(z) - 1$, and therefore z_0 would be a parabolic periodic point of P. We conclude that all zeros of $P^{qp^n}(z) - z$, and hence of h, are simple. In particular, h has precisely $i_n(g^q) - i_{n-1}(g^q)$ zeros in $\mathfrak{m}_K$. It also follows that a zero of h cannot be a zero of $P^{qp^{n-1}}(z) - z$. In view of part (2) of Lemma 2.1, this implies that the zeros of h are precisely the periodic points of P of minimal period qp^n. Since $P(\mathfrak{m}_K) = \mathfrak{m}_K$, it follows that the set Z_n of zeros of h in $\mathfrak{m}_K$ is a union of periodic orbits of minimal period qp^n. We conclude that $\# Z_n = i_n(g^q) - i_{n-1}(g^q)$ is divisible by qp^n. This completes the proof of the theorem. □

https://doi.org/10.1112/S0010437X15007575 Published online by Cambridge University Press

3.2 Minimally ramified power series

In this section we introduce the notion of 'minimally ramified' power series, which is motivated by the following proposition.

Proposition 3.2. *Let p be a prime number, k a field of characteristic p, and γ a root of unity in k. If we denote by q the order of γ, then for every power series $g(\zeta) = \gamma\zeta + \cdots$ in $k[[\zeta]]$ and every integer $n \geqslant 0$, we have*

$$i_n(g^q) \geqslant q\frac{p^{n+1}-1}{p-1}. \tag{3.2}$$

If p is odd (respectively, $p = 2$) and equality holds for some $n \geqslant 1$ (respectively, $n \geqslant 2$), then equality holds for every $n \geqslant 0$.

Remark 3.3. In contrast with the case where p is odd, when $p = 2$ equality in (3.2) for $n = 1$ does not necessarily imply that we have equality in (3.2) for every $n \geqslant 0$. In fact, suppose that $p = 2$ and put $g(\zeta) := \gamma\zeta(1 + \zeta^q)$ if $q \equiv 1 \bmod 4$, and $g(\zeta) := \gamma\zeta(1 + \zeta^q + \zeta^{2q})$ if $q \equiv -1 \bmod 4$. Then a direct computation shows that $i_1(g^q) = 3q$ and $i_2(g^q) > 7q$.

The proof of Proposition 3.2 is at the end of this section.

Motivated by Proposition 3.2, and following the terminology introduced by Laubie *et al.* [LMS02] in the case $q = 1$, we make the following definition.

Definition 3.4. Let p be a prime number, k a field of characteristic p, γ a root of unity in k, and q the order of γ. Then a power series $g(\zeta) = \gamma\zeta + \cdots$ in $k[[\zeta]]$ is *minimally ramified* if, for every integer $n \geqslant 0$,

$$i_n(g^q) = q\frac{p^{n+1}-1}{p-1}.$$

To prove Proposition 3.2, we use several times the following consequence of [LS98, Corollary 1]; see also [Kea92, Theorem 7] for the case $q = 1$.

Lemma 3.5. *Let p be a prime number, k a field of characteristic p, γ a root of unity, and $g(\zeta) = \gamma\zeta + \cdots$ a power series in $k[[\zeta]]$. If p is odd (respectively, $p = 2$), then g is minimally ramified if and only if (3.2) holds with equality for $n = 0$ and $n = 1$ (respectively, $n = 0$, $n = 1$, and $n = 2$).*

We also use the following lemma several times; see also [Ser68, Exercice 3, § 4] or [Kea92, Lemma 3] for the case $q = 1$.

Lemma 3.6. *Let p be a prime number, k a field of characteristic p, γ a root of unity in k, and q the order of γ. Then for each power series*

$$g(\zeta) = \gamma\zeta + \cdots$$

in $k[[\zeta]]$ and every integer $n \geqslant 0$ such that $i_n(g^q)$ is finite, the following properties hold:

1. *if $i_n(g^q)$ is not divisible by p, then $i_{n+1}(g^q) \geqslant p i_n(g^q) + q$;*
2. *if $i_n(g^q)$ is divisible by p, then $i_{n+1}(g^q) = p i_n(g^q)$.*

Proof. For each integer $m \geqslant 1$ define the power series $\Delta_m(\zeta)$ inductively by $\Delta_1(\zeta) := g^{qp^n}(\zeta) - \zeta$, and for $m \geqslant 2$ by

$$\Delta_m(\zeta) := \Delta_{m-1}(g^{qp^n}(\zeta)) - \Delta_{m-1}(\zeta).$$

An induction argument shows that

$$\Delta_m(\zeta) = \sum_{j=0}^{m} \binom{m}{j} (-1)^{m-j} g^{qp^n j}(\zeta).$$

https://doi.org/10.1112/S0010437X15007575 Published online by Cambridge University Press

Taking $m = p$, we obtain $\Delta_p(\zeta) = g^{qp^{n+1}}(\zeta) - \zeta$. Noting that $i := \operatorname{ord}(\Delta_1)$ is equal to $i_n(g^q) + 1$, put

$$\Delta_1(\zeta) = \sum_{j=i}^{+\infty} a_j \zeta^j,$$

so that $a_i \neq 0$.

Given an integer $m \geqslant 1$, put

$$o := \operatorname{ord}(\Delta_m) \quad \text{and} \quad \Delta_m(\zeta) = \sum_{j=o}^{+\infty} b_j \zeta^j,$$

so that $b_o \neq 0$. Then we have

$$\begin{aligned}\Delta_{m+1}(\zeta) &= \sum_{j=o}^{+\infty} b_j((\zeta + \Delta_1(\zeta))^j - \zeta^j)\\ &= \sum_{j=o}^{+\infty} b_j(\zeta^j(1 + a_i\zeta^{i-1} + \cdots)^j - \zeta^j)\\ &\equiv b_o a_i o \zeta^{o+i-1} \mod \langle \zeta^{o+i} \rangle\end{aligned}$$

in $k[[\zeta]]$. It follows that

$$\operatorname{ord}(\Delta_{m+1}) \geqslant \operatorname{ord}(\Delta_m) + i_n(g^q), \tag{3.3}$$

with equality if and only if $\operatorname{ord}(\Delta_m)$ is not divisible by p. Since $\operatorname{ord}(\Delta_1) = i_n(g^q) + 1$, when $i_n(g^q)$ is divisible by p for every integer $m \geqslant 1$ we have $\operatorname{ord}(\Delta_m) = mi_n(g^q) + 1$. Taking $m = p$ and using $\operatorname{ord}(\Delta_p) = i_{n+1}(g^q) + 1$, we conclude that $i_{n+1}(g^q) = pi_n(g^q)$. This proves part (2). To prove part (1), suppose that $i_n(g^q)$ is not divisible by p and that $i_{n+1}(g^q)$ is finite. Let ℓ be the integer in $\{1, \ldots, p-1\}$ such that $\ell \cdot i_n(g^q) \equiv -1 \mod \langle p \rangle$. Applying (3.3) inductively, we obtain that for every m in $\{1, \ldots, \ell\}$ we have $\operatorname{ord}(\Delta_m) = mi_n(g^q) + 1$. Since $\ell \cdot i_n(g^q) + 1$ is divisible by p, by (3.3) with $m = \ell$ we have $\operatorname{ord}(\Delta_{\ell+1}) \geqslant (\ell+1)i_n(g^q) + 2$. In the case $\ell = p-1$ we obtain $\operatorname{ord}(\Delta_p) \geqslant pi_n(g^q) + 2$. If $\ell \neq p-1$, then using (3.3) inductively we also obtain $\operatorname{ord}(\Delta_p) \geqslant pi_n(g^q) + 2$. So this last inequality holds in all cases. Using $\operatorname{ord}(\Delta_p) = i_{n+1}(g^q) + 1$ and the fact that $i_{n+1}(g^q)$ and $i_n(g^q)$ are both divisible by q by Theorem D, we conclude that $i_{n+1}(g^q) \geqslant pi_n(g^q) + q$. This proves part (1) and completes the proof of the lemma. □

Proof of Proposition 3.2. To prove that we have (3.2) for every $n \geqslant 0$, we proceed by induction. The case $n = 0$ follows from the fact that $i_0(g^q)$ is divisible by q when finite; see Theorem D. Let $n \geqslant 0$ be an integer for which (3.2) holds, and suppose that $i_{n+1}(g^q)$, and hence $i_n(g^q)$, is finite. Using $i_{n+1}(g^q) \geqslant i_n(g^q) + 1$ (cf. Lemma 3.6) and that $i_{n+1}(g^q) - i_n(g^q)$ is divisible by qp^{n+1} (Theorem D), we have

$$i_{n+1}(g^q) \geqslant i_n(g^q) + qp^{n+1} \geqslant q\frac{p^{n+1}-1}{p-1} + qp^{n+1} = q\frac{p^{n+2}-1}{p-1}.$$

This completes the proof of the induction step, and that (3.2) holds for every $n \geqslant 0$.

To prove the last part of the proposition, suppose p is odd (respectively, $p = 2$) and that for some $n \geqslant 1$ (respectively, $n \geqslant 2$) we have $i_n(g^q) = q(p^{n+1} - 1)/(p-1)$. We prove by induction that for every ℓ in $\{0, \ldots, n\}$ we have $i_{n-\ell}(g^q) = q(p^{n-\ell+1} - 1)/(p-1)$. When $\ell = 0$ this holds by hypothesis. Suppose this holds for some ℓ in $\{0, \ldots, n-1\}$. In particular, $i_{n-\ell}(g^q)$ is not divisible

https://doi.org/10.1112/S0010437X15007575 Published online by Cambridge University Press

by p, and by part (2) of Lemma 3.6 the number $i_{n-\ell-1}(g^q)$ is not divisible by p either. Thus, by part (1) of the same lemma we have

$$pi_{n-\ell-1}(g^q) + q \leqslant i_{n-\ell}(g^q) = q\frac{p^{n-\ell+1}-1}{p-1},$$

and therefore $i_{n-\ell-1}(g^q) \leqslant q(p^{n-\ell}-1)/(p-1)$. Since we have already proved the reverse inequality, we obtain $i_{n-\ell-1}(g^q) = q(p^{n-\ell}-1)/(p-1)$. This completes the proof of the induction step, and of the fact that for every ℓ in $\{0,\dots,n\}$ we have $i_{n-\ell}(g^q) = q(p^{n-\ell+1}-1)/(p-1)$. Combined with Lemma 3.5, this implies the last part of the proposition. □

3.3 Almost minimally ramified power series

For a ground field of characteristic 2, in this section we study those power series that are 'almost minimally ramified' (Proposition 3.7 and Definition 3.8). We use this and the results in § 3.2 to characterize in arbitrary characteristic the occurrence of (3.1) in terms of (almost) minimally ramified power series (Corollary 3.10). In turn, this allows us to show that, in some cases, the existence of an optimal cycle implies that the reduction of the map is (almost) minimally ramified (Corollary 3.11).

Proposition 3.7. *Let k be a field of characteristic 2, γ a root of unity in k, q the order of γ, and $g(\zeta) = \gamma\zeta + \cdots$ a power series in $k[[\zeta]]$. Then the following properties hold:*

(1) *if g is not minimally ramified, then, for every integer $n \geqslant 2$,*

$$i_n(g^q) \geqslant 2^{n+1}q; \tag{3.4}$$

(2) *if equality holds in (3.4) for $n = 0$ or for some $n \geqslant 2$, then it holds for every $n \geqslant 0$.*

The proof of this proposition is at the end of this section.

Definition 3.8. Let k be a field of characteristic 2, γ a root of unity in k, and q the order of γ. Then a power series $g(\zeta) = \gamma\zeta + \cdots$ in $k[[\zeta]]$ is *almost minimally ramified* if, for every integer $n \geqslant 0$,

$$i_n(g^q) = 2^{n+1}q.$$

The following is a direct consequence of Proposition 3.7.

Corollary 3.9. *Let k be a field of characteristic 2, γ a root of unity in k, and q the order of γ. If $g(\zeta) = \gamma\zeta + \cdots$ is a power series in $k[[\zeta]]$ such that for some integer $n \geqslant 2$ we have $i_n(g^q) \leqslant 2^{n+1}q$, then g is either minimally ramified or almost minimally ramified.*

The following corollary is a consequence of Propositions 3.2 and 3.7.

Corollary 3.10. *Let p be a prime number, and k a field of characteristic p. Then for every root of unity γ in k of order q, and every power series $g(\zeta) = \gamma\zeta + \cdots$ in $k[[\zeta]]$, the following properties hold.*

(1) *Suppose that p is odd and that for some integer $n \geqslant 1$ such that $i_{n-1}(g^q)$ is finite, we have $i_n(g^q) - i_{n-1}(g^q) = qp^n$. Then g is minimally ramified.*

(2) *Suppose that $p = 2$ and that for some $n \geqslant 2$ such that $i_{n-1}(g^q)$ is finite, we have $i_n(g^q) - i_{n-1}(g^q) = 2^nq$. Then g is either minimally ramified, or almost minimally ramified.*

https://doi.org/10.1112/S0010437X15007575 Published online by Cambridge University Press

Proof. To prove part (1), suppose that p is odd and let $n \geqslant 1$ be such that $i_{n-1}(g^q)$ is finite and $i_n(g^q) = i_{n-1}(g^q) + qp^n$. Suppose by contradiction that $i_{n-1}(g^q)$ is divisible by p. Then by part (2) of Lemma 3.6 we have $i_n(g^q) = pi_{n-1}(g^q)$, so

$$qp^n = i_n(g^q) - i_{n-1}(g^q) = (p-1)i_{n-1}(g^q).$$

Since $i_{n-1}(g^q)$ is divisible by q (Theorem D), this implies that $p-1$ divides p^n. However, this is not possible because $p-1$ is even and p^n is odd. We conclude that $i_{n-1}(g^q)$ is not divisible by p. Then part (1) of Lemma 3.6 implies that $i_n(g^q) \geqslant pi_{n-1}(g^q) + q$, so

$$i_n(g^q) = i_{n-1}(g^q) + qp^n \leqslant (i_n(g^q) - q)/p + qp^n,$$

and $i_n(g^q) \leqslant q(p^{n+1}-1)/(p-1)$. Then Proposition 3.2 implies that g is minimally ramified. This proves part (1).

To prove part (2), suppose that $p = 2$ and let $n \geqslant 2$ be such that $i_{n-1}(g^q)$ is finite and $i_n(g^q) = i_{n-1}(g^q) + 2^n q$. By Lemma 3.6,

$$i_n(g^q) = i_{n-1}(g^q) + 2^n q \leqslant i_n(g^q)/2 + 2^n q.$$

We thus have $i_n(g^q) \leqslant 2^{n+1}q$, and by Corollary 3.9 the power series g is either minimally ramified or almost minimally ramified. □

Corollary 3.11. *Let p, K, λ, and q be as in Lemma 2.3 and let $n \geqslant 1$ be an integer and $P(z) = \lambda z + \cdots$ in $\mathcal{O}_K[z]$ a polynomial having an optimal cycle of period qp^n. Then the following properties hold:*

(1) *if p is odd, then $\widetilde{P}$ is minimally ramified;*
(2) *if $p = 2$ and $n \geqslant 2$, then $\widetilde{P}$ is either minimally ramified, or almost minimally ramified.*

Proof. If the reduction of P is non-linear, then for every integer n the order $i_n(\widetilde{P}^q)$ is finite, and therefore the assertions are direct consequences of Lemma 2.3 and Corollary 3.10. Thus, to complete the proof of the corollary we just need to show that the reduction of P is non-linear. Suppose by contradiction that this is not the case. Extending K if necessary, we assume that it is algebraically closed. Then there is μ in $\mathfrak{m}_K \setminus \{0\}$ such that the polynomial $Q(w) := \mu^{-1}P(\mu w)$ is in $\mathcal{O}_K[w]$. Note that the map $M_\mu(w) = \mu w$ maps the periodic points of Q to those of P preserving minimal periods. Thus, applying Lemma 2.3 to Q, we conclude that P cannot have an optimal cycle. This contradiction proves that the reduction of P is non-linear and completes the proof of the corollary. □

Proof of Proposition 3.7. To prove (3.4) with $n = 2$, note first that by Proposition 3.2 with $n = 1$ we have $i_1(g^q) \geqslant 3q$. Suppose that $i_1(g^q) = 3q$, and note that by Theorem D we have $i_0(g^q) = q$, and either $i_2(g^q) = 7q$ or $i_2(g^q) \geqslant 11q$. But we cannot have $i_2(g^q) = 7q$, for otherwise Lemma 3.5 would imply that g is minimally ramified. Thus, $i_2(g^q) \geqslant 11q$. This proves (3.4) with $n = 2$ when $i_1(g^q) = 3q$. If $i_1(g^q) > 3q$, then by Theorem D we have $i_1(g^q) \geqslant 4q$, and by Lemma 3.6 we have $i_2(g^q) \geqslant 2i_1(g^q) \geqslant 8q$. This proves that in all the cases we have (3.4) with $n = 2$. For $n \geqslant 3$ inequality (3.4) is then obtained by applying Lemma 3.6 inductively. This completes the proof of part (1).

To prove part (2), suppose that $i_0(g^q) = 2q$. Applying Lemma 3.6 repeatedly, we conclude that for every $n \geqslant 1$ we have $i_n(g^q) = 2^{n+1}q$. Suppose now that for some $n \geqslant 2$ we have $i_n(g^q) = 2^{n+1}q$. If $n \geqslant 3$, then, applying Lemma 3.6 repeatedly, we obtain

$$i_2(g^q) \leqslant i_n(g^q)/2^{n-2} = 8q, \quad i_1(g^q) \leqslant i_2(g^q)/2 \leqslant 4q, \quad i_0(g^q) \leqslant i_1(g^q)/2 \leqslant 2q. \tag{3.5}$$

https://doi.org/10.1112/S0010437X15007575 Published online by Cambridge University Press

Together with Theorem D, this implies either $i_0(g^q) = q$ or $i_0(g^q) = 2q$. In the latter case we obtain the desired conclusion by applying part (2) of Lemma 3.6 repeatedly. It remains to consider the case $i_0(g^q) = q$. Since $i_1(g^q) \leqslant 4q$ and $i_2(g^q) \leqslant 8q$, by Theorem D we must have $i_1(g^q) = 3q$ and $i_2(g^q) = 7q$. However, by Lemma 3.5 this implies that g is minimally ramified. We thus obtain a contradiction that completes the proof of part (2) and of the proposition. □

4. Characterizing minimally ramified power series

In this section we give a characterization of minimally ramified power series (Theorem E). This characterization is best expressed in terms of the iterative residue, which is a conjugacy invariant introduced by Écalle in the complex setting; see [Éca75]. We define this invariant for a restricted class of power series that is sufficient for our purposes.

Let p be a prime number and k a field of characteristic p. Denote by $\mathscr{K}_k$ the set of power series $g(\zeta)$ in $k[[\zeta]]$ satisfying $g(0) = 0$ and $g'(0) \neq 0$. It is a group under composition. We say that two power series $g(\zeta)$ and $\widehat{g}(\zeta)$ in $\mathscr{K}_k$ are *conjugate* if there is a power series $h(\zeta)$ in $\mathscr{K}_k$ such that $\widehat{g}(\zeta) = h \circ g \circ h^{-1}(\zeta)$. Note that in this case we have $\widehat{g}'(0) = g'(0)$. Moreover, if $\gamma := g'(0)$ is a root of unity and we denote by q its order, then for every integer $n \geqslant 0$ we have $i_n(g^q) = i_n(\widehat{g}^q)$.[6] In particular, minimal ramification is invariant under conjugacy.

Let γ be a root of unity in k, let q be its order, and let $g(\zeta)$ be a power series in $k[[\zeta]]$ satisfying $g'(0) = \gamma$. In the case $\gamma = 1$, so that $q = 1$, put

$$g(\zeta) = \zeta(1 + a_1\zeta + a_2\zeta^2 + \cdots),$$

and assume that $a_1 \neq 0$. Then the *iterative residue* résit(g)[7] *of* g is

$$\text{résit}(g) := 1 - \frac{a_2}{a_1^2}.$$

Note that the condition $a_1 \neq 0$ is equivalent to $i_0(g) = 1$. To define the iterative residue in the case $\gamma \neq 1$, so that $q \geqslant 2$, we use the fact that $g(\zeta)$ is conjugate to a power series of the form

$$\widehat{g}(\zeta) = \gamma\zeta\left(1 + \sum_{j=1}^{+\infty} a_j \zeta^{jq}\right),$$

see Proposition 4.1. In general, the power series $\widehat{g}$ is not uniquely determined by g. To define the 'iterative residue' of g we restrict to the case when $a_1 \neq 0$. This last condition is equivalent to $i_0(g^q) = q$ (Proposition 4.1), so it only depends on g. When this condition is satisfied, the quotient a_2/a_1^2 only depends on g (Proposition 4.1) and we define the *iterative residue of* g by

$$\text{résit}(g) := \frac{q+1}{2} - \frac{a_2}{a_1^2}.$$

Note that in the case $p = 2$ the number q is odd, so the quotient $(q + 1)/2$ is an integer and it thus represents an element of k. Note also that in this case we have $q = 1$ in k.

[6] In fact, $i_n(g^q) + 1$ is equal to the multiplicity of $\zeta = 0$ as a fixed point of $g^{qp^n}(\zeta)$, and this is clearly invariant under conjugacy.

[7] We use Écalle's notation 'résit', which is an abbreviation of the French term *résidue itératif* corresponding to 'iterative residue'.

https://doi.org/10.1112/S0010437X15007575 Published online by Cambridge University Press

Theorem E. *Let p be a prime number, k a field of characteristic p, and γ a root of unity in k. Moreover, let q be the order of γ and let $g(\zeta)$ be a power series in $k[[\zeta]]$ of the form*

$$g(\zeta) = \gamma\zeta + \cdots .$$

If p is odd (respectively, $p = 2$), then g is minimally ramified if and only if

$$i_0(g^q) = q \text{ and } \text{résit}(g) \neq 0$$
$$\text{(respectively, } i_0(g^q) = q,\ \text{résit}(g) \neq 0, \text{ and } \text{résit}(g) \neq 1).$$

When p is odd and $q = 1$, Theorem E is [Riv03, Exemple 3.19], phrased in terms of the iterative residue.

A direct consequence of Theorem E is that for every integer q and every root of unity γ of order q in a field of positive characteristic k, there is a minimally ramified polynomial $g(\zeta) = \gamma\zeta + \cdots$ in $k[\zeta]$ of degree $q + 1$ or $2q + 1$. This is exploited in § 5.

The proof of Theorem E is given in § 4.2, after showing in § 4.1 the results needed to define the iterative residue.

4.1 Conjugacy classes

The purpose of this section is to prove the following proposition that was used above to define the iterative residue.

Proposition 4.1. *Let p be a prime number, k a field of characteristic p, γ a root of unity in k, and q the order of γ. Then every power series $g(\zeta)$ in $k[[\zeta]]$ satisfying $g(\zeta) = \gamma\zeta + \cdots$ is conjugate to a power series of the form*

$$\widehat{g}(\zeta) = \gamma\zeta\left(1 + \sum_{j=1}^{+\infty} a_j \zeta^{jq}\right).$$

Moreover, we have $a_1 \neq 0$ if and only if $i_0(g^q) = q$, and in this case the quotient a_2/a_1^2 depends only on g.

The proof of this proposition depends on a couple of lemmas.

The following lemma is stated in a stronger form than is needed for the proof of Proposition 4.1; it is used in the proofs of Propositions 5.3 and 5.6.

Lemma 4.2. *Let p be a prime number, k a field of characteristic p, and $q \geqslant 2$ an integer that is not divisible by p. Given γ in k^* satisfying $\gamma^q = 1$, and a_1 and a_2 in k, let $g(\zeta)$ be a power series in $k[[\zeta]]$ satisfying*

$$g(\zeta) \equiv \gamma\zeta(1 + a_1\zeta^q + a_2\zeta^{2q}) \mod \langle \zeta^{2q+2} \rangle$$

in $k[[\zeta]]$. Then for every integer $\ell \geqslant 1$,

$$g^\ell(\zeta) \equiv \gamma^\ell\zeta\left(1 + \ell a_1\zeta^q + \left(\ell a_2 + (q+1)\frac{\ell(\ell-1)}{2}a_1^2\right)\zeta^{2q}\right) \mod \langle \zeta^{2q+2} \rangle. \tag{4.1}$$

Proof. We proceed by induction. When $\ell = 1$ the congruence (4.1) holds by definition of g. Let $\ell \geqslant 1$ be an integer for which (4.1) holds. Then, using $q \geqslant 2$, we have

$$\begin{aligned} g^{\ell+1}(\zeta) \equiv{}& \gamma^\ell[\gamma\zeta(1 + a_1\zeta^q + a_2\zeta^{2q})] \\ &\times \left(1 + \ell a_1\zeta^q(1 + a_1\zeta^q)^q + \left(\ell a_2 + (q+1)\frac{\ell(\ell-1)}{2}a_1^2\right)\zeta^{2q}\right) \mod \langle \zeta^{2q+2} \rangle \end{aligned}$$

https://doi.org/10.1112/S0010437X15007575 Published online by Cambridge University Press

$$
\begin{aligned}
&\equiv \gamma^{\ell+1}\zeta(1+a_1\zeta^q+a_2\zeta^{2q})\\
&\quad\times\left(1+\ell a_1\zeta^q+\left(\ell a_2+\left(q\ell+(q+1)\frac{\ell(\ell-1)}{2}\right)a_1^2\right)\zeta^{2q}\right) \mod \langle\zeta^{2q+2}\rangle\\
&\equiv \gamma^{\ell+1}\zeta\left(1+(\ell+1)a_1\zeta^q+\left((\ell+1)a_2+(q+1)\frac{\ell(\ell+1)}{2}a_1^2\right)\zeta^{2q}\right) \mod \langle\zeta^{2q+2}\rangle.
\end{aligned}
$$

This proves the induction step, and completes the proof of the lemma. □

Lemma 4.3. *Let p be a prime number, k a field of characteristic p, γ a root of unity in k, and let q be the order of γ. Given A and $\widehat{A}$ in k^* and B and $\widehat{B}$ in k, let $g(\zeta)$ and $\widehat{g}(\zeta)$ be power series in $k[[\zeta]]$ satisfying*

$$g(\zeta)\equiv\gamma\zeta(1+A\zeta^q+B\zeta^{2q}) \mod \langle\zeta^{2q+2}\rangle$$

and

$$\widehat{g}(\zeta)\equiv\gamma\zeta(1+\widehat{A}\zeta^q+\widehat{B}\zeta^{2q}) \mod \langle\zeta^{2q+2}\rangle$$

in $k[[\zeta]]$. If $g(\zeta)$ and $\widehat{g}(\zeta)$ are conjugate, then

$$\frac{B}{A^2}=\frac{\widehat{B}}{\widehat{A}^2}.$$

Proof. Let λ be in k^* and let $h(\zeta)$ be a power series in $k[[\zeta]]$ of the form

$$h(\zeta)=\lambda\zeta(1+\beta_1\zeta+\beta_2\zeta^2+\cdots),$$

such that $\widehat{g}(\zeta)=h\circ g\circ h^{-1}(\zeta)$. Then

$$h\circ g(\zeta)\equiv\lambda\gamma\zeta(1+\beta_1\gamma\zeta+\cdots+\beta_{q-1}\gamma^{q-1}\zeta^{q-1}) \mod \langle\zeta^{q+1}\rangle,$$

and on the other hand

$$\widehat{g}\circ h(\zeta)\equiv\gamma\lambda\zeta(1+\beta_1\zeta+\cdots+\beta_{q-1}\zeta^{q-1}) \mod \langle\zeta^{q+1}\rangle.$$

Comparing coefficients, we obtain

$$\beta_1=\cdots=\beta_{q-1}=0.$$

Therefore,

$$
\begin{aligned}
h\circ g(\zeta)&\equiv\lambda\gamma\zeta(1+A\zeta^q)\\
&\quad\times(1+\beta_q\zeta^q+\beta_{q+1}\gamma\zeta^{q+1}+\cdots+\beta_{2q-1}\gamma^{q-1}\zeta^{2q-1}) \mod \langle\zeta^{2q+1}\rangle\\
&\equiv\lambda\gamma\zeta(1+(A+\beta_q)\zeta^q+\beta_{q+1}\gamma\zeta^{q+1}+\cdots+\beta_{2q-1}\gamma^{q-1}\zeta^{2q-1}) \mod \langle\zeta^{2q+1}\rangle.
\end{aligned}
$$

On the other hand,

$$
\begin{aligned}
\widehat{g}\circ h(\zeta)&\equiv\gamma\lambda\zeta(1+\beta_q\zeta^q+\cdots+\beta_{2q-1}\zeta^{2q-1})(1+\widehat{A}\lambda^q\zeta^q) \mod \langle\zeta^{2q+1}\rangle\\
&\equiv\gamma\lambda\zeta(1+(\beta_q+\widehat{A}\lambda^q)\zeta^q+\beta_{q+1}\zeta^{q+1}+\cdots+\beta_{2q-1}\zeta^{2q-1}) \mod \langle\zeta^{2q+1}\rangle.
\end{aligned}
$$

Comparing coefficients, we obtain

$$A=\widehat{A}\lambda^q \quad\text{and}\quad \beta_{q+1}=\cdots=\beta_{2q-1}=0.$$

https://doi.org/10.1112/S0010437X15007575 Published online by Cambridge University Press

In particular, we have

$$h(\zeta) \equiv \lambda\zeta(1 + \beta_q\zeta^q + \beta_{2q}\zeta^{2q}) \mod \langle \zeta^{2q+2} \rangle.$$

Thus

$$\begin{aligned} h \circ g(\zeta) &\equiv \lambda\gamma\zeta(1 + A\zeta^q + B\zeta^{2q})(1 + \beta_q\zeta^q(1 + A\zeta^q)^q + \beta_{2q}\zeta^{2q}) \mod \langle \zeta^{2q+2} \rangle \\ &\equiv \lambda\gamma\zeta(1 + A\zeta^q + B\zeta^{2q})(1 + \beta_q\zeta^q + (q\beta_q A + \beta_{2q})\zeta^{2q}) \mod \langle \zeta^{2q+2} \rangle \\ &\equiv \lambda\gamma\zeta(1 + (A + \beta_q)\zeta^q + (B + (q+1)\beta_q A + \beta_{2q})\zeta^{2q}) \mod \langle \zeta^{2q+2} \rangle, \end{aligned}$$

and, on the other hand,

$$\begin{aligned} \widehat{g} \circ h(\zeta) &\equiv \gamma\lambda\zeta(1 + \beta_q\zeta^q + \beta_{2q}\zeta^{2q})(1 + \widehat{A}\lambda^q\zeta^q(1 + \beta_q\zeta^q)^q + \widehat{B}\lambda^{2q}\zeta^{2q}) \mod \langle \zeta^{2q+2} \rangle \\ &\equiv \gamma\lambda\zeta(1 + \beta_q\zeta^q + \beta_{2q}\zeta^{2q})(1 + \widehat{A}\lambda^q\zeta^q + (q\widehat{A}\lambda^q\beta_q + \widehat{B}\lambda^{2q})\zeta^{2q}) \mod \langle \zeta^{2q+2} \rangle \\ &\equiv \gamma\lambda\zeta(1 + (\beta_q + \widehat{A}\lambda^q)\zeta^q + (\beta_{2q} + (q+1)\widehat{A}\lambda^q\beta_q + \widehat{B}\lambda^{2q})\zeta^{2q}) \mod \langle \zeta^{2q+2} \rangle. \end{aligned}$$

Comparing coefficients and using $\lambda^q = A/\widehat{A}$, we obtain the lemma. □

Proof of Proposition 4.1. The last assertion is given by Lemma 4.3. Since $i_0(\widehat{g}^q) = i_0(g^q)$, the equivalence between $a_1 \neq 0$ and $i_0(g^q) = q$ is trivial when $q = 1$, and it follows from Lemma 4.2 with $\ell = q$ when $q \geqslant 2$.

It remains to prove the first assertion of the proposition. In the case $q = 1$, take $\widehat{g} = g$. Assume that $q \geqslant 2$. Let $s_0(\zeta)$ and $h_0(\zeta)$ be the power series in $k[[\zeta]]$ defined by

$$s_0(\zeta) := 1 \quad \text{and} \quad h_0(\zeta) := \zeta.$$

We define inductively for every integer $\ell \geqslant 1$ polynomials $s_\ell(\zeta)$ and $h_\ell(\zeta)$ in $k[\zeta]$ of degree at most $\ell + 1$ and $[\ell/q]$, respectively, such that

$$h_\ell(\zeta) \equiv h_{\ell-1}(\zeta) \mod \langle \zeta^{\ell+1} \rangle \quad \text{and} \quad s_\ell(\zeta) \equiv s_{\ell-1}(\zeta) \mod \langle \zeta^{[(\ell-1)/q]} \rangle,$$

and such that the power series $g_\ell(\zeta) := h_\ell \circ g \circ h_\ell^{-1}(\zeta)$ in $k[[\zeta]]$ satisfies

$$g_\ell(\zeta) \equiv \gamma\zeta s_\ell(\zeta^q) \mod \langle \zeta^{\ell+2} \rangle. \tag{4.2}$$

This clearly implies the first assertion of the proposition.

Note that

$$g_0(\zeta) := h_0 \circ g \circ h_0^{-1}(\zeta) = g(\zeta) \equiv \gamma\zeta \mod \langle \zeta^2 \rangle,$$

so (4.2) is satisfied when $\ell = 0$. Let $\ell \geqslant 1$ be an integer for which $s_{\ell-1}(\zeta)$ and $h_{\ell-1}(\zeta)$ are already defined and satisfy (4.2) with ℓ replaced by $\ell - 1$, and let A in k be such that

$$g_{\ell-1}(\zeta) \equiv \gamma\zeta(s_{\ell-1}(\zeta^q) + A\zeta^\ell) \mod \langle \zeta^{\ell+2} \rangle.$$

In the case where ℓ is divisible by q, the congruence (4.2) is verified if we put

$$h_\ell(\zeta) := h_{\ell-1}(\zeta) \quad \text{and} \quad s_\ell(\zeta) := s_{\ell-1}(\zeta) + A\zeta^{\ell/q}.$$

Suppose that ℓ is not divisible by q. Put $\alpha := -A/(\gamma^\ell - 1)$, and define

$$h(\zeta) := \zeta(1 + \alpha\zeta^\ell).$$

https://doi.org/10.1112/S0010437X15007575 Published online by Cambridge University Press

Moreover, put

$$h_\ell(\zeta) := h \circ h_{\ell-1}(\zeta) \quad \text{and} \quad s_\ell(\zeta) := s_{\ell-1}(\zeta).$$

Then

$$g_\ell(\zeta) = h_\ell \circ g \circ h_\ell^{-1}(\zeta) = h \circ g_{\ell-1} \circ h^{-1}(\zeta),$$

so there is B in k such that

$$\begin{aligned} g_\ell(\zeta) &\equiv \gamma\zeta(s_{\ell-1}(\zeta^q) + B\zeta^\ell) \mod \langle \zeta^{\ell+2} \rangle \\ &\equiv \gamma\zeta(s_\ell(\zeta^q) + B\zeta^\ell) \mod \langle \zeta^{\ell+2} \rangle. \end{aligned}$$

Thus, to complete the proof of the induction step it is enough to show that $B = 0$. To do this, note that by our definition of α,

$$\begin{aligned} h \circ g_{\ell-1}(\zeta) &= g_{\ell-1}(\zeta)(1 + \alpha g_{\ell-1}(\zeta)^\ell) \\ &\equiv \gamma\zeta(s_{\ell-1}(\zeta^q) + A\zeta^\ell)(1 + \alpha\gamma^\ell\zeta^\ell) \mod \langle \zeta^{\ell+2} \rangle \\ &\equiv \gamma\zeta(s_{\ell-1}(\zeta^q) + (A + \alpha\gamma^\ell)\zeta^\ell) \mod \langle \zeta^{\ell+2} \rangle \\ &\equiv \gamma\zeta(s_{\ell-1}(\zeta^q) + \alpha\zeta^\ell) \mod \langle \zeta^{\ell+2} \rangle. \end{aligned}$$

On the other hand,

$$\begin{aligned} g_\ell \circ h(\zeta) &\equiv \gamma h(\zeta)(s_{\ell-1}(h(\zeta)^q) + Bh(\zeta)^\ell) \mod \langle \zeta^{\ell+2} \rangle \\ &\equiv \gamma\zeta(1 + \alpha\zeta^\ell)(s_{\ell-1}(\zeta^q) + B\zeta^\ell) \mod \langle \zeta^{\ell+2} \rangle \\ &\equiv \gamma\zeta(s_{\ell-1}(\zeta^q) + (\alpha + B)\zeta^\ell) \mod \langle \zeta^{\ell+2} \rangle. \end{aligned}$$

Comparing coefficients, we conclude that $B = 0$. This completes the proof of the induction step and of the proposition. □

4.2 Proof of Theorem E

The proof of Theorem E is given after the following proposition, which is the special case $q = 1$. When p is odd, the proposition is [Riv03, Exemple 3.19]. We include its short proof for completeness.

Proposition 4.4. *Let p be a prime number and k a field of characteristic p. Given a_1 and a_2 in k, let $g(\zeta)$ be a power series in $k[[\zeta]]$ satisfying*

$$g(\zeta) \equiv \zeta(1 + a_1\zeta + a_2\zeta^2) \mod \langle \zeta^4 \rangle$$

in $k[[\zeta]]$. If p is odd (respectively, $p = 2$), then g is minimally ramified if and only if

$$a_1 \neq 0 \text{ and } a_2 \neq a_1^2 \text{ (respectively, } a_1 \neq 0,\ a_2 \neq 0, \text{ and } a_2 \neq a_1^2\text{).}$$

Proof. Note that $i_0(g) = 1$ is equivalent to $a_1 \neq 0$. Since this is necessary for g to be minimally ramified, we assume that $a_1 \neq 0$. In part (1) we prove the proposition when p is odd, and in part (2) when $p = 2$.

(1) Suppose that p is odd. Note that by Proposition 3.2 the power series g is minimally ramified if and only if $i_1(g) = p + 1$.

For n in $\{1, \ldots, p\}$ define the power series $\Delta_n(\zeta)$ in $k[[\zeta]]$ inductively by $\Delta_1(\zeta) := g(\zeta) - \zeta$, and for n in $\{2, \ldots, p\}$ by

$$\Delta_n(\zeta) := \Delta_{n-1}(g(\zeta)) - \Delta_{n-1}(\zeta).$$

Note that $\Delta_p(\zeta) = g^p(\zeta) - \zeta$.

https://doi.org/10.1112/S0010437X15007575 Published online by Cambridge University Press

We prove first that

$$\Delta_{p-1}(\zeta) \equiv -a_1^{p-1}\zeta^p - a_1^{p-2}(a_2 - a_1^2)\zeta^{p+1} \mod \langle \zeta^{p+2} \rangle. \tag{4.3}$$

To do this, first we prove by induction that, for every n in $\{1, \dots, p-1\}$,

$$\Delta_n(\zeta) \equiv n! a_1^n \zeta^{n+1} \mod \langle \zeta^{n+2} \rangle. \tag{4.4}$$

When $n = 1$ this is true by the definition of Δ_1. Let n in $\{1, \dots, p-2\}$ be such that (4.4) holds, and let B in k be such that

$$\Delta_n(\zeta) \equiv n! a_1^n \zeta^{n+1} + B\zeta^{n+2} \mod \langle \zeta^{n+3} \rangle.$$

Then

$$\begin{aligned} \Delta_{n+1}(\zeta) &\equiv n! a_1^n \zeta^{n+1}(1 + a_1\zeta)^{n+1} + B\zeta^{n+2} \\ &\quad - (n! a_1^n \zeta^{n+1} + B\zeta^{n+2}) \mod \langle \zeta^{n+3} \rangle. \\ &\equiv (n+1)! a_1^{n+1} \zeta^{n+2} \mod \langle \zeta^{n+3} \rangle. \end{aligned}$$

This proves the induction step and (4.4). To prove (4.3), put $A' := a_1^{p-2}$ and note that by (4.4) with $n = p-2$ there are B' and C' in k such that

$$\Delta_{p-2}(\zeta) \equiv A'\zeta^{p-1} + B'\zeta^p + C'\zeta^{p+1} \mod \langle \zeta^{p+2} \rangle.$$

We thus have

$$\begin{aligned} \Delta_{p-1}(\zeta) &\equiv A'\zeta^{p-1}(1 + a_1\zeta + a_2\zeta^2)^{p-1} + B'\zeta^p(1 + a_1\zeta)^p + C'\zeta^{p+1} \\ &\quad - (A'\zeta^{p-1} + B'\zeta^p + C'\zeta^{p+1}) \mod \langle \zeta^{p+2} \rangle \\ &\equiv -A'a_1\zeta^p + A'(a_1^2 - a_2)\zeta^{p+1} \mod \langle \zeta^{p+2} \rangle. \end{aligned}$$

This proves (4.3).

To complete the proof, put

$$A'' := -a_1^{p-1} \quad \text{and} \quad B'' := -a_1^{p-2}(a_2 - a_1^2),$$

and note that by (4.3) there is C'' in k such that

$$\Delta_{p-1}(\zeta) \equiv A''\zeta^p + B''\zeta^{p+1} + C''\zeta^{p+2} \mod \langle \zeta^{p+3} \rangle.$$

Using $p \geqslant 3$, we have

$$\begin{aligned} \Delta_p(\zeta) &\equiv A''\zeta^p(1 + a_1\zeta + a_2\zeta^2)^p + B''\zeta^{p+1}(1 + a_1\zeta)^{p+1} + C''\zeta^{p+2} \\ &\quad - (A''\zeta^p + B''\zeta^{p+1} + C''\zeta^{p+2}) \mod \langle \zeta^{p+3} \rangle \\ &\equiv a_1 B''\zeta^{p+2} \mod \langle \zeta^{p+3} \rangle \\ &\equiv -a_1^{p-1}(a_2 - a_1^2)\zeta^{p+2} \mod \langle \zeta^{p+3} \rangle. \end{aligned}$$

This proves that we have $i_1(g) = p + 1$ if and only if $a_2 \neq a_1^2$, and completes the proof of the proposition when p is odd.

(2) Suppose that $p = 2$. Note that by Proposition 3.2 the power series g is minimally ramified if and only if $i_2(g^q) = 7$.

Put

$$\Delta_1(\zeta) := g(\zeta) - \zeta \quad \text{and} \quad \Delta_2(\zeta) := \Delta_1(g(\zeta)) - \Delta_1(\zeta),$$

https://doi.org/10.1112/S0010437X15007575 Published online by Cambridge University Press

and note that $\Delta_2(\zeta) = g^2(\zeta) - \zeta$. Letting a_3 and a_4 in k be such that

$$g(\zeta) \equiv \zeta(1 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3 + a_4\zeta^4) \mod \langle \zeta^6 \rangle,$$

we have

$$\begin{aligned}\Delta_2(\zeta) \equiv{}& a_1\zeta^2(1 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3)^2 + a_2\zeta^3(1 + a_1\zeta + a_2\zeta^2)^3 \\ &+ a_3\zeta^4(1 + a_1\zeta)^4 + a_4\zeta^5 \\ &- (a_1\zeta^2 + a_2\zeta^3 + a_3\zeta^4 + a_4\zeta^5) \mod \langle \zeta^6 \rangle \\ \equiv{}& a_1\zeta^2(1 + a_1^2\zeta^2) + a_2\zeta^3(1 + a_1\zeta + (a_2 + a_1^2)\zeta^2) \\ &- (a_1\zeta^2 + a_2\zeta^3) \mod \langle \zeta^6 \rangle \\ \equiv{}& a_1(a_2 + a_1^2)\zeta^4 + a_2(a_2 + a_1^2)\zeta^5 \mod \langle \zeta^6 \rangle.\end{aligned}$$

We thus obtain

$$g^2(\zeta) \equiv \zeta(1 + a_1(a_2 + a_1^2)\zeta^3 + a_2(a_2 + a_1^2)\zeta^4) \mod \langle \zeta^6 \rangle. \tag{4.5}$$

Put

$$\widehat{\Delta}_1(\zeta) := g^2(\zeta) - \zeta \quad \text{and} \quad \widehat{\Delta}_2(\zeta) := \widehat{\Delta}_1(g^2(\zeta)) - \widehat{\Delta}_1(\zeta),$$

and note that $\widehat{\Delta}_1(\zeta) = \Delta_2(\zeta)$ and $\widehat{\Delta}_2(\zeta) = g^4(\zeta) - \zeta$. So, if we put

$$A := a_1(a_2 + a_1^2) \quad \text{and} \quad B := a_2(a_2 + a_1^2),$$

then by (4.5) there are C, D, and E in k such that

$$\widehat{\Delta}_1(\zeta) \equiv A\zeta^4 + B\zeta^5 + C\zeta^6 + D\zeta^7 + E\zeta^8 \mod \langle \zeta^9 \rangle.$$

Then we have

$$\begin{aligned}\widehat{\Delta}_2(\zeta) \equiv{}& A\zeta^4(1 + A\zeta^3 + B\zeta^4)^4 + B\zeta^5(1 + A\zeta^3)^5 + C\zeta^6 + D\zeta^7 + E\zeta^8 \\ &- (A\zeta^4 + B\zeta^5 + C\zeta^6 + D\zeta^7 + E\zeta^8) \mod \langle \zeta^9 \rangle \\ \equiv{}& AB\zeta^8 \mod \langle \zeta^9 \rangle \\ \equiv{}& a_1a_2(a_2 + a_1^2)^2\zeta^8 \mod \langle \zeta^9 \rangle.\end{aligned}$$

This proves that $i_2(g^q) = 7$ if and only if $a_2 \neq 0$ and $a_2 \neq a_1^2$, and completes the proof of the proposition when $p = 2$. □

Proof of Theorem E. Since minimal ramification is invariant under conjugacy, by Proposition 4.1 we can assume that $g(\zeta)$ is of the form

$$g(\zeta) = \gamma\zeta\left(1 + \sum_{j=1}^{+\infty} a_j\zeta^{jq}\right).$$

By Proposition 4.1 when $q \geqslant 2$, we have $a_1 \neq 0$ if and only if $i_0(g^q) = q$. Since this last condition is necessary for g to be minimally ramified, from now on we assume that $a_1 \neq 0$.

Put

$$\pi(\zeta) := \zeta^q \quad \text{and} \quad \widehat{g}(\zeta) := \zeta\left(1 + \sum_{j=1}^{+\infty} a_j\zeta^j\right)^q,$$

and note that $\pi \circ g = \widehat{g} \circ \pi$. Since q is not divisible by p, this implies that, for every integer $n \geqslant 1$,

$$i_n(g) = \operatorname{ord}\left(\left(\frac{g^{qp^n}(\zeta)}{\zeta}\right)^q - 1\right) = \operatorname{ord}\left(\frac{\widehat{g}^{qp^n} \circ \pi(\zeta) - \pi(\zeta)}{\pi(\zeta)}\right) = qi_n(\widehat{g}^q) = qi_n(\widehat{g}).$$

Thus g is minimally ramified if and only if $\widehat{g}$ is. Then the theorem is a direct consequence of Proposition 4.4. □

https://doi.org/10.1112/S0010437X15007575 Published online by Cambridge University Press

5. Optimal cycles

In this section we address the optimality of the periodic points lower bounds (1.4) and (2.2). In § 5.1 we prove a general version of Theorem B which we state as Theorem B′. This result implies in particular that the lower bound (1.4) is optimal. In § 5.2 we exhibit concrete polynomials that satisfy the conclusions of Theorem A; see Propositions 5.3 and 5.6. Part (1) of Proposition 5.3 implies that inequality (2.2) is optimal. The proof of Theorem C is given at the end of § 5.2.

5.1 Optimality of the periodic points lower bound

The purpose of this section is to prove the following result, which is a more general version of Theorem B.

Theorem B′. *Let p be a prime number, $(K, |\cdot|)$ an algebraically closed field of residue characteristic p, and $q \geqslant 1$ an integer that is not divisible by p. Then the following properties hold.*

(1) *Let λ in K be such that $|\lambda| = 1$ and such that the order of $\widetilde{\lambda}$ in $\widetilde{K}^*$ is q. Moreover, let $n \geqslant 1$ be an integer and $P(z) = \lambda z + \cdots$ a polynomial in $\mathcal{O}_K[z]$ having an optimal cycle of period qp^n. Then this is the only cycle of minimal period qp^n of f, and if p is odd, then the reduction of P is minimally ramified. If $p = 2$ and $n \geqslant 2$, then the reduction of P is minimally ramified or almost minimally ramified.*

(2) *Let F be the prime field of K, γ a root of unity in $\widetilde{K}$ of order q, and $g(\zeta) = \gamma\zeta + \cdots$ a polynomial in $\widetilde{K}[\zeta]$ that is either minimally ramified if p is odd, or minimally ramified or almost minimally ramified if $p = 2$. Then for all integers $n \geqslant 1$ and $d \geqslant \max\{\deg(g), p\}$, there is a non-zero polynomial $R_n(\alpha_1, \ldots, \alpha_d)$ in $F[\alpha_1, \ldots, \alpha_d]$ such that the following property holds. If $a_1, \ldots, a_d$ in $\mathcal{O}_K$ are such that the reduction of the polynomial $P(z) := a_1 z + \cdots + a_d z^d$ is g and such that $R_n(a_1, \ldots, a_n) \neq 0$, then P has an optimal cycle of period qp^n.*

The proof of Theorem B′ is at the end of this section. We use the following general criterion, which is stated in a more general form than is needed for this section.

Proposition 5.1. *Let p be a prime number, and $(K, |\cdot|)$ an algebraically closed ultrametric field of residue characteristic p. Given an integer $q \geqslant 1$ that is not divisible by p, let λ in K be such that $|\lambda| = 1$, and such that the order of $\widetilde{\lambda}$ in $\widetilde{K}^*$ is equal to q. Then, for every power series $f(z) = \lambda z + \cdots$ in $\mathcal{O}_K[[z]]$, the following properties hold.*

(1) *Suppose that* $\operatorname{wideg}(f^q(z) - z) = q + 1$ *and $\lambda^q \neq 1$. Then f has a unique periodic orbit in $\mathfrak{m}_K \backslash \{0\}$ of minimal period q, and for every periodic point w_0 in this orbit, inequality (2.2) holds with equality.*

(2) *Let $n \geqslant 1$ be an integer, and suppose that*

$$\operatorname{wideg}\left(\frac{f^{qp^n}(z) - z}{f^{qp^{n-1}}(z) - z}\right) = qp^n,$$

and that for every periodic point z_0 of period qp^{n-1} we have $(f^{qp^n})'(z_0) \neq 1$. Then there is a unique cycle of f of minimal period qp^n, and this cycle is optimal.

Note that to formulate part (2), we used the fact that the power series $f^{qp^{n-1}}(z) - z$ divides $f^{qp^n}(z) - z$ in $\mathcal{O}_K[[z]]$; this is obtained by applying Lemma 2.2 with $g = f^{qp^{n-1}}$ and $m = p$.

Proof of Proposition 5.1. To prove part (1), note first that every periodic point of f in $\mathfrak{m}_K \backslash \{0\}$ of minimal period q is a zero of $(f^q(z) - z)/z$. Thus, our hypothesis $\operatorname{wideg}(f^q(z) - z) = q + 1$ implies

https://doi.org/10.1112/S0010437X15007575 Published online by Cambridge University Press

that there is at most one periodic orbit of f in $\mathfrak{m}_K\backslash\{0\}$ of minimal period q. To prove that such a periodic orbit exists, note that our hypotheses $\lambda^q \neq 1$ and $\operatorname{wideg}(f^q(z)-z) = q+1$ imply that there is at least one zero w_0 of $(f^q(z)-z)/z$ in $\mathfrak{m}_K\backslash\{0\}$. Then w_0 is a periodic point of f of period q, and Lemma 2.1 implies that the minimal period of w_0 is q. This proves that there is a unique periodic orbit of f in $\mathfrak{m}_K\backslash\{0\}$ of period q. In view of our hypothesis $\operatorname{wideg}(f^q(z)-z) = q+1$, part (1) of Lemma 2.3 implies that (2.2) holds with equality. This completes the proof of part (1).

To prove part (2), put

$$h(z) := \frac{f^{qp^n}(z)-z}{f^{qp^{n-1}}(z)-z},$$

and note that every periodic point of f of minimal period qp^n is a zero of h. Thus, our hypothesis $\operatorname{wideg}(h) = qp^n$ implies that there is at most one periodic orbit of f of minimal period qp^n. To prove that such a periodic orbit exists, note that our hypothesis $\operatorname{wideg}(h) = qp^n$ implies that h has a zero z_0 in $\mathfrak{m}_K$. Then z_0 is also a zero of $f^{qp^n}(z)-z$, and therefore z_0 is a periodic point of f of period qp^n. Suppose by contradiction that the minimal period of z_0 is not qp^n. Then Lemma 2.1 implies that z_0 is of period qp^{n-1}, and therefore a zero of $f^{qp^{n-1}}(z)-z$. By hypothesis we also have $(f^{qp^n})'(z_0) \neq 1$. On the other hand, since z_0 is also a zero of h, it follows that z_0 is a multiple zero of $f^{qp^n}(z)-z$. This implies that z_0 is also a zero of $(f^{qp^n})'(z)-1$, so $(f^{qn})'(z_0) = 1$. We thus obtain a contradiction that shows that the minimal period of z_0 is qp^n, and that there is a unique periodic orbit of f of minimal period qp^n. Finally, note that our hypothesis $\operatorname{wideg}(h) = qp^n$, together with part (2) of Lemma 2.3, implies that (2.2) holds with equality. This completes the proof of part (2), and of the lemma. □

Lemma 5.2. *Let K be a field, $d \geqslant 2$ an integer, and $a_1, \ldots, a_d$ in K algebraically independent over the prime field of K. If the characteristic p of K is positive, suppose in addition that $d \geqslant p$. Then the polynomial*

$$a_1 z + \cdots + a_d z^d$$

in $K[z]$ has no parabolic periodic point.

Proof. When the characteristic of K is zero, the desired assertion is Lemma 3.1. Suppose that the characteristic p of K is positive and that $d \geqslant p$. Denote by $\mathbb{F}_p$ the prime field of K, and by $\overline{\mathbb{F}}_p$ an algebraic closure of $\mathbb{F}_p$.

Suppose by contradiction that there are an integer $n \geqslant 1$ and a periodic point z_0 of period n of the polynomial $P(z) := a_1 z + \cdots + a_d z^d$ in $K[z]$, such that $(P^n)'(z_0)$ is a root of unity. Let $\sigma : \mathbb{F}_p[z_0, a_1, \ldots, a_d] \to \overline{\mathbb{F}}_p$ be a ring homomorphism such that $\sigma(a_p) = 1$, and such that for each j in $\{1, \ldots, d\}$ different from p we have $\sigma(a_j) = 0$. Then $\sigma(P)(z) = z^p$, $\sigma(z_0)$ is a periodic point of period n of $\sigma(P)$, and $(\sigma(P)^n)'(\sigma(z_0)) = \sigma((P^n)'(z_0))$ is a root of unity. On the other hand, $\sigma(P)'$ is the zero polynomial, so $(\sigma(P)^n)'(\sigma(z_0)) = 0$. This contradiction completes the proof of the lemma. □

Proof of Theorem B′. The uniqueness statement in part (1) is given by part (2) of Lemma 2.3. The rest of the assertions of part (1) are given by Corollary 3.11.

To prove part (2), let $\alpha_0, \ldots, \alpha_d$ be algebraically independent over F, and consider the polynomial

$$Q(z) = \alpha_1 z + \cdots + \alpha_d z^d$$

in $F[\alpha_1, \ldots, \alpha_d][z]$. Let $R_n(\alpha_0, \ldots, \alpha_d)$ in $F[\alpha_0, \ldots, \alpha_d]$ be the resultant of the polynomials

$$Q^{qp^{n-1}}(z) - z \quad \text{and} \quad (Q^{qp^n})'(z) - 1.$$

Lemma 5.2 with $P = Q$ implies that $R_n(\alpha_0, \dots, \alpha_d)$ is non-zero. If n and P are as in the statement of part (2) of the theorem, then

$$\operatorname{wideg}\left(\frac{P^{qp^n}(z) - z}{P^{qp^{n-1}}(z) - z}\right) = i_n(g^q) - i_{n-1}(g^q) = qp^n,$$

and for every periodic point z_0 of P of period qp^{n-1} we have $(P^{qp^n})'(z_0) \neq 1$. Then by part (2) of Proposition 5.1 with $f = P$, the polynomial P has an optimal cycle of period qp^n. This completes the proof. □

5.2 Concrete polynomials having optimal cycles

The purpose of this section is to exhibit concrete polynomials having optimal cycles. The case where p is odd is covered by Proposition 5.3, and the case $p = 2$ by Proposition 5.6. Theorem A is a direct consequence of these propositions.

The proof of Theorem C is given at the end of this section.

Proposition 5.3. *Let p be a prime number, and $(K, |\cdot|)$ an algebraically closed ultrametric field of residue characteristic p. Given an integer $q \geqslant 1$ that is not divisible by p, let λ in K be transcendental over the prime field of K, such that $|\lambda| = 1$, and such that the order of $\widetilde{\lambda}$ in $\widetilde{K}^*$ is equal to q. Moreover, let $P(z)$ be the polynomial in $K[z]$ defined by*

$$P(z) := \lambda z(1 + z^q),$$

if p does not divide $q + 1$, and by

$$P(z) := \lambda z(1 + z^q + z^{2q})$$

otherwise. Then the following properties hold.

(1) *There is a unique periodic orbit of P in $\mathfrak{m}_K \backslash \{0\}$ of minimal period q, and for every periodic point w_0 in this orbit, inequality (2.2) holds with equality.*

(2) *If p is odd, then for every $n \geqslant 1$ there is a unique periodic orbit of P of minimal period qp^n. Furthermore, for every point z_0 in this orbit, inequality (1.4) holds with equality.*

Remark 5.4. If K in the proposition above is of positive characteristic, then for λ in K such that $|\lambda| = 1$ and such that the order of $\widetilde{\lambda}$ in $\widetilde{K}^*$ is q, the hypothesis that λ is transcendental over the prime field of K is equivalent to $\lambda^q \neq 1$.

Remark 5.5. In the case where p divides $q + 1$, our results imply that the conclusions of part (2) of Proposition 5.3 are false for the polynomial $\lambda z(1 + z^q)$.

Proposition 5.6. *Let $(K, |\cdot|)$ be an algebraically closed ultrametric field of residue characteristic 2. Given an odd integer $q \geqslant 1$, let λ in K be transcendental over the prime field of K, such that $|\lambda| = 1$, and such that the order of $\widetilde{\lambda}$ in $\widetilde{K}^*$ is q. In the case where the characteristic of K is zero, put*

$$Q(z) := \lambda z(1 + z^{2q}).$$

In the case where the characteristic of K is 2, let μ in $\mathfrak{m}_K$ be algebraically independent with respect to λ over the prime field of K, and put

$$Q(z) := \lambda z(1 + \mu z^q + z^{2q}).$$

Then, for every integer $n \geqslant 1$ there is a unique periodic orbit of Q of minimal period $2^n q$. Furthermore, for every periodic point z_0 in this orbit, inequality (1.4) holds with equality.

https://doi.org/10.1112/S0010437X15007575 Published online by Cambridge University Press

Remark 5.7. If K in either Proposition 5.3 or 5.6 is of characteristic zero, then λ can be allowed to be algebraic over the prime field of K, as long as λ avoids a finite set of exceptional values that depends on n. Similarly, in the case where K in Proposition 5.6 is of characteristic 2, we show that for each n there is a non-zero polynomial R_n in λ and μ with coefficients in the prime field of K, such that the conclusions of the proposition hold whenever $R_n(\lambda, \mu)$ is non-zero. Thus, λ and μ can be allowed to be algebraic over the prime field of K, as long as (λ, μ) avoids a curve in $K \times K$ that depends on n.

Remark 5.8. In the Appendix we show that, when K is of characteristic 2, the conclusions of Proposition 5.6 are false if we let $\mu = 0$; see Remark A.2.

The following lemma is the main ingredient in the proofs of Propositions 5.3 and 5.6, and of Theorem C.

Lemma 5.9. *Let K be a field, and λ in K that is transcendental over the prime field of K. Moreover, let $q \geqslant 1$ be an integer, and let $P(z)$ be the polynomial in $K[z]$ defined by either*

$$P(z) := \lambda z(1 + z^q) \quad \textit{or} \quad P(z) := \lambda z(1 + z^q + z^{2q}).$$

If the characteristic p of K is positive, suppose in addition that p does not divide q. Then $P(z)$ has no parabolic periodic point.

Proof. Let F be the prime field of K. Without loss of generality assume that K is an algebraic closure of the field $F(\lambda)$.

Case 1: the characteristic of K is zero. We give the proof in the case $P(z) = \lambda z(1+z^q+z^{2q})$. The proof in the case $P(z) = \lambda z(1+z^q)$ is analogous.[8] Given α in K, consider the polynomial $Q_\alpha(z) := \alpha^2 z + \alpha z^{q+1} + z^{2q+1}$ in $K[z]$. Note that if for β in K we put $h_\beta(z) := \beta z$, then

$$h_\beta^{-1} \circ Q_{\beta^q} \circ h_\beta(z) = \beta^{2q} z(1 + z^q + z^{2q}).$$

Thus, to prove that $P(z)$ has no parabolic periodic point, it is enough to show that if α is transcendental over F, then Q_α has no parabolic periodic point.

Let $m \geqslant 1$ be an integer, and let $R(\alpha)$ be the resultant of the polynomials

$$Q_\alpha^m(z) - z \quad \text{and} \quad (Q_\alpha^m)'(z) - 1,$$

viewed as a polynomial in α with coefficients in F. Note that Q_α has a periodic point of period m and multiplier 1 if and only if $R(\alpha) = 0$. Since α is transcendental over F, to show that $R(\alpha)$ is different from zero it is enough to show that the polynomial R is non-zero. Note that when $\alpha = 0$ we have $Q_0^m(z) = z^{(2q+1)^m}$, and that the polynomials

$$Q_0^m(z) - z = z^{(2q+1)^m} - z \quad \text{and} \quad (Q_0^m)'(z) - 1 = (2q+1)^m z^{(2q+1)^m - 1} - 1$$

have no common zero. This implies that $R(0)$ is different from zero, and therefore that R is non-zero. We conclude that $R(\alpha)$ is different from zero, and that Q_α has no periodic point of period m and multiplier 1. Since $m \geqslant 1$ is arbitrary, we conclude that Q_α, and hence P, has no parabolic periodic point.

[8] Note also that the proof in Case 2.1, stated for the case where the characteristic of K is positive, also works in the case where the characteristic of K is zero.

https://doi.org/10.1112/S0010437X15007575 Published online by Cambridge University Press

Case 2: the characteristic p of K is positive. Let $m \geqslant 1$ be an integer, and let $R(\lambda)$ be the resultant of the polynomials

$$P^m(z) - z \quad \text{and} \quad (P^m)'(z) - 1,$$

viewed as a polynomial in λ with coefficients in F. Note that P has a periodic point of period m and multiplier 1 if and only if $R(\lambda) = 0$. Since λ is transcendental over the prime field of K, to prove that $R(\lambda)$ is different from zero it is enough to show that the polynomial R is non-zero. To do this, endow K with a non-trivial norm $|\cdot|$, let λ_0 in K be such that $|\lambda_0| > 1$, and let $P_0(z)$ be the polynomial in $K[z]$ defined in the same way as $P(z)$, but with λ replaced by λ_0. We show below, in several cases, that every periodic point of P_0 is repelling. This implies that P_0 has no parabolic periodic point, and therefore that $R(\lambda_0)$ is different from zero. In turn this implies that R is non-zero, that $R(\lambda)$ is different from 0, and that P has no periodic point of period m and multiplier 1. Since $m \geqslant 1$ is an arbitrary integer, this completes the proof of the lemma.

Case 2.1: $P_0(z) = \lambda_0 z(1 + z^q)$. To prove that every periodic point of $P_0(z) := \lambda_0 z(1 + z^q)$ is repelling, it is enough to show that for every periodic point w of P_0 we have $|P_0'(w)| > 1$. Note first that if w in K satisfies $|w| > 1$, then

$$|P_0(w)| = |\lambda_0| \cdot |w|^{q+1} > |w| > 1.$$

Repeating this argument, we obtain that for every integer $\ell \geqslant 1$ we have $|P_0^\ell(w)| > |w| > 1$, so w cannot be periodic. On the other hand, if w is in $\mathcal{O}_K$ and

$$|w| = |1 + w^q| = 1,$$

then $|P_0(w)| = |\lambda_0| > 1$, so by the previous consideration w cannot be periodic either. This proves that every periodic point w of P_0 is such that either

$$|w| < 1 \quad \text{or} \quad |1 + w^q| < 1.$$

If $|w| < 1$, then

$$|P_0'(w)| = |\lambda_0| \cdot |1 + (q+1)w^q| = |\lambda_0| > 1.$$

Otherwise $|1 + w^q| < 1$, so $|w^q| = 1$,

$$|P_0'(w) - \lambda_0 q w^q| = |\lambda_0| \cdot |1 + w^q| < |\lambda_0|,$$

and therefore $|P_0'(w)| = |\lambda_0| > 1$. This completes the proof that every periodic point of P_0 is repelling.

Case 2.2: $P_0(z) = \lambda_0 z(1 + z^q + z^{2q})$ and $p \neq 3$. As in Case 2.1, to prove that every periodic point of P_0 is repelling, we prove that for every periodic point w of P_0 we have $|P_0'(w)| > 1$. Note first that if w is in K and $|w| > 1$, then

$$|P_0(w)| = |\lambda_0| \cdot |w|^{2q+1} > |w| > 1,$$

so w cannot be periodic. On the other hand, if w is in $\mathcal{O}_K$ and

$$|w| = |1 + w^q + w^{2q}| = 1,$$

then $|P_0(w)| = |\lambda_0| > 1$, so by the previous consideration w cannot be periodic either. This proves that each periodic point w of P_0 satisfies either

$$|w| < 1 \quad \text{or} \quad |1 + w^q + w^{2q}| < 1.$$

https://doi.org/10.1112/S0010437X15007575 Published online by Cambridge University Press

If $|w| < 1$, then

$$|P_0'(w)| = |\lambda_0| \cdot |1 + (q+1)w^q + (2q+1)w^{2q}| = |\lambda_0| > 1.$$

Suppose that $|1 + w^q + w^{2q}| < 1$, and note that, together with our assumption $p \neq 3$, this implies $|1 + 2w^q| = 1$. On the other hand,

$$|P_0'(w) - \lambda_0 q w^q (1 + 2w^q)| = |\lambda_0| \cdot |1 + w^q + w^{2q}| < |\lambda_0|,$$

so $|P_0'(w)| = |\lambda_0| > 1$. This completes the proof that every periodic point of P_0 is repelling.

Case 2.3: $P_0(z) = \lambda_0 z(1 + z^q + z^{2q})$ and $p = 3$. Note that

$$P_0(z) = \lambda_0 z(1 - z^q)^2,$$

and that the fixed point $z = 0$ of P_0 is repelling.

To prove that every periodic point of P_0 is repelling, consider the function $\varrho \colon K \to (0, +\infty]$ defined by

$$\varrho(z) := \frac{1}{|z|^{2/3} \cdot |1 - z^q|^{1/3}},$$

viewed as a singular metric ϱ on K. Below we show that for every periodic point w_0 of P_0 different from zero, the derivative

$$|P_0'|_\varrho(w_0) := |P_0'(w_0)| \frac{\varrho(P_0(w_0))}{\varrho(w_0)}$$

is finite and satisfies $|P_0'|_\varrho(w_0) > 1$. Denoting the orbit of w_0 by $\mathcal{O}$, this implies that the multiplier $\prod_{w \in \mathcal{O}} P_0'(w)$ of w_0 satisfies

$$\left| \prod_{w \in \mathcal{O}} P_0'(w) \right| = \prod_{w \in \mathcal{O}} \left(|P_0'(w)| \frac{\varrho(P_0(w))}{\varrho(w)} \right) = \prod_{w \in \mathcal{O}} |P_0'|_\varrho(w) > 1,$$

so w_0 is repelling. Since $z = 0$ is a repelling fixed point of P_0, it follows that every periodic point of P_0 is repelling.

Let w_0 be a periodic point of P_0 different from zero, and let $\mathcal{O}$ be its orbit. Note that every element w of $\mathcal{O}$ is different from zero. On the other hand, no element of $\mathcal{O}$ can be a zero of $1 - z^q$, because every zero of $1 - z^q$ is mapped to zero by P_0. Thus, ϱ is finite on $\mathcal{O}$, and therefore $|P_0'|_\varrho$ is also finite on $\mathcal{O}$; in particular, $|P_0'|_\varrho(w_0)$ is finite. It remains to prove that $|P_0'|_\varrho(w_0) > 1$. To do this, we prove first that for each w in $\mathcal{O}$ we have either $|w| < 1$ or $|1 - w^q| < 1$. Suppose by contradiction that for some w in $\mathcal{O}$ we have $|w| > 1$. This implies that

$$|P_0(w)| = |\lambda| \cdot |w|^{2q+1} > |w| > 1.$$

Repeating this argument, we conclude that for every integer $\ell \geqslant 1$ we have $|P_0^\ell(w)| > |w| > 1$, so w cannot be periodic. This contradiction proves that $\mathcal{O}$ is contained in $\mathcal{O}_K$. Suppose by contradiction that for some w in $\mathcal{O}$ we have $|w| = |1 - w^q| = 1$. Then $|P_0(w)| = |\lambda_0| > 1$, so by the previous consideration w cannot be periodic. This contradiction proves that for every w in $\mathcal{O}$ we have either $|w| < 1$ or $|1 - w^q| < 1$. To prove that $|P_0'|_\varrho(w_0) > 1$, suppose first that $|w_0| < 1$. Note that $P_0(w_0)$ is in $\mathcal{O}$, and therefore in $\mathcal{O}_K$. On the other hand, we have

$$|P_0(w_0)| = |\lambda_0| \cdot |w_0| \quad \text{and} \quad |P_0'(w_0)| = |\lambda_0|,$$

https://doi.org/10.1112/S0010437X15007575 Published online by Cambridge University Press

so

$$\begin{aligned}|P_0'|_\varrho(w_0) &= |\lambda_0| \cdot \left(\frac{|w_0|}{|P_0(w_0)|}\right)^{2/3} \cdot \frac{1}{|1 - P_0(w_0)^q|^{1/3}} \\ &= |\lambda_0|^{1/3} \cdot \frac{1}{|1 - P_0(w_0)^q|^{1/3}} \geqslant |\lambda_0|^{1/3} > 1.\end{aligned}$$

It remains to consider the case where $|1 - w_0^q| < 1$. Then there is a zero ζ_q of $1 - z^q$, such that $\varepsilon := w_0 - \zeta_q$ satisfies $|\varepsilon| < 1$. Note that

$$|1 - w_0^q| = |\varepsilon|, \quad |P_0(w_0)| = |\lambda_0| \cdot |\varepsilon|^2 \quad \text{and} \quad |P_0'(w_0)| = |\lambda_0| \cdot |\varepsilon|.$$

So

$$\begin{aligned}|P_0'|_\varrho(w_0) &= |\lambda_0| \cdot |\varepsilon| \cdot \frac{1}{|P_0(w_0)|^{2/3}} \cdot \left(\frac{|1 - w_0^q|}{|1 - P_0(w_0)^q|}\right)^{1/3} \\ &= |\lambda_0|^{1/3} \cdot \frac{1}{|1 - P_0(w_0)^q|^{1/3}} \geqslant |\lambda_0|^{1/3} > 1.\end{aligned}$$

This completes the proof of the lemma. □

Proof of Proposition 5.3. Suppose that p is odd. Theorem E implies that $\widetilde{P}$ is minimally ramified. Thus, $\operatorname{wideg}(P^q(z) - z) = q + 1$, and for every integer $n \geqslant 1$ we have

$$\operatorname{wideg}\left(\frac{P^{qp^n}(z) - z}{P^{qp^{n-1}}(z) - z}\right) = qp^n.$$

Then the desired assertions are a direct consequence of Proposition 5.1 and Lemma 5.9.

It remains to prove part (1) when $p = 2$. Note that our hypotheses imply that q is odd, and that $P(z) = \lambda(1 + z^q + z^{2q})$. By Lemma 4.2 with $p = 2$ and $\ell = q$, we have $i_0(\widetilde{P}^q) = q$. Then $\operatorname{wideg}(P^q(z) - z) = q + 1$, and the desired assertion is given by part (1) of Proposition 5.1. This completes the proof of the proposition. □

Proof of Proposition 5.6. By Lemma 4.2 with $p = 2$ and $\ell = q$, we have $i_0(\widetilde{P}) = 2q$. So by part (2) of Proposition 3.7, $\widetilde{P}$ is almost minimally ramified. It follows that, for every integer $n \geqslant 1$,

$$\operatorname{wideg}\left(\frac{P^{2^n q}(z) - z}{P^{2^{n-1} q}(z) - z}\right) = 2^n q.$$

Thus, in view of part (2) of Proposition 5.1, it is enough to prove that P has no parabolic periodic point. If the characteristic of K is zero, this is given by Lemma 5.9 with $p = 2$ and q replaced by $2q$. Suppose that the characteristic of K is 2. Let $m \geqslant 1$ be an integer, and let $R(\lambda, \mu)$ be the resultant of the polynomials

$$Q^m(z) - z \quad \text{and} \quad (Q^m)'(z) - 1,$$

viewed as a polynomial in λ and μ with coefficients in the prime field F of K. Note that Q has a periodic point of period m and multiplier 1 if and only if $R(\lambda, \mu) = 0$. Since μ is algebraically independent with respect to λ over F, to prove that $R(\lambda, \mu)$ is different from zero it is enough to show that the polynomial R is non-zero. To do this, let $P(z)$ be the polynomial in $K[z]$ defined by

$$P(z) = \lambda(1 + z^q + z^{2q}).$$

By Lemma 5.9 this polynomial has no parabolic periodic point. This implies that $R(\lambda, 1)$ is different from zero, and therefore that R is non-zero. Since $m \geqslant 1$ is arbitrary, this completes the proof of the proposition. □

https://doi.org/10.1112/S0010437X15007575 Published online by Cambridge University Press

Proof of Theorem C. Part (2) is given by Corollary 3.11. To prove part (1), note that the hypotheses imply that, for every $n \geqslant 1$,

$$\operatorname{wideg}\left(\frac{P_\lambda^{qp^n}(z) - z}{P_\lambda^{qp^{n-1}}(z) - z}\right) = qp^n.$$

So, in this case, the assertions of the theorem are a direct consequence of Lemma 5.9 with $q = 1$ and part (2) of Proposition 5.1. □

Acknowledgements
We thank Tom Tucker for useful conversations regarding the lifting argument in Lemmas 3.1 and 5.2. We also thank Thomas Ward and the referees for various comments that helped improve the exposition of the paper. Part of this article was developed while the authors were visiting the Institute for Computational and Experimental Research in Mathematics (ICERM). We would like to thank this institute for the excellent working conditions provided.

Appendix. Normalized polynomials without periodic points of high minimal period

In this appendix we give examples of normalized polynomials having no periodic point of high minimal period (Proposition A.1). A consequence is that a polynomial of the form $f(z) = \lambda z(1+z^{2q})$ cannot be used to show that inequality (1.4) is sharp when $p = 2$ and K is of characteristic 2; see Remark A.2 below.

Proposition A.1. *Let p be a prime number and $(K, |\cdot|)$ an ultrametric field of characteristic p. Moreover, let λ in K be such that $|\lambda| = 1$ and such that the order q of $\widetilde{\lambda}$ in $\widetilde{K}^*$ is finite, and let $S(z)$ be a polynomial in $\mathcal{O}_K[z]$ such that $S(0) = 1$ and such that $\operatorname{wideg}(S(z) - 1)$ is finite. If in addition $\lambda^q \neq 1$, then the minimal period of every periodic point of*

$$Q(z) := \lambda z S(z)^p$$

in $\mathfrak{m}_K \backslash \{0\}$ is equal to q. Furthermore, the set F of all such points is non-empty and finite, and for each a in F the multiplicity m_a of a as a fixed point of Q^q is finite and divisible by p, and for every integer $n \geqslant 1$ the multiplicity of a as a fixed point of Q^{qp^n} is equal to $p^n m_a$.

Note that the hypotheses of this proposition imply that λ is not a root of unity. Thus $z = 0$ is an irrationally indifferent fixed point of Q, and therefore for every integer $k \geqslant 1$ the multiplicity of $z = 0$ as a fixed point of Q^k is equal to 1.

Remark A.2. Letting $p = 2$ and $S(z) = 1 + z^q$ in Proposition A.1, we obtain that for every integer $n \geqslant 1$ the polynomial $Q(z) = \lambda z(1 + z^{2q})$ has no periodic point of minimal period equal to qp^n. This shows that the conclusions of Proposition 5.6 are false if we let $\mu = 0$.

Remark A.3. For Q as in Proposition A.1, the set $\mathfrak{m}_K$ is an indifferent component of the Fatou set of Q.[9] So Proposition A.1 shows that Q has an indifferent component of the Fatou set that only

[9] This follows from the fact that Q has integer coefficients and that its reduction is of degree at least 2; see, for example, [Riv03, Propositions 3.18 and 5.2].

https://doi.org/10.1112/S0010437X15007575 Published online by Cambridge University Press

has finitely many periodic points.[10] In contrast, in the p-adic case every indifferent component of the Fatou set contains infinitely many periodic points; see [Riv03, Corollaire 5.13].

The rest of this appendix is devoted to the proof of Proposition A.1. The following lemma is the main ingredient in the proof. Recall that for an ultrametric field K and a polynomial $P(z)$ in $\mathcal{O}_K[z]$, we use $\langle P(z)\rangle$ to denote the ideal of $\mathcal{O}_K[z]$ generated by this polynomial.

Lemma A.4. *Let K be an ultrametric field characteristic p, let $A(z)$ and $T_0(z)$ be polynomials in $\mathcal{O}_K[z]$, and put*

$$Q_\dagger(z) := z(1 + A(z)\cdot T_0(z))^p.$$

Then for each integer $n \geqslant 1$ there exists a polynomial $T_n(z)$ in $\mathcal{O}_K[z]$ such that

$$Q_\dagger^{p^n}(z) = z(1 + A(z)^{p^n}\cdot T_n(z))^p. \tag{A.1}$$

Moreover, $T_1(0) = T_0(0)^p$, and for $n \geqslant 2$ we have in $\mathcal{O}_K[z]$,

$$T_n(z) \equiv T_{n-1}(z)^p \mod \langle zA(z)^{p^{n-1}}\rangle. \tag{A.2}$$

Before proving this lemma, we state and prove the following result.

Lemma A.5. *Let K be an ultrametric field of characteristic p, let $U_\#(z)$ be a polynomial in $\mathcal{O}_K[z]$, and put $Q_\#(z) := zU_\#(z)^p$. Then for each integer $k \geqslant 1$ there is a polynomial $U(z)$ in $\mathcal{O}_K[z]$ such that $Q_\#^k(z) = zU(z)^p$.*

Proof. We proceed by induction in k. The desired property is satisfied with $k = 1$ by definition of $Q_\#$. Given an integer $k \geqslant 1$, suppose that there is a polynomial $U(z)$ in $\mathcal{O}_K[z]$ such that $Q_\#^k(z) = zU(z)^p$. Then

$$Q_\#^{k+1}(z) = Q_\#^k(z)U_\#(Q_\#^k(z))^p = z(U(z)U_\#(Q_\#^k(z)))^p.$$

This completes the proof of the induction step and of the lemma. □

Proof of Lemma A.4. We prove the first assertion of the lemma by induction. Let $n \geqslant 0$ be an integer for which there is a polynomial $T_n(z)$ in $\mathcal{O}_K[z]$ satisfying (A.1). We prove that there is a polynomial T_{n+1} in $\mathcal{O}_K[z]$ satisfying (A.1) with n replaced by $n + 1$. To do this, we prove by induction that, for every integer $j \geqslant 1$,

$$Q_\dagger^{jp^n}(z) \equiv z\prod_{k=0}^{j-1}[1 + A(z)^{p^n}\cdot T_n(Q_\dagger^{kp^n}(z))]^p \mod \langle z^{p+1}A(z)^{p^{2n+2}}\rangle. \tag{A.3}$$

By the first induction hypothesis this holds for $j = 1$. Suppose that it holds for an integer $j \geqslant 1$. Using the first induction hypothesis again, we have

$$Q_\dagger^{(j+1)p^n}(z) = Q_\dagger^{jp^n}(z)[1 + A(Q_\dagger^{jp^n}(z))^{p^n}\cdot T_n(Q_\dagger^{jp^n}(z))]^p. \tag{A.4}$$

[10] Other examples of such Fatou components (which, however, only contain parabolic periodic points) can be obtained as follows. Consider a polynomial $P(z)$ in $K(z)$ of degree at least 2 whose coefficients are algebraic over the prime field of K, and such that $z = 0$ is an indifferent fixed point of P. Then P has good reduction, and therefore $\mathfrak{m}_K$ is a Fatou component of P; see, for example, [Riv03, § 4.5]. Furthermore, $z = 0$ is the only periodic point of P in $\mathfrak{m}_K$. In fact, if we denote by $q \geqslant 1$ the order of $P'(0)$, then for every integer $k \geqslant 1$ the multiplicity of $z = 0$ as a fixed point of P^{qk} coincides with wideg$(P^{qk}(z) - z)$. Together with Lemma 2.1, this implies that $z = 0$ is the only periodic point of P in $\mathfrak{m}_K$.

https://doi.org/10.1112/S0010437X15007575 Published online by Cambridge University Press

On the other hand, by the second induction hypothesis we have

$$Q_{\dagger}^{jp^n}(z) \equiv z \mod \langle zA(z)^{p^{n+1}} \rangle. \tag{A.5}$$

Consequently

$$A(Q_{\dagger}^{jp^n}(z)) \equiv A(z) \mod \langle zA(z)^{p^{n+1}} \rangle,$$

and therefore

$$A(Q_{\dagger}^{jp^n}(z))^{p^n} \equiv A(z)^{p^n} \mod \langle zA(z)^{p^{2n+1}} \rangle.$$

Together with (A.3) and (A.4), we obtain (A.3) with j replaced by $j+1$. This proves the induction step of the second induction, and shows that (A.3) holds for every integer $j \geqslant 1$. To complete the proof of the induction step of the first induction, note that for each integer $k \geqslant 1$ we have by (A.5), with j replaced by k,

$$T_n(Q_{\dagger}^{kp^n}(z)) \equiv T_n(z) \mod \langle zA(z)^{p^{n+1}} \rangle.$$

So if we put $m_n := \min\{p^{2n+2}, p^{n+2} + p^{n+1}\}$, then by (A.3) we have

$$Q_{\dagger}^{jp^n}(z) \equiv z(1 + A(z)^{p^n} \cdot T_n(z))^{jp} \mod \langle z^{p+1} A(z)^{m_n} \rangle.$$

Taking $j = p$, we obtain

$$Q_{\dagger}^{p^{n+1}}(z) \equiv z(1 + A(z)^{p^{n+1}} \cdot T_n(z)^p)^p \mod \langle z^{p+1} A(z)^{m_n} \rangle.$$

Since $m_n \geqslant p^{n+2}$, using Lemma A.5 with $U_{\#}(z) = 1 + A(z)T_0(z)$ and $k = p^{n+1}$, we conclude that there is a polynomial $T_{n+1}(z)$ in $\mathcal{O}_K[z]$ for which (A.1) is satisfied with n replaced by $n+1$. We have thus completed the proof of the first induction step and, as a consequence, shown that (A.1) holds for every integer $n \geqslant 1$.

When $n = 0$ we have $m_0 = p^2$ and the last displayed equation implies that $T_1(0) = T_0(0)^p$. On the other hand, note that for $n \geqslant 2$ we have $m_{n-1} = p^{n+1} + p^n$, so the last displayed equation with n replaced by $n-1$, combined with Lemma A.5 with $U_{\#}(z) = 1 + A(z)T_0(z)$ and $k = p^n$, shows (A.2) for $n \geqslant 2$. This completes the proof of the lemma. □

Proof of Proposition A.1. Extending K if necessary, assume that K is algebraically closed and complete with respect to $|\cdot|$. Let η in K be such that $\eta^p = \lambda$, so that

$$Q(z) = z(\eta S(z))^p \quad \text{and} \quad \frac{Q(z) - z}{z} = (\eta S(z) - 1)^p.$$

In the case $q \geqslant 2$, it follows that the polynomial Q has no fixed point in $\mathfrak{m}_K \backslash \{0\}$. Thus, in view of Lemma 2.1, to prove that the minimal period of every periodic point of Q in $\mathfrak{m}_K \backslash \{0\}$ is equal to q, we just need to show that for every integer $n \geqslant 1$, every fixed point of Q^{qp^n} in $\mathfrak{m}_K$ is also a fixed point of Q^q. To do this, note that by Lemma A.5 with $U_{\#}(z) = \eta S(z)$ and $k = q$ there is a polynomial $U(z)$ in $\mathcal{O}_K[z]$ such that $Q^q(z) = zU(z)^p$. Our hypothesis $S(0) = 1$ implies that $U(0) = 1$. On the other hand, our hypothesis that $\operatorname{wideg}(S(z) - 1)$ is finite implies that $\operatorname{wideg}(Q)$ and, hence, $\operatorname{wideg}(Q^q)$ are both finite and greater than or equal to 2. In turn, this implies that $\operatorname{wideg}(U(z) - 1)$ is finite and non-zero. Thus the set F of fixed points of Q^q in $\mathfrak{m}_K \backslash \{0\}$ is non-empty and finite, and for each a in F the multiplicity m_a of a as a fixed point of Q^q is finite and divisible by p. Put

$$A(z) := \prod_{a \in F} (z - a)^{m_a/p},$$

https://doi.org/10.1112/S0010437X15007575 Published online by Cambridge University Press

and note that, by applying Lemma 2.4 repeatedly, it follows that there is a polynomial $T_0(z)$ in $\mathcal{O}_K(z)$ such that

$$|T_0(0)| = 1 \quad \text{and} \quad Q^q(z) = z(1 + A(z) \cdot T_0(z))^p.$$

So we can apply Lemma A.4 with $Q_\dagger = Q^q$. We obtain that for each integer $n \geqslant 1$ there is a polynomial $T_n(z)$ in $\mathcal{O}_K[z]$ such that

$$Q^{qp^n}(z) = z(1 + A(z)^{p^n} \cdot T_n(z))^p. \tag{A.6}$$

Moreover, by an induction argument we conclude that for every $n \geqslant 1$ we have $T_n(0) = T_0(0)^{p^n}$. In particular, for every integer $n \geqslant 1$ we have $|T_n(0)| = 1$. This implies that every fixed point Q^{qp^n} in $\mathfrak{m}_K \backslash \{0\}$ is a zero of A and therefore a fixed point of Q^q. Furthermore, for every zero a of A, the multiplicity of $z = a$ as a zero of $Q^{qp^n}(z) - z$ is equal to $p^n m_a$. This completes the proof of the proposition. □

References

Ber90 V. G. Berkovich, *Spectral theory and analytic geometry over non-Archimedean fields*, Mathematical Surveys and Monographs, vol. 33 (American Mathematical Society, Providence, RI, 1990).

Éca75 J. Écalle, *Théorie itérative: introduction à la théorie des invariants holomorphes*, J. Math. Pures Appl. (9) **54** (1975), 183–258.

EEW04a M. Einsiedler, G. Everest and T. Ward, *Morphic heights and periodic points*, in *Number theory (New York, 2003)* (Springer, New York, 2004), 167–177.

EEW04b M. Einsiedler, G. Everest and T. Ward, *Periodic points for good reduction maps on curves*, Geom. Dedicata **106** (2004), 29–41.

Her87 M.-R. Herman, *Recent results and some open questions on Siegel's linearization theorem of germs of complex analytic diffeomorphisms of* $\mathbf{C}^n$ *near a fixed point*, in *VIIIth International congress on mathematical physics (Marseille, 1986)* (World Scientific, Singapore, 1987), 138–184.

HY83 M. Herman and J.-C. Yoccoz, *Generalizations of some theorems of small divisors to non-Archimedean fields*, in *Geometric dynamics (Rio de Janeiro, 1981)*, Lecture Notes in Mathematics, vol. 1007 (Springer, Berlin, 1983), 408–447.

Kea92 K. Keating, *Automorphisms and extensions of* $k((t))$, J. Number Theory **41** (1992), 314–321.

Lan02 S. Lang, *Algebra*, Graduate Texts in Mathematics, vol. 211, third edition (Springer, New York, 2002).

LMS02 F. Laubie, A. Movahhedi and A. Salinier, *Systèmes dynamiques non archimédiens et corps des normes*, Compositio Math. **132** (2002), 57–98.

LS98 F. Laubie and M. Saïne, *Ramification of some automorphisms of local fields*, J. Number Theory **72** (1998), 174–182.

Li96 H.-C. Li, *p-adic periodic points and Sen's theorem*, J. Number Theory **56** (1996), 309–318.

Lin04 K.-O. Lindahl, *On Siegel's linearization theorem for fields of prime characteristic*, Nonlinearity **17** (2004), 745–763.

Lin10 K.-O. Lindahl, *Divergence and convergence of conjugacies in non-Archimedean dynamics*, in *Advances in p-adic and non-Archimedean analysis*, Contemporary Mathematics, vol. 508 (American Mathematical Society, Providence, RI, 2010), 89–109.

Lin13 K.-O. Lindahl, *The size of quadratic p-adic linearization disks*, Adv. Math. **248** (2013), 872–894.

https://doi.org/10.1112/S0010437X15007575 Published online by Cambridge University Press

LR15 K.-O. Lindahl and J. Rivera-Letelier, *Generic parabolic points are isolated in positive characteristic*, Preprint (2015), arXiv:1501.03965v1.

Lub94 J. Lubin, *Non-Archimedean dynamical systems*, Compositio Math. **94** (1994), 321–346.

Lub95 J. Lubin, *Sen's theorem on iteration of power series*, Proc. Amer. Math. Soc. **123** (1995), 63–66.

Mil06 J. Milnor, *Dynamics in one complex variable*, Annals of Mathematics Studies, vol. 160, third edition (Princeton University Press, Princeton, NJ, 2006).

Pér97 R. Pérez-Marco, *Fixed points and circle maps*, Acta Math. **179** (1997), 243–294.

Riv03 J. Rivera-Letelier, *Dynamique des fonctions rationnelles sur des corps locaux*, Astérisque **287** (2003), 147–230; Geometric methods in dynamics. II.

Sen69 S. Sen, *On automorphisms of local fields*, Ann. of Math. (2) **90** (1969), 33–46.

Ser68 J.-P. Serre, *Corps Locaux*, Publications de l'Institut de Mathématique de l'Université de Nancago, No. 8, second edition (Hermann, Paris, 1968).

Win04 J.-P. Wintenberger, *Automorphismes des corps locaux de caractéristique p*, J. Théor. Nombres Bordeaux **16** (2004), 429–456.

Yoc95 J.-C. Yoccoz, *Centralisateurs et conjugaison différentiable des difféomorphismes du cercle*, Astérisque **231** (1995), 89–242; Petits diviseurs en dimension 1.

Karl-Olof Lindahl karl-olof.lindahl@lnu.se
Department of Mathematics, Linnæus University, 351 95, Växjö, Sweden

Juan Rivera-Letelier riveraletelier@mat.puc.cl
Facultad de Matemáticas, Pontificia Universidad Católica de Chile, Avenida Vicuña Mackenna 4860, Santiago, Chile

https://doi.org/10.1112/S0010437X15007575 Published online by Cambridge University Press