1-1-2004

The Growth of Valuations on Rational Function Fields in Two Variables

Edward Mosteig
Loyola Marymount University, emosteig@lmu.edu

Moss Sweedler

PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 132, Number 12, Pages 3473–3483
S 0002-9939(04)07456-8
Article electronically published on July 20, 2004

THE GROWTH OF VALUATIONS ON RATIONAL FUNCTION FIELDS IN TWO VARIABLES

EDWARD MOSTEIG AND MOSS SWEEDLER

(Communicated by Michael Stillman)

ABSTRACT. Given a valuation on the function field $k(x,y)$, we examine the set of images of nonzero elements of the underlying polynomial ring $k[x,y]$ under this valuation. For an arbitrary field k, a Noetherian power series is a map $z : \mathbb{Q} \to k$ that has Noetherian (i.e., reverse well-ordered) support. Each Noetherian power series induces a natural valuation on $k(x,y)$. Although the value groups corresponding to such valuations are well-understood, the restrictions of the valuations to underlying polynomial rings have yet to be characterized. Let Λ_n denote the images under the valuation v of all nonzero polynomials $f \in k[x,y]$ of at most degree n in the variable y. We construct a bound for the growth of Λ_n with respect to n for arbitrary valuations, and then specialize to valuations that arise from Noetherian power series. We provide a sufficient condition for this bound to be tight.

1. INTRODUCTION

Throughout this paper, we denote by $\mathbb{N}$ the set of natural numbers, $\mathbb{Z}$ the set of integers, $\mathbb{Z}^+$ the set of positive integers, and $\mathbb{Q}$ the set of rational numbers. Given $r \in \mathbb{Q}$, we define $r\mathbb{N} = \{rn : n \in \mathbb{N}\}$ and $r\mathbb{Z} = \{rz : z \in \mathbb{Z}\}$. Whenever R is a ring or additive monoid, the set of nonzero elements of R is denoted $R^\star$.

As demonstrated by Zariski in [13], if char $k = 0$ and if a valuation v on $k(x,y)$ has a corresponding value group that can be embedded in $\mathbb{Q}$, then v must come from a series expansion of the form $c_1 t^{e_1} + c_2 t^{e_2} + c_3 t^{e_3} + \cdots$ where $c_i \in k$, $e_i \in \mathbb{Q}$, and $e_i > e_{i+1}$. In [6], Mac Lane and Schilling construct the value group corresponding to such a valuation; that is, they describe the image of the nonzero elements of the function field $k(x,y)$ under a valuation that is given by a series expansion. The purpose of this paper is to illuminate the behavior of the image $\Lambda = \{v(f) : f \in k[x,y]^\star\}$ (called the *value monoid*) of the nonzero elements of the underlying polynomial ring $k[x,y]$ under such a valuation. In this paper, we study $\Lambda_n = \{v(f(x,y)) : f \in k[x,y]^\star \text{ and } \deg_y(f) \leq n\}$ and examine its growth in terms of n.

The results in this paper grew out of a study of the relationship between valuations and Gröbner bases. In [12], Sweedler shows how to generalize the standard algorithms of Gröbner bases by replacing term orders with a valuation that has the following three properties: (i) $v(k^\star) = \{0\}$, (ii) the residue class field of v is k, and (iii) the value monoid Λ is a well-ordered set. The notion that valuations

Received by the editors January 10, 2002 and, in revised form, July 14, 2003.
2000 *Mathematics Subject Classification.* Primary 13F30, 13F25; Secondary 13P10.
Key words and phrases. Valuations, generalized power series, Gröbner bases.

generalize the concept of term orders is made precise in [9], in which conditions are given that describe when a valuation is equivalent to a term order in this context. The next natural step was to study valuations that do not arise from term orders, and so we began with valuations that are defined by series expansions. It turns out that no such valuation is directly linked to a term order, but not all such valuations satisfy properties (i), (ii), and (iii) described above. In particular, there are many such valuations whose corresponding value monoids are not well-ordered (or worse, are not even nonnegative). In fact, Proposition 4.2 of [11] shows that if the valuation v is defined by a series with bounded denominators, then v cannot possibly be well-ordered. Thus we must only consider series with unbounded denominators, a large class of which has been shown to lead to well-ordered value monoids in [10]. To apply the algorithms of [12] to these valuations, we need more information than just the fact that the value monoids are well-ordered. The main result of this paper, that the growth of the sets of the form Λ_n is constant, will provide information about the way in which reduction algorithms from [12] behave. In [8], we will combine results from this paper and [10] to produce a minimal set of generators for the value monoid.

The theory of valuations and generalized Gröbner bases has recently appeared in coding theory, both in terms of code construction and their decoding algorithms. One can study algebraic-geometric codes through the use of valuations in place of algebraic geometry, which essentially comes down to describing a basis for the value monoid. The construction of such codes appears in [11], in which the generators of the corresponding value monoid are computed for a specific example. An alternative description of this construction is given in [3], and we provide more commentary in an example at the end of this paper. Following this example, we pose an open question.

2. Power series and valuations

To construct the valuations described by Zariski in [13], we begin by discussing generalized power series. Given a field k, we define the *support* of a function $z : \mathbb{Q} \to k$ as $\operatorname{Supp}(z) = \{e \in \mathbb{Q} : z(e) \neq 0\}$. So that we may interpret such functions as generalized power series, we use the following formal notation:

$$z = \sum_{e \in \operatorname{Supp}(z)} z(e)t^e. \tag{2.1}$$

We adopt the convention that t is shorthand for the series t^1.

Definition 2.1. A subset $T \subset \mathbb{Q}$ is called *Noetherian* (or reverse well-ordered) if every subset of T has a largest element. We say that a function $f : \mathbb{Q} \to R$ is a *Noetherian power series* if $\operatorname{Supp}(f)$ is Noetherian. We denote the set of all Noetherian power series by $k\langle\langle t^{\mathbb{Q}}\rangle\rangle$.

According to [4], $k\langle\langle t^{\mathbb{Q}}\rangle\rangle$ forms a field where addition is defined pointwise and multiplication is defined via convolution:

$$(f+g)(q) = f(q) + g(q), \qquad (fg)(q) = \sum_{\substack{u,v \in \mathbb{Q} \\ u+v=q}} f(u)g(v).$$

Definition 2.2. A nonzero series $z \in k\langle\langle t^{\mathbb{Q}}\rangle\rangle$ is *simple* if it can be written as $z = \sum_{i=1}^{n} c_i t^{e_i}$, where $c_i \in k^\star$, $n \in \mathbb{Z}^+ \cup \{\infty\}$ and $e_i > e_{i+1}$. A series written in this

form is implicitly assumed to have nonzero coefficients with descending exponents. Write each exponent as $e_i = n_i/d_i$ where $\gcd(n_i, d_i) = 1$. For $i \in \mathbb{Z}^+$, we define $r_i = \operatorname{lcm}(d_1, \ldots, d_i)$ and call $\mathbf{r} = (r_0, r_1, r_2, \ldots)$ the *ramification sequence* of z.

The field of *Laurent series* $k((t))$ consists of all functions from $\mathbb{Z}$ to k with well-ordered support, whereas the field of *reverse Laurent series* $k((t^{-1}))$ is defined as the set of all functions from $\mathbb{Z}$ to k with Noetherian support. Note that we can naturally embed the rational function field in one variable, $k(t)$, into both $k((t))$ and $k((t^{-1}))$. The collection $\bigcup_{r\in\mathbb{Z}^+} k((t^{1/r}))$ is called the field of *Puiseux series* whereas the collection $\bigcup_{r\in\mathbb{Z}^+} k((t^{-1/r}))$ is called the field of *reverse Puiseux series.* Given a Puiseux series (resp., reverse Puiseux series) w, the smallest positive integer r such that $w \in k((t^{1/r}))$ (resp., $w \in k((t^{-1/r}))$) is called the *ramification index* of w.

Puiseux's Theorem states that if k is an algebraically closed field of characteristic zero, then the field of (reverse) Puiseux series is an algebraic closure of the field of (reverse) Laurent series. If k has positive characteristic, then the field of (reverse) Puiseux series is strictly contained in the algebraic closure of the field of (reverse) Laurent series. Kedlaya in [5] produced a characterization of the generalized power series that are algebraic over the Laurent power series field when k has positive characteristic. The result below follows from this characterization.

Theorem 2.3. *Let k be a field, and let $z \in k\langle\langle t^{\mathbb{Q}}\rangle\rangle$ be a simple series. If k has positive characteristic, assume that no term of the ramification sequence of z is divisible by char k. Then z is algebraic over $k((t^{-1}))$ iff z is a reverse Puiseux series.*

Note that the collection of Puiseux series with finite support coincides with the collection of reverse Puiseux series with finite support. The result below follows directly from techniques found in [1] and [2].

Proposition 2.4. *Let k be a field, and let $w = c_1 t^{m_1/n} + \cdots + c_s t^{m_s/n}$ be a finite Puiseux expansion with ramification index n where $m_i \in \mathbb{Z}^\star$, $n \in \mathbb{Z}^+$, and $c_i \in k^\star$. If k has positive characteristic, then assume that n is not divisible by char k. Then the minimal polynomial of w over $k(t)$ is $p(y) = \prod_{i=0}^{n-1}(y - w_i) \in k(t)[y]$, where*

$$w_i = c_1(\zeta^i t^{1/n})^{m_1} + \cdots + c_s(\zeta^i t^{1/n})^{m_s},$$

and ζ is a primitive n^{th} root of unity.

We now provide background information about valuations and demonstrate how to use Noetherian power series to construct a special class of valuations on $k(x, y)$. Let K be a field, $(G, <)$ be an ordered additive abelian group (i.e., $<$ is a total order with $g_1 \leq g_2 \Rightarrow g_1 + h \leq g_2 + h \ \forall g_1, g_2, h \in G$), and let $v : K^\star \to G$ be a group homomorphism where we think of $K^\star$ as the multiplicative subgroup of invertible elements of K. We say v is a *valuation* if it satisfies the strong triangle inequality

$$v(a + b) \leq \max(v(a), v(b)) \quad \text{for } a, b \in K^\star \text{ with } a + b \neq 0,$$

which easily implies $v(a + b) = \max(v(a), v(b))$ for $a, b \in K^\star$ with $v(a) \neq v(b)$.

We chose an order for the triangle inequality in the definition of a valuation above that is the opposite of the conventional order given for Krull valuations. In addition, we use power series with Noetherian support rather than the traditional generalized power series with well-ordered support. Both of these choices were

dictated by the fact that this work grew out of a study of the relationship between valuations, term orders, and filtrations. For more details, see [9].

Definition 2.5. Let v be a valuation on K, and let R be a subring of K. The image $v(K^\star)$ is called the *value group* corresponding to v, and the submonoid $v(R^\star)$ of $v(K^\star)$ is called the *value monoid corresponding to* R.

Definition 2.6. We define $\mathcal{LE} : k\langle\langle t^{\mathbb{Q}}\rangle\rangle^\star \to \mathbb{Q}$ by $\mathcal{LE}(z) = \max\{s : s \in \operatorname{Supp}(z)\}$. We call $\mathcal{LE}(z)$ the *leading exponent* of z.

Note that $\mathcal{LE}(z_1 z_2) = \mathcal{LE}(z_1) + \mathcal{LE}(z_2)$. Moreover, we have $\mathcal{LE}(z_1 + z_2) \leq \max(\mathcal{LE}(z_1), \mathcal{LE}(z_2))$, with equality holding in case $\mathcal{LE}(z_1) \neq \mathcal{LE}(z_2)$. Thus $\mathcal{LE}$ is a valuation on $k\langle\langle t^{\mathbb{Q}}\rangle\rangle$, and so it induces a valuation on any embedding $k(x,y) \hookrightarrow k\langle\langle t^{\mathbb{Q}}\rangle\rangle$. We only consider embeddings of the form $\varphi_z : k(x,y) \hookrightarrow k\langle\langle t^{\mathbb{Q}}\rangle\rangle$ that map $x \mapsto t$, $y \mapsto z$, where t and z are algebraically independent over k. It follows that the composite map $\mathcal{LE} \circ \varphi_z : k(x,y) \to \mathbb{Q}$ is a valuation on $k(x,y)$.

According to Zariski [13], every series $z \in k\langle\langle t^{\mathbb{Q}}\rangle\rangle$ can be written in the form $z = z_\omega + z'$ where z_ω is simple, and every element of $\operatorname{Supp}(z')$ is strictly less than every element of $\operatorname{Supp}(z_\omega)$. Moreover, Mac Lane and Schilling show in [6] that if $f(x,y) \in k(x,y)^\star$, then $\mathcal{LE}(f(t,z)) = \mathcal{LE}(f(t,z_\omega))$ whenever k has characteristic zero. Mac Lane and Schilling also prove that if k has characteristic zero, then the value group $\{\mathcal{LE}(f(t,z)) : f(x,y) \in k(x,y)^\star\}$ is precisely the subgroup of $\mathbb{Q}$ generated by the elements of $\operatorname{Supp}(z) \cup \{1\}$. As previously stated, our goal is to describe the behavior of the value monoid corresponding to $k[x,y]$ under the valuation $\mathcal{LE} \circ \varphi_z$ when k is of arbitrary characteristic.

3. Decomposing simple series

Simple series $z \in k\langle\langle t^{\mathbb{Q}}\rangle\rangle$ may be decomposed into a (possibly infinite) sum of reverse Puiseux series $z_0, z_1, z_2, \ldots$. Given $z \in k\langle\langle t^{\mathbb{Q}}\rangle\rangle$, we define z_0 to consist of all terms of z with integral exponents, and we define $z_1, z_2, \ldots$ inductively. Roughly, if $\mathcal{LE}(z-(z_0+\cdots+z_i)) = n_i/d_i$ for relatively prime n_i, d_i, then collect the terms of $z-(z_0+\cdots+z_i)$ in $k((t^{-1/r_i}))$, where $r_i = \operatorname{lcm}(d_1, \ldots, d_i)$, to form z_{i+1}. This process, which is described more precisely in Algorithm 3.1, insures that if $z_0, \ldots, z_n$ are the first $n+1$ summands in the decomposition of z, then $\sum_{j=0}^{n} z_j$ includes all terms of z whose ramification indices divide the *lcm* of the ramification indices of $z_0, \ldots, z_n$. As an example, if we begin with the series $z = t^{35/2} + t^{37/3} + t^{12} + t^{21/5} + t^4 + t^{1/6}$, it decomposes as the sum of $z_0 = t^{12} + t^4$, $z_1 = t^{35/2}$, $z_2 = t^{37/3} + t^{1/6}$, $z_3 = t^{21/5}$.

We now describe arbitrary countable sums of series. Let $z_1, z_2, z_3, \ldots$ be a (possibly infinite) sequence of elements of $k\langle\langle t^{\mathbb{Q}}\rangle\rangle$ whose supports are pairwise disjoint. Define the sum of $z_1, z_2, z_3, \ldots$ to be the function $S : \mathbb{Q} \to k$ given by

$$S(\lambda) = \begin{cases} z_i(\lambda) & \text{if } \lambda \in \operatorname{Supp}(z_i); \\ 0 & \text{otherwise.} \end{cases}$$

In case $z_1, z_2, z_3, \ldots$ is an infinite sequence, we denote the corresponding sum by $z_1 + z_2 + z_3 + \cdots$, and in case $z_1, z_2, \ldots, z_n$ is a finite sequence with n terms, we denote the sum by $z_1 + z_2 + \cdots + z_n$.

Note that the sum of an infinite sequence of elements of $k\langle\langle t^{\mathbb{Q}}\rangle\rangle$ need not be an element of $k\langle\langle t^{\mathbb{Q}}\rangle\rangle$. Indeed, if $z_n = t^n$, then the support of $z_1 + z_2 + z_3 + \cdots$ is not Noetherian. However, beginning with a simple series $z \in k\langle\langle t^{\mathbb{Q}}\rangle\rangle$, our technique decomposes z as $z = z_1 + z_2 + z_3 + \cdots$, where each z_n is a reverse Puiseux series.

Algorithm 3.1. Let k be a field, and let $z \in k\langle\langle t^{\mathbb{Q}}\rangle\rangle$ be a nonzero simple series $\sum c_i t^{e_i}$ that is written according to Definition 2.2. We define $R_0 = 1$, $z_0 = \sum_{e \in \mathbb{Z} \cap \mathrm{Supp}(z)} z(e)t^e$, and $u_0 = z - z_0$. We now recursively define $z_1, z_2, \ldots$. If $u_n = 0$, then set $z_i = 0$ for all $i > n$. Otherwise, if $u_n \neq 0$, we write

$$\mathcal{L}E(u_n) = a_{n+1}/b_{n+1},$$

where $a_{n+1} \in \mathbb{Z}^\star, b_{n+1} \in \mathbb{Z}^+, \gcd(a_{n+1}, b_{n+1}) = 1$. Then we define

$$\begin{aligned} R_{n+1} &:= \mathrm{lcm}(b_1, \ldots, b_{n+1}), \\ E_{n+1} &:= \mathrm{Supp}(u_n) \cap (1/R_{n+1})\mathbb{Z}, \\ z_{n+1} &:= \sum_{e \in E_{n+1}} z(e)t^e \in k((t^{-1/R_{n+1}})), \\ u_{n+1} &:= u_n - z_{n+1}. \end{aligned}$$

Note that if we begin with a series $z \in k\langle\langle t^{\mathbb{Q}}\rangle\rangle$ and produce $z_0, z_1, z_2, \ldots$ as calculated in the above algorithm, then

$$z = z_1 + z_2 + z_3 + \cdots.$$

We call this the *natural decomposition* of z, and we call $z_0, z_1, z_2, \ldots$ the *components* of the natural decomposition. If this decomposition only has finitely many nonzero components, then we say that the natural decomposition is *finite*. Otherwise, we say that the natural decomposition is *infinite*.

Note that in the natural decomposition of z, the components are reverse Puiseux series since the denominators of elements of the support of z_n are bounded above by R_n. Moreover, if z_n is nonzero and $n > 0$, then $\mathcal{L}E(z_n) > \mathcal{L}E(z_{n+1})$.

Lemma 3.2. *Let k be a field, and let $z \in k\langle\langle t^{\mathbb{Q}}\rangle\rangle$ be a simple series with natural decomposition $z = z_0 + z_1 + z_2 + \cdots$. Given $n \in \mathbb{N}$, if $z_n \neq 0$, then the ramification index of $z_0 + z_1 + \cdots + z_n$ is R_n, where R_n is given in Algorithm 3.1.*

Proof. Define a_i and b_i as in Algorithm 3.1. If $z_n \neq 0$, then $\mathcal{L}E(z_i) = a_i/b_i$ for $1 \leq i \leq n$, and $\mathrm{lcm}(b_1, \ldots, b_n) = R_n$. Thus the ramification index of $z_0 + \cdots + z_n$ is at least R_n. However, every exponent of every term of this sum has a denominator that divides R_n, and so the ramification index is exactly R_n. □

Lemma 3.3. *Let k be a field, and let $z \in k\langle\langle t^{\mathbb{Q}}\rangle\rangle$ be a simple series. If k has positive characteristic, assume that no term of the ramification sequence of z is divisible by char k. The following conditions are equivalent.*

(1) *z is transcendental over $k((t^{-1}))$.*
(2) *z is not a reverse Puiseux series.*
(3) *$\lim R_n = \infty$.*
(4) *z has an infinite natural decomposition.*

Proof. The equivalence of (i) and (ii) is an immediate consequence of Theorem 2.3. The equivalence of (ii) and (iii) follows from the fact that the denominators of the exponents of elements of $\mathrm{Supp}(z)$ are unbounded if and only if $\lim R_n = \infty$. Whenever R_n and R_{n+1} are defined, we have $R_{n+1} > R_n$, and so the equivalence of (iii) and (iv) follows immediately. □

4. Growth of the value monoid

Given a submonoid M of a commutative monoid N, we define an equivalence relation on N by setting $n_1 \sim_M n_2$ if and only if there exist $m_1, m_2 \in M$ such that $m_1 + n_1 = m_2 + n_2$. Denote by N/M the collection of all equivalence classes under this relation, and for $n \in N$, let $\overline{n}$ denote the equivalence class containing n. We define a quotient map from N to N/M that sends n to $\overline{n}$. The set N/M has an additive monoid structure, called the *quotient monoid of N with respect to M*, where we define $\overline{n_1} + \overline{n_2} = \overline{n_1 + n_2}$.

At this point, we concentrate on the case where the quotient monoid N/M is constructed from a valuation. In particular, given a subring A of a field C, we set N to be the value group $v(C^\star)$ and the submonoid M will be $v(A^\star)$.

Lemma 4.1. *Let A be a subring of a field C, and let v be a valuation on C. Given $c \in C, n \in \mathbb{Z}^+$, there is at most one element in*

$$v((Ac^n + Ac^{n-1} + \cdots + Ac + A)^\star)/v(A^\star)$$

that does not lie in

$$v((Ac^{n-1} + \cdots + Ac + A)^\star)/v(A^\star).$$

Proof. Suppose $p, q \in (Ac^n + \cdots + A)^\star$ such that

$$\overline{v(p)}, \overline{v(q)} \notin v((Ac^{n-1} + \cdots + A)^\star)/v(A^\star). \tag{4.1}$$

We must prove that $\overline{v(p)} = \overline{v(q)}$. Write p and q in the form $p = ac^n + P$, $q = bc^n + Q$ with $a, b \in A$ and $P, Q \in Ac^{n-1} + \cdots + Ac + A$. If $a = 0$, then $p = P \in Ac^{n-1} + \cdots + Ac + A$, contradicting (4.1). Similarly, $b \neq 0$.

If $v(bp) = v(aq)$, then $v(b) + v(p) = v(a) + v(q)$. Thus $v(p) \sim_{v(A^\star)} v(q)$, and so $\overline{v(p)} = \overline{v(q)}$.

If $v(bp) \neq v(aq)$, then define w by $w = bp - aq = bP - aQ \in Ac^{n-1} + \cdots + A$. By the strong triangle inequality, $v(w) = \max(v(bp), v(aq))$. Suppose that $v(w) = v(bp)$. Since $v(1) = 0$, we have $v(w) + v(1) = v(b) + v(p)$. Thus $v(w) \sim_{v(A^\star)} v(p)$, and so $\overline{v(w)} = \overline{v(p)}$. However, $\overline{v(w)} \in v(Ac^n + \cdots + A)^\star/v(A^\star)$, which contradicts our assumption in (4.1) that $\overline{v(p)} \notin v((Ac^{n-1} + \cdots + A)^\star)/v(A^\star)$. □

Since $v(A^\star)/v(A^\star)$ is a singleton set, repeated applications of Lemma 4.1 yield the following.

Corollary 4.2. *The set $v((Ac^n + \cdots + Ac + A)^\star)/v(A^\star)$ has cardinality at most $n + 1$.*

Given a polynomial $f(x, y) \in k[x, y]$, define $\deg_y(f(x, y))$ to be the smallest $n \geq 0$ such that $f(x, y) \in k[x]y^n + k[x]y^{n-1} + \cdots + k[x]y + k[x]$. Define

$$\Lambda_n(z) = \{\mathcal{L}E(f(t, z)) \ : \ f \in k[x, y]^\star \text{ and } \deg_y(f(x, y)) \leq n\}.$$

We now provide a bound on the growth of the value monoid with respect to $\deg_y(f(x, y))$ of the polynomials in $k[x, y]$.

Proposition 4.3. *Let k be a field, and let z be a simple series $\sum_{i=1}^{\infty} c_i t^{e_i} \in k\langle\langle t^{\mathbb{Q}} \rangle\rangle$ that is transcendental over $k(t)$.*

(i) *For $n \geq 1$, there is at most one element in $\Lambda_n(z)/\Lambda_0(z)$ that is not in $\Lambda_{n-1}(z)/\Lambda_0(z)$.*
(ii) *The set $\Lambda_n(z)/\Lambda_0(z)$ has cardinality at most $n + 1$.*

Proof. Set $A = k[t], C = k(t, z)$, $c = z$ and note that $\Lambda_0(z) = \mathcal{LE}(A^\star)$ and $\Lambda_n(z) = \mathcal{LE}((Ac^n + \cdots + Ac + A)^\star)$. Then part (i) follows directly from Lemma 4.1, and part (ii) follows directly from Corollary 4.2. □

We will see that this result can be improved if we impose extra conditions on z. In particular, we will show in Theorem 4.10 that if no term of the ramification index of z is divisible by char k and if the equivalent conditions of Lemma 3.3 hold, then the bound given by Proposition 4.3 is tight. To this end, we first exploit the structure of the natural decomposition of z to produce some preliminary results.

Proposition 4.4. *Let k be a field, and let $z \in k\langle\langle t^{\mathbb{Q}}\rangle\rangle$ be a simple series. If k has positive characteristic, assume that no term of the ramification sequence of z is divisible by char k. Suppose z has an infinite natural decomposition $z = z_0 + z_1 + z_2 + z_3 + \cdots$. Define a_i, b_i, and R_i as in Algorithm 3.1. Then for each $n \in \mathbb{N}$ such that $z_n \neq 0$, there exists $f(x, y) \in k[x, y]$ such that $\deg_y(f(x, y)) = R_n$ and*

$$\mathcal{LE}(f(t, z)) = \mathcal{LE}(z_{n+1}) + q/R_n,$$

for some $q \in \mathbb{Z}$.

Proof. Choose n so that $z_n \neq 0$. We begin by computing the minimal polynomial of

$$w_0 := \sum_{\substack{e \in \mathrm{Supp}(z) \\ e > \mathcal{LE}(z_{n+1})}} z(e)t^e$$

over $k(t)$. Since w_0 precisely consists of the terms of z whose support is greater than $\mathcal{LE}(z_{n+1})$,

$$\mathcal{LE}(z - w_0) = \mathcal{LE}(z_{n+1}). \tag{4.2}$$

The ramification index of $z_0 + \cdots + z_n$ is R_n by Lemma 3.2, and so

$$\bigcup_{i=0}^{n} \mathrm{Supp}(z_i) \subset \mathrm{Supp}(z_0 + z_1 + \cdots + z_n) \subset (1/R_n)\mathbb{Z}.$$

However, $\mathrm{Supp}(w_0) \subset \bigcup_{i=0}^{n} \mathrm{Supp}(z_i)$, and so

$$\mathrm{Supp}(w_0) \subset (1/R_n)\mathbb{Z}. \tag{4.3}$$

It is not difficult to see that the ramification index of w_0 is also R_n since its support contains $\mathcal{LE}(z_1), \ldots, \mathcal{LE}(z_n)$. Let ζ be a primitive R_n^{th} root of unity. According to Proposition 2.4, w_0 has minimal polynomial

$$h(t, y) = (y - w_0) \cdots (y - w_{R_n - 1}) \in k(t)[y] \tag{4.4}$$

over $k(t)$, where $w_0, \ldots, w_{R_n - 1}$ are distinct reverse Puiseux series. By choosing an appropriate $g(t) \in k[t]$, we find that $g(t)h(t, y) \in k[t, y]$. Define $f(x, y) \in k[x, y]$ to be the polynomial such that

$$f(t, y) = g(t)h(t, y). \tag{4.5}$$

By (4.4) it is clear that $\deg_y(f(x, y)) = R_n$, and so we only have left to show that $\mathcal{LE}(f(t, z)) = \mathcal{LE}(z_{n+1}) + (q/R_n)$ for some $q \in \mathbb{Z}$.

We now demonstrate that $\mathcal{LE}(z - w_j) \in (1/R_n)\mathbb{Z}$ for $1 \leq j \leq R_n - 1$. Each element of $\mathrm{Supp}(w_j)$ is greater than $\mathcal{LE}(z_{n+1})$, and so

$$\mathcal{LE}(z - w_j) \geq \mathcal{LE}(z_{n+1}). \tag{4.6}$$

Suppose, for contradiction, that equality holds in (4.6). Then the terms of z whose exponents lie above $\mathcal{L}E(z_{n+1})$ must identically agree with the terms of w_j. Moreover, w_0 consists precisely of the terms of z whose exponents lie above $\mathcal{L}E(z_{n+1})$, and so $w_j = w_0$. However, this is only possible if $j = 0$, a contradiction. Therefore, the inequality (4.6) is strict, and so by (4.3),

$$\mathcal{L}E(z - w_j) \in \mathrm{Supp}(w_j) = \mathrm{Supp}(w_0) \subset (1/R_n)\mathbb{Z}.$$

Substituting z for y in (4.4) and (4.5), we obtain $h(t,z) = (z - w_0)\cdots(z - w_{R_n-1})$ and $f(t,z) = g(t)h(t,z)$. Using these equations in conjunction with (4.2), we compute

$$\begin{aligned}\mathcal{L}E(f(t,z)) = \mathcal{L}E(g(t)h(t,z)) &= \mathcal{L}E(g(t)) + \mathcal{L}E(z - w_0) + \sum_{i=1}^{R_n-1} \mathcal{L}E(z - w_j) \\ &= \mathcal{L}E(g(t)) + \mathcal{L}E(z_{n+1}) + \sum_{i=1}^{R_n-1} \mathcal{L}E(z - w_j).\end{aligned}$$

Since $\mathcal{L}E(g(t)) \in \mathbb{Z}$ and $\mathcal{L}E(z - w_j) \in (1/R_n)\mathbb{Z}$ for all $1 \le j \le R_n - 1$ by (4), we have $\mathcal{L}E(g(t)) + \sum_{i=1}^{R_n-1} \mathcal{L}E(z - w_j) = q/R_n$ for some $q \in \mathbb{Z}$, and so $\mathcal{L}E(f(t,z)) = \mathcal{L}E(z_{n+1}) + q/R_n$. □

Definition 4.5. The set of integers $\{a_0, \ldots, a_{m-1}\}$ forms a *complete set of residues* modulo m if for any integer a, there exists $0 \le j \le m-1$ such that m divides $a - a_j$.

We quote the following simple result of number theory without proof.

Lemma 4.6. *Suppose $\{a_0, \ldots, a_{m-1}\}$ forms a complete set of residues modulo m. Given two relatively prime nonzero integers r, s, the set*

$$\{ir + a_j s \ : \ 0 \le i \le s-1, \ 0 \le j \le m-1\}$$

forms a complete set of residues modulo ms.

Lemma 4.7. *Let k be a field, and let $f_0, \ldots, f_{m-1} \in k[x,y]$ such that $\deg_y(f_i) = i$. Suppose $v : k(x,y) \to \mathbb{Q}$ is a valuation such that $\{mv(f_0), \ldots, mv(f_{m-1})\}$ forms a complete set of residues modulo m. Suppose $f_m \in k[x,y]$ such that $\deg_y(f_m) = m$ and $v(f_m) = a/b$ where a and b are relative prime integers with b positive. Let $L = \mathrm{lcm}(m,b)$. If $L > m$, then there exist $f_{m+1}, \ldots, f_{L-1} \in k[x,y]$ such that $\deg_y(f_i) = i$ and*

$$\{Lv(f_0), \ldots, Lv(f_{L-1})\}$$

forms a complete set of residues modulo L.

Proof. To simplify the notation in this proof, given $a, b \in \mathbb{Z}^+$, we denote their least comon multiple and greatest common divisor by $[a,b]$ and (a,b), respectively. Using the identity $(m/(b,m), b/(b,m)) = 1$ in conjunction with the assumption $(a,b) = 1$, it follows that $(ma/(b,m), b/(b,m)) = 1$, and so

$$\Big(\frac{La}{b}, \frac{L}{m}\Big) = \Big(\frac{[b,m]a}{b}, \frac{[b,m]}{m}\Big) = \Big(\frac{ma}{(b,m)}, \frac{b}{(b,m)}\Big) = 1.$$

By Lemma 4.6 with $a_j = mv(f_j)$, $r = La/b$, $s = L/m$, we see that

$$\Big\{i\Big(\frac{La}{b}\Big) + mv(f_j)\Big(\frac{L}{m}\Big) \ : \ 0 \le i \le (L/m) - 1, \ 0 \le j \le m-1\Big\}$$

forms a complete set of residues modulo L.

For $0 \leq i \leq (L/m) - 1$, $0 \leq j \leq m - 1$, we define $f_{mi+j} = (f_m)^i f_j$. It follows that $\deg_y(f_{mi+j}) = mi + j$ and

$$Lv(f_{mi+j}) = L(iv(f_m) + v(f_j)) = i\Big(\frac{La}{b}\Big) + mv(f_j)\Big(\frac{L}{m}\Big).$$

Thus, $\{Lv(f_0), \ldots, Lv(f_{L-1})\}$ forms a complete set of residues modulo L. □

Here we state another simple result of elementary number theory without proof.

Lemma 4.8. *Suppose n_1/d_1 and n_2/d_2 are rational numbers written in reduced form and $n_1/d_1 - n_2/d_2 = q/r$ where q/r is not assumed to be written in reduced form. Then* $\operatorname{lcm}(d_1, r) = \operatorname{lcm}(d_2, r)$.

For each $n \in \mathbb{N}$, we generate a polynomial $f_n(x, y)$ such that $\deg_y(f_n(x, y)) = n$, and $\mathcal{LE}(f_n(t, z))$ is not equivalent to the images of any of the other polynomials mod $\mathbb{N}$.

Lemma 4.9. *Let k be a field, and let $z \in k\langle\langle t^{\mathbb{Q}}\rangle\rangle$ be a simple series. If k has positive characteristic, assume that no term of the ramification sequence of z is divisible by char k. Suppose z has an infinite natural decomposition $z = z_0 + z_1 + z_2 + \cdots$. Define R_i as in Algorithm 3.1. Then there exist polynomials $f_0, \ldots, f_{R_n - 1} \in k[x, y]$ such that $\deg_y(f_i(x, y)) = i$ and*

$$\{R_n \mathcal{LE}(f_i(t, z)) : \ 0 \leq i \leq R_n - 1\}$$

is a complete set of residues modulo R_n.

Proof. We prove the result by induction on n. When $n = 0$, set $f_0(x, y) = x$, and the result follows.

The least common multiple of the denominators of the $\mathcal{LE}(f_i(t, z))$'s (when written as fractions in reduced form) is R_n since $R_n \mathcal{LE}(f_i(t, z))$ is congruent to 1 modulo R_n for some choice of i. According to Proposition 4.4 there exists $f(x, y) \in k(x, y)$ such that $\deg_y(f(x, y)) = R_n$ and $\mathcal{LE}(f(t, z)) = \mathcal{LE}(z_{n+1}) + q/R_n$, where $q \in \mathbb{Z}$. Let a/b be the reduced form of $\mathcal{LE}(f(t, z))$ and a_{n+1}/b_{n+1} be the reduced form of $\mathcal{LE}(z_{n+1})$. If we set $n_1 = a$, $n_2 = a_{n+1}$, $d_1 = b$, $d_2 = b_{n+1}$, $q = q$, $r = R_n$, then by Lemma 4.8, we have $\operatorname{lcm}(b, R_n) = \operatorname{lcm}(b_{n+1}, R_n) = R_{n+1}$.

Thus, by setting $v = \mathcal{LE}$, $m = R_n$, $f_m = f$ in Lemma 4.7, we get polynomials $f_0, \ldots, f_{R_{n+1}-1} \in k(x, y)$ such that $\deg_y(f_i(x, y)) = i$ and $\{R_{n+1} \mathcal{LE}(f_i(t, z)) : \ 0 \leq i \leq R_{n+1} - 1\}$ is a complete set of residues modulo R_{n+1}. □

We conclude by showing that the bound given by Proposition 4.3 is tight when we impose extra conditions on the series $z \in k\langle\langle t^{\mathbb{Q}}\rangle\rangle$.

Theorem 4.10. *Let k be a field, and let $z \in k\langle\langle t^{\mathbb{Q}}\rangle\rangle$ be a simple series. If k has positive characteristic, assume that no term of the ramification sequence of z is divisible by char k. Suppose furthermore that z is not a reverse Puiseux series. Then for $1 \leq n \in \mathbb{Z}$, the quotient Λ_n/Λ_0 has cardinality one greater than that of Λ_{n-1}/Λ_0, or equivalently, Λ_n/Λ_0 has cardinality $n + 1$.*

Proof. Define R_n as in Algorithm 3.1. By Proposition 3.3, the natural decomposition is infinite. Therefore, the result holds for $r = R_n - 1$ because by Lemma 4.9, the cardinality of $\Lambda_{R_n - 1}/\Lambda_0$ is R_n. Note that by Proposition 3.3, $R_n - 1$ gets arbitrarily large. According to Proposition 4.3, Λ_r/Λ_0 has cardinality at most $r+1$. Suppose for some $s \in \mathbb{N}$ that Λ_s/Λ_0 has cardinality less than or equal to s. By

Proposition 4.3 and induction it follows that for any $t \in \mathbb{N}$ the set Λ_{s+t}/Λ_0 has cardinality less than or equal to $s+t$. But there exists an n such that $R_n - 1 \geq s$ and the cardinality of $\Lambda_{R_n-1}/\Lambda_0$ is R_n. This contradiction shows that there is no $s \in \mathbb{N}$ such that Λ_s/Λ_0 has cardinality less than or equal to s. □

Example 4.11. In Example 5.2 of [11], O'Sullivan generates a valuation on $k(x,y)$ by a series of blow-ups. The valuation in this example alternatively can be described in terms of power series by selecting

$$z = t^2 + \sum_{j=1}^{\infty} 2^{(1-j)} t^{(1+2^{-j})} = t^2 + t^{3/2} + (1/2)t^{5/4} + (1/4)t^{9/8} + (1/8)t^{17/16} + \cdots \tag{4.7}$$

and sending $x \mapsto t, y \mapsto z$. O'Sullivan determines that $1, \frac{3}{2}, \frac{11}{4}, \frac{43}{8}$, and $\frac{171}{16}$ are among the generators of the value monoid, further claiming that the value monoid is infinitely generated, though he states that the proof is fairly long and thus omitted. Now, according to Theorem 4.10, this claim holds true not only for the series given in (4.7), but rather for any series $z \in k\langle\langle t^{\mathbb{Q}} \rangle\rangle$ satisfying the conditions required by Theorem 4.10. In fact, Theorem 4.10 (in conjunction with the proof of Proposition 4.4) provides a method for constructing infinitely many generators of the value monoid that cannot be generated by a finite set. Moreover, as stated in the introduction, by utilizing Theorem 4.10 and results from [10], it is possible to create an algorithm that produces a minimal set of generators for the value monoid generated by an arbitrary series $z \in k\langle\langle t^{\mathbb{Q}} \rangle\rangle$. This is useful both for purposes of code construction and decoding algorithms.

One should naturally question the necessity of the extra condition imposed on $z \in k\langle\langle t^{\mathbb{Q}} \rangle\rangle$ in Theorem 4.10 in case k has positive characteristic. In contrast, Proposition 4.3 provides a characteristic-free upper bound on the growth of valuations, and so we leave it as an open question to determine the extent of the necessity of the condition required by Theorem 4.10.

References

1. S. S. Abhyankar and T. T. Moh, Newton-Puiseux expansion and generalized Tschirnhausen transformation, part 1, *J. Reine Angew. Math* **260** (1973) 47–83. MR 49:2724
2. Dominique Duval, Rational Puiseux Series, *Compositio Mathematica* **70** (1989) 119–154. MR 90c:14001
3. Olav Geil and Ruud Pellikaan, On the Structure of Order Domains, *Finite Fields and Their Applications* **9** (2002) 369–396. MR 2003i:13034
4. H. Hahn, Über die nichtarchimedischen Größensysteme, *Sitz. Akad. Wiss. Wien* **116** (1907) 601–655.
5. Kiran Kedlaya, The Algebraic Closure of the Power Series Field in Positive Characteristic, *Proceedings of the American Mathematical Society* **129** (2001) 3461–3470. MR 2003a:13025
6. Saunders Mac Lane and O.F.G. Schilling, Zero-Dimensional Branches of Rank One on Algebraic Varieties, *Annals of Mathematics* **40** (1939) 507–520. MR 1:26c
7. Edward Mosteig, *A Valuation-Theoretic Approach to Polynomial Computations*, Doctoral Thesis, Cornell University, 2000.
8. Edward Mosteig, Value Monoids of Zero-Dimensional Valuations of Rank One, in preparation.
9. Edward Mosteig and Moss Sweedler, Valuations and Filtrations, *Journal of Symbolic Computation* **34** (2002), no. 5, 399-435. MR 2003j:12008
10. Edward Mosteig, Computing Leading Exponents of Noetherian Power Series, *Communications in Algebra* **30** (2002) 6055–6069. MR 2003j:13030
11. Michael E. O'Sullivan, New Codes for the Berlekamp-Massey-Sakata Algorithm, *Finite Fields and Their Applications* **7** (2001) 293–317. MR 2002b:94050

12. Moss Sweedler, Ideal Bases and Valuation Rings, manuscript, 1986, available at http://math.usask.ca/fvk/Valth.html.
13. Oscar Zariski, The reduction of the singularities of an algebraic surface, *Annals of Mathematics* **40** (1939) 639–689. MR 1:26d

Department of Mathematics, Loyola Marymount University, Los Angeles, California 90045
E-mail address: emosteig@lmu.edu

Department of Mathematics, Cornell University, Ithaca, New York 14853
E-mail address: moss_sweedler@cornell.edu