MARCEL DEKKER, INC. • 270 MADISON AVENUE • NEW YORK, NY 10016

COMMUNICATIONS IN ALGEBRA®
Vol. 30, No. 12, pp. 6055–6069, 2002

COMPUTING LEADING EXPONENTS OF NOETHERIAN POWER SERIES

Edward Mosteig*

Department of Mathematics, Tulane University, 6823 Saint Charles Avenue, New Orleans, LA 70118

ABSTRACT

For a field k of characteristic zero, we study the field of Noetherian power series, $k\langle\langle t^{\mathbb{Q}}\rangle\rangle$, which consists of maps $z : \mathbb{Q} \to k$ whose supports are Noetherian (i.e., reverse well-ordered) subsets of $\mathbb{Q}$. There is a canonical valuation $\mathcal{L}E : k\langle\langle t^{\mathbb{Q}}\rangle\rangle \to \mathbb{Q} \cup \{-\infty\}$ that sends a nonzero series to the maximum element of its support. Given a nonzero polynomial $f(x, y) \in k[x, y]$ and a series $z \in k\langle\langle t^{\mathbb{Q}}\rangle\rangle$ that is transcendental over $k(t)$, we construct a formula for $\mathcal{L}E(f(t, z))$ in terms of the roots of $f(t, y) \in k(t)[y]$. Using this formula, we find sufficient conditions for $\{\mathcal{L}E(f(t, z)) : f(x, y) \in k[x, y]^\star\}$ to be a well-ordered subset of $\mathbb{Q}$. In particular, this set is well-ordered in case the support of z consists solely of positive numbers.

*Current address: Loyola Marymount University, Department of Mathematics, One LMU Drive, Suite 2700, Los Angeles, CA 90045. E-mail: emosteig@lmu.edu

DOI: 10.1081/AGB-120016031 0092-7872 (Print); 1532-4125 (Online)

1 INTRODUCTION

Moss Sweedler developed a theory of generalized Gröbner bases using valuation theory in an unpublished manuscript.[12] Instead of using term orders, he relies on valuation rings in $k(\mathbf{x}) = k(x_1, \ldots, x_n)$ that are positioned appropriately with respect to the underlying polynomial ring $k[\mathbf{x}] = k[x_1, \ldots, x_n]$. The first class of valuation rings that can be used in this context were described in earlier work by the present authors.[6,8] This paper studies and extends this class by using different techniques.

A *valuation* on a field F is a map $v\colon F \to G \cup \{-\infty\}$, where G is an ordered abelian group, that satisfies the following three properties:

(i) $v(f) = -\infty$ if and only if $f = 0$,
(ii) $v(fg) = v(f) + v(g)$,
(iii) $v(f+g) \leq \max\{v(f), v(g)\}$.

If v is a valuation then the map $F \to G \cup \{\infty\}$ given by $f \mapsto -v(f)$ is a valuation as defined by Krull.[3] One of the most important necessary conditions for v to be suitable for use in the context of Sweedler's work is the following:

$$\{v(f(\mathbf{x})) : f(\mathbf{x}) \in k[\mathbf{x}]^\star\} \text{ must be a well-ordered subset of } G.$$

Since our work is closely related to Gröbner bases, it turns out that the valuations defined above are more compatible with these studies than are Krull valuations. Note that the axioms above for a valuation are satisfied when replacing v by 'leading term' with respect to a fixed term order.

Although Gröbner bases formed the original motivation for this paper, the results herein may have other applications. Since well-orderedness is a generally useful property, it is possible that proofs in other areas may depend on these results. Examples of proofs and techniques that utilize well-orderedness include Fermat's method of infinite descent in number theory and the proof of the validity of Buchberger's criterion in computational commutative algebra.

In this paper, we focus on a class of valuations on $k(x, y)$ where k is a field of characteristic zero. In particular, we consider valuations that arise from (Noetherian) generalized power series as discussed by Zariski[13] and MacLane and Schilling.[5] For a suitable choice of $z \in k\langle\langle t^{\mathbb{Q}}\rangle\rangle$, we can embed $k(x, y)$ in $k\langle\langle t^{\mathbb{Q}}\rangle\rangle$ via $x \mapsto t^1$, $y \mapsto z$ (where t^1 denotes the map $\mathbb{Q} \to k$ that sends 1 to 1 and all other numbers to 0). The natural valuation $\mathcal{LE}\colon k\langle\langle t^{\mathbb{Q}}\rangle\rangle \to \mathbb{Q}$ given in Definition 2.1 induces a valuation on $k(x, y)$. The focus of this paper (see Theorem 5.1) is to determine conditions that guarantee

$$\{\mathcal{LE}(f(t^1, z)) : f(x, y) \in k[x, y]^\star\}$$

is a well-ordered subset of $\mathbb{Q}$. Traditionally, generalized power series are defined to have well-ordered support rather than Noetherian support. Our decision to use series with Noetherian support is due to the connections of this work with the theory of Gröbner bases.[8,12]

2 LEADING EXPONENTS

In this section, we introduce some of the key objects that are of importance to us. We begin with the following notational conventions which will be used throughout the paper. We denote by $\mathbb{Q}^+$ the set of nonnegative rational numbers. Given $r \in \mathbb{Q}$, we define $r\mathbb{Z} = \{rz : z \in \mathbb{Z}\}$ and $r\mathbb{N} = \{rn : n \in \mathbb{N}\}$. Whenever R is a ring or monoid, we denote by $R^\star$ the nonzero elements of R.

Let $(T, \leq)$ be a totally ordered set. We say that T is *well-ordered* if every subset of T has a smallest element. We say that T is *Noetherian* (or *reverse well-ordered*) if every subset of T has a largest element.

Given a function $z : \mathbb{Q} \to k$, the *support* of z is defined by $\mathrm{Supp}(z) = \{r \in \mathbb{Q} : z(r) \neq 0\}$. The collection of *Noetherian power series*, denoted by $k\langle\langle t^{\mathbb{Q}} \rangle\rangle$, consists of all functions from $\mathbb{Q}$ to k with Noetherian support. As demonstrated by Hahn, this collection of functions forms a field in which addition is defined pointwise and multiplication is defined via convolution.[4] More precisely, if $z_1, z_2 \in k\langle\langle t^{\mathbb{Q}} \rangle\rangle$ and $q \in \mathbb{Q}$, then

$$(z_1 + z_2)(q) = z_1(q) + z_2(q),$$
$$(z_1 z_2)(q) = \sum_{\substack{u,v \in \mathbb{Q} \\ u+v=q}} z_1(u) z_2(v).$$

Since $\mathrm{Supp}(z_1)$ and $\mathrm{Supp}(z_2)$ are Noetherian, for any given $q \in \mathbb{Q}$, there are only finitely many pairs $u, v \in \mathbb{Q}$ such that $u + v = q$ and $f(u)g(v) \neq 0$, and so the above multiplication is well-defined.[9–11] Symbolically, it is convenient to denote a Noetherian power series as a sum:

$$z = \sum_{s \in \mathrm{Supp}(z)} z(s) t^s,$$

where $z(s)$ denotes the image of s under z. A typical example of a Noetherian power series is the function $z : \mathbb{Q} \to k$ given by

$$z(q) = \begin{cases} 1 & \text{if } \ q = 2^{-n} \text{ or } q = 2^{-n} - 1 \text{ for some } n \in \mathbb{N}^\star; \\ 0 & \text{otherwise.} \end{cases}$$

This function can be represented as a formal sum:

$$z = (t^{1/2} + t^{1/4} + t^{1/8} + \cdots) + (t^{-1/2} + t^{-3/4} + t^{-7/8} + \cdots). \quad (1)$$

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

Definition 2.1. *We define* $\mathcal{L}E : k\langle\langle t^{\mathbb{Q}}\rangle\rangle \to \mathbb{Q} \cup \{-\infty\}$ *by*

$$\mathcal{L}E(z) = \begin{cases} \max\{s : s \in \mathrm{Supp}(z)\} & \text{if } z \neq 0; \\ -\infty & \text{if } z = 0. \end{cases}$$

We call $\mathcal{L}E(z)$ *the leading exponent of* z.

Note that $\mathcal{L}E(z_1 z_2) = \mathcal{L}E(z_1) + \mathcal{L}E(z_2)$. Moreover, we have the following *strong triangle inequality*:

$$\mathcal{L}E(z_1 + z_2) \leq \max(\mathcal{L}E(z_1), \mathcal{L}E(z_2)),$$

with equality holding in case $\mathcal{L}E(z_1) \neq \mathcal{L}E(z_2)$.

Now $\mathcal{L}E$ yields a valuation on the rational function field in two variables. Indeed, we have natural embedding $\varphi : k(x, y) \hookrightarrow k\langle\langle t^{\mathbb{Q}}\rangle\rangle$ that maps $x \mapsto t$, $y \mapsto z$, where t and z are algebraically independent over k, i.e., z is transcendental over $k(t)$. By the comments following Theorem 5.1, we will see that there are many Noetherian series that are transcendental over $k(t)$. Using this embedding, it follows that the composite map $\mathcal{L}E \circ \varphi : k(x, y) \to \mathbb{Q}$ is a valuation on $k(x, y)$. To provide valuations that are suitable for use in the theory developed by Sweedler,[12] we give conditions in Sec. 5 that guarantee

$$\{\mathcal{L}E(f(t, z)) : f(x, y) \in k[x, y]^{\star}\}$$

is a well-ordered subset of $\mathbb{Q}$.

3 PUISEUX SERIES

Although we are interested in the leading exponents of series taken from $k\langle\langle t^{\mathbb{Q}}\rangle\rangle$, it is first necessary to study various subrings of $k\langle\langle t^{\mathbb{Q}}\rangle\rangle$. We can identify the polynomial ring $k[t]$ with the subring of $k\langle\langle t^{\mathbb{Q}}\rangle\rangle$ consisting of all series $z \in k\langle\langle t^{\mathbb{Q}}\rangle\rangle$ such that $\mathrm{Supp}(z)$ is a finite subset of $\mathbb{N}$. It immediately follows that the rational function field $k(t)$ can be embedded in $k\langle\langle t^{\mathbb{Q}}\rangle\rangle$. The field of *reverse Laurent series* $k\langle\langle t\rangle\rangle$ is defined as the set of all functions from $\mathbb{Z}$ to k with Noetherian support.

The algebraic closure of the field of reverse Laurent series can be described by Puiseux's Theorem. Although the classical formulation of this theorem deals with series that have well-ordered support rather than Noetherian support, the following statement is similar to that found in any standard textbook.[1]

Theorem 3.1 (Puiseux's Theorem)**.** *If k is an algebraically closed field of characteristic zero, then the field of reverse Puiseux series defined by $\cup_{r\in\mathbb{N}^\star} k\langle\langle t^{1/r}\rangle\rangle$ is an algebraic closure of $k\langle\langle t\rangle\rangle$.*

Definition 3.2. *Given a reverse Puiseux series w, the smallest positive integer r such that $w \in k\langle\langle t^{1/r}\rangle\rangle$ is called the ramification index of w.*

We have the following inclusions:

$$k(t) \subset k\langle\langle t\rangle\rangle \subset \bigcup_{r\in\mathbb{N}^\star} k\langle\langle t^{1/r}\rangle\rangle \subset k\langle\langle t^{\mathbb{Q}}\rangle\rangle.$$

Definition 3.3. *A series $z \in k\langle\langle t^{\mathbb{Q}}\rangle\rangle$ is said to be infinite if* $\mathrm{Supp}(z)$ *is an infinite subset of $\mathbb{Q}$.*

Definition 3.4. *We say that $z \in k\langle\langle t^{\mathbb{Q}}\rangle\rangle$ is bounded if* $\mathrm{Supp}(z)$ *is a bounded subset of $\mathbb{Q}$. In this case, we call the greatest lower bound (in $\mathbb{R}$) of* $\mathrm{Supp}(z)$ *the limit of z.*

Definition 3.5. *We say that a nonzero series $z \in k\langle\langle t^{\mathbb{Q}}\rangle\rangle$ is simple if it can be written in the form*

$$z = \sum_{i=1}^{n} c_i t^{e_i},$$

where $c_i \in k^\star, n \in \mathbb{N}^\star \cup \{\infty\}, e_i \in \mathbb{Q}, e_i > e_{i+1}$. Whenever we write a series in this form, we implictly assume that each c_i is nonzero and the e_i's are written in descending order. We call $\mathbf{e} = (e_1, e_2, \ldots)$ the exponent sequence of z and write each exponent as $e_i = n_i/d_i$ where $n_i \in \mathbb{Z}$, $d_i \in \mathbb{N}^\star$, $\gcd(n_i, d_i) = 1$. *(In case $n_i = 0$, we set $d_i = 1$.) We call $\mathbf{n} = (n_1, n_2, \ldots)$ the numerator sequence of z and $\mathbf{d} = (d_1, d_2, \ldots)$ the denominator sequence of z.*

Definition 3.6. *Let $z \in k\langle\langle t^{\mathbb{Q}}\rangle\rangle$ be a simple series written as in Definition* 3.5. *We define $z^{(0)} = 0$. Let $m \in \mathbb{N}^\star$. If* $\mathrm{Supp}(z)$ *has at most m elements, then we define $z^{(m)} = z$. If* $\mathrm{Supp}(z)$ *has more than m elements, we define $z^{(m)} = c_1 t^{e_1} + \cdots + c_m t^{e_m}$.*

Definition 3.7. *Let $z_1, z_2 \in k\langle\langle t^{\mathbb{Q}}\rangle\rangle$. If $z_1^{(m)} = z_2^{(m)}$ for all $m \in \mathbb{N}^\star$, then we say that z_1 and z_2 agree to infinite order. If $z_1^{(m)} = z_2^{(m)}$ but $z_1^{(m+1)} \neq z_2^{(m+1)}$ for* *some $m \in \mathbb{N}$, we say that z_1 and z_2 agree to order m. Thus two series z_1 and z_2 agree to order m if their first m terms are the same, but their $(m+1)$st terms are different.*

MacLane and Schilling argue that if $z_1, z_2 \in k\langle\langle t^{\mathbb{Q}}\rangle\rangle$ are two series that agree to infinite order, then for any $f(x,y) \in k[x,y]^\star$, $\mathcal{L}E(f(t,z_1)) = \mathcal{L}E(f(t,z_2))$.[5] Now for any series $z \in k\langle\langle t^{\mathbb{Q}}\rangle\rangle$, there exists a unique simple series $z_\omega \in k\langle\langle t^{\mathbb{Q}}\rangle\rangle$ such that z and z_ω agree to infinite order.[5,8] For example, if z is given by (1), then

$$z_\omega = t^{1/2} + t^{1/4} + t^{1/8} + \cdots.$$

Thus for our purposes it suffices to restrict our study that of simple series.

Definition 3.8. *Let $z \in k\langle\langle t^{\mathbb{Q}}\rangle\rangle$ be a simple series with infinite support, written as in Definition 3.5. We define $r_0 = 1$ and for $m \geq 1$, we define r_m to be the ramification index of $z^{(m)}$, and call $\mathbf{r} = (r_0, r_1, r_2, \ldots)$ the ramification sequence of z.*

Example 3.9. Consider the series

$$z = t^{1/2} + t^{1/3} + t^{1/5} + \cdots.$$

This series has exponent sequence $(1/2, 1/3, 1/5, \ldots)$, numerator sequence $(1, 1, 1, \ldots)$, denominator sequence $(2, 3, 5, \ldots)$, and ramification sequence $(1, 2, 6, 30, \ldots)$.

We state the following simple lemma without proof.

Lemma 3.10. *Let $z \in k\langle\langle t^{\mathbb{Q}}\rangle\rangle$ be a simple series with infinite support. If $\mathbf{d}$ is the denominator sequence of z and $\mathbf{r}$ is the ramification sequence of z, then for $m \geq 1$, $r_m = \operatorname{lcm}(d_1, \ldots, d_m)$.*

Note that $z \in k\langle\langle t^{\mathbb{Q}}\rangle\rangle$ is reverse Puiseux if and only its ramification series eventually stabilizes. Puiseux's theorem states that any reverse Puiseux series w is algebraic over $k\langle\langle t\rangle\rangle$. The following result tells us how to construct the minimal polynomial of w over $k\langle\langle t\rangle\rangle$.[2]

Proposition 3.11. *Let k be an algebraically closed field of characteristic zero. Suppose*

$$w = \sum_{j=1}^{n} c_j t^{e_j} = \sum_{j=1}^{n} c_j t^{n_j/d_j}$$

is a Puiseux series of ramification index r and is written in the form according to Definition 3.5. *Then the minimal polynomial of w over* $k\langle\langle t\rangle\rangle$ *is* $\prod_{i=1}^{r}(y-w_i)\in k\langle\langle t\rangle\rangle[y]$ *where*

$$w_i=\sum_{j=1}^{n}c_j(\zeta^i t^{1/r})^{(rn_j/d_j)},\quad 1\le i\le r,$$

and ζ *is a primitive rth root of unity. Note that the conjugate* w_r *is simply w itself.*

4 LEADING EXPONENTS OF MINIMAL POLYNOMIALS OF SKEW PUISEUX SERIES

In this section, k is an algebraically closed field of characteristic zero and $z\in k\langle\langle t^{\mathbb{Q}}\rangle\rangle$ is a simple series written as in Definition 3.5. We make the assumption in this section that z is transcendental over $k(t)$.

Given $f(x,y)\in k[x,y]^{\star}$, we can think of $f(t,y)$ as an element of $k\langle\langle t\rangle\rangle[y]$ and then factor $f(t,y)$ as $f(t,y)=q(t)p_1(y)\cdots p_s(y)$ where $q(t)\in k[t]$ and each $p_i(y)$ is a monic irreducible polynomial in $k\langle\langle t\rangle\rangle[y]$. Since $\mathcal{LE}(f(t,z))=\mathcal{LE}(g(t))+\sum_{i=1}^{s}p_i(z)$ and $\mathcal{LE}(g(t))=\deg(g(t))$, we need to compute $\mathcal{LE}(p_i(z))$ for each i in order to construct a formula for $\mathcal{LE}(f(t,z))$. The purpose of this section is to compute $\mathcal{LE}(p_i(z))$ for each irreducible factor $p_i(y)$. Since $p_i(y)\in k\langle\langle t\rangle\rangle[y]$ is a monic irreducible polynomial, it is the minimal polynomial of some reverse Puiseux series.

Let w be a reverse Puiseux series of ramification index R that is algebraic over $k(t)$ (and hence is algebraic over $k\langle\langle t\rangle\rangle$), and let $p(y)\in k\langle\langle t\rangle\rangle[y]$ be the minimal polynomial of w over $k\langle\langle t\rangle\rangle$. We write $p(y)$ in the form $\prod_{i=1}^{R}(y-w_i)$, as given by Proposition 3.11. Since z is transcendental over $k(t)$ and w is algebraic over $k(t)$, we know that they cannot be the same, and so they must agree to some finite order. Choose m to be the smallest positive integer such that each of the roots $w_1,\dots,w_R$ agrees with z to an order of at most m. By permuting the roots, we assume without loss of generality than w agrees with z to order m.

Notation 4.1. In summary, we make the following assumptions throughout this section.

- $z\in k\langle\langle t^{\mathbb{Q}}\rangle\rangle$ is transcendental over $k(t)$ with exponent, numerator, denominator, and ramification sequences **e**, **n**, **d**, and **r**.
- w is a reverse Puiseux series that is algebraic over $k(t)$ and has ramification index R.

- w has minimal polynomial $\prod_{i=1}^{R}(y - w_i)$ over $k\langle\langle t\rangle\rangle$ in which the conjugates of w are written according to Proposition 3.11.
- z and w agree to order m, and no conjugate of w agrees with z to an order greater than m.

To obtain a formula for $\mathcal{LE}(p(z))$ in terms of the exponents of z and w (see Proposition 4.6), we first prove some preliminary results concerning the conjugates of w over $k\langle\langle t\rangle\rangle$.

Lemma 4.2. *If $0 \le j \le m$, the jth terms of z and w_i are the same if and only if d_j divides i.*

Proof. Since z and w agree to an order of at most m and $0 \le j \le m$, it follows that z and w must have the same jth term. If we write this common term as

$$c_j t^{e_j} = c_j t^{n_j/d_j} = c_j (t^{1/R})^{(Rn_j/d_j)},$$

then by Proposition 3.11, the jth term of w_i is

$$c_j (\zeta^i t^{1/R})^{(Rn_j/d_j)},$$

where ζ is a primitive Rth root of unity. Thus the jth terms of z and w_i are identical exactly when $\zeta^{iRn_j/d_j} = 1$, which occurs whenever R divides iRn_j/d_j. However, this occurs exactly when in_j/d_j is an integer. Since n_j and d_j are relatively prime, this is equivalent to the condition $d_j | i$. □

Suppose $0 \le i < j \le m$. Since

$$r_j = \operatorname{lcm}(d_1, \ldots, d_j) = \operatorname{lcm}(r_i, d_{i+1}, \ldots, d_j),$$

it follows that $r_i | r_j$. Given two Puiseux series P_1, P_2 with disjoint supports (i.e., $\operatorname{Supp}(P_1) \cap \operatorname{Supp}(P_2) = \emptyset$), it is not difficult to prove that the ramification index of $P_1 + P_2$ is the least common multiple of the ramification indices of P_1 and P_2. We decompose w as $w = w^{(j)} + (w - w^{(j)})$, noting that $w^{(j)}$ and $w - w^{(j)}$ have disjoint supports. Thus the ramification index of w is a multiple of the ramification index of $w^{(j)}$. However, the ramification index of w is R and the ramification index of $w^{(j)}$ $(= z^{(j)})$ is r_j, and so $r_j | R$. In summary, we have the following divisibility relations:

$$1 = r_0 \mid r_1 \mid r_2 \mid \cdots \mid r_m \mid R. \tag{2}$$

Lemma 4.3. *If $0 \le j \le m$, then the number of conjugates of w that agree with z to an order of at least j is R/r_j.*

Proof. By Lemma 4.2, the first j terms of z and w_i agree if and only if $d_1, \ldots, d_j$ all divide i, which is equivalent to $\operatorname{lcm}(d_1, \ldots, d_j)|i$. By Lemma 3.10, $\operatorname{lcm}(d_1, \ldots, d_j)$ is simply r_j, and so the number of conjugates of w that agree with z to an order of at least j is the cardinality of $\{i : 0 \leq i \leq R,\ r_j|i\}$. However, this set has R/r_j elements, and the claim has been justified. □

We decompose z and w as $z = z^{(m)} + (z - z^{(m)})$ and $w = w^{(m)} + (w - w^{(m)})$. Since z and w agree to order m, $z^{(m)} = w^{(m)}$ and the first term of $z - z^{(m)}$ is different than the first term of $w - w^{(m)}$. Thus

$$\begin{aligned} \mathcal{L}E(z - w) &= \mathcal{L}E((z - z^{(m)}) - (w - w^{(m)})) \\ &= \max(\mathcal{L}E(z - z^{(m)}), \mathcal{L}E(w - w^{(m)})). \end{aligned} \tag{3}$$

Since $\mathcal{L}E(z - z^{(m)}) = e_{m+1}$, this provides us with the useful inquality

$$\mathcal{L}E(z - w) \geq e_{m+1}. \tag{4}$$

Lemma 4.4. *Suppose* $0 \leq j \leq m - 1$. *The number of conjugates of* w *that agree with* z *to order* j *is* $R/r_j - R/r_{j+1}$. *For each such conjugate* w_i, $\mathcal{L}E(z - w_i) = e_{j+1}$.

Proof. By Lemma 4.3, the number of conjugates that agree with z to an order of at least j is R/r_j, of which R/r_{j+1} conjugates agree with to z to an order of at least $j + 1$. Thus the first claim follows. Since z and w_i agree to order j, the first j terms of both z and w_i cancel in the expression $z - w_i$. Therefore, $\mathcal{L}E(z - w_i)$ is the exponent of either the $(j + 1)$st term of z or the $(j + 1)$st term of w_i. However, these two terms both have exponent e_{j+1}, and so the second claim holds. □

Lemma 4.5. *The number of conjugates of* w *that agree with* z *to order* m *is* R/r_m. *For each such conjugate* w_i, $\mathcal{L}E(z - w_i) = \mathcal{L}E(z - w)$.

Proof. By Lemma 4.3, the number of conjugates that agree with z to an order of at least m is R/r_m. Since no conjugate of w agrees with z to an order greater than m, the first claim follows. By (3), $\mathcal{L}E(z - w) = \max(\mathcal{L}E(z - z^{(m)}), \mathcal{L}E(w - w^{(m)}))$. Equation (3) depends only on the fact that z and w agree to order m. Thus for each conjuagte w_i that agrees with z to order m, we have $\mathcal{L}E(z - w_i) = \max(\mathcal{L}E(z - z^{(m)}), \mathcal{L}E(w_i - w_i^{(m)}))$. Since w and w_i agree to an order of at least m (they both agree with z to order m) and the exponents of w and w_i are identical by Proposition 3.11, it follows that $\mathcal{L}E(w - w^{(m)}) = \mathcal{L}E(w_i - w_i^{(m)})$. Thus $\mathcal{L}E(z - w) = \mathcal{L}E(z - w_i)$. □

We now combine these previous results to produce a formula for the leading exponent of the minimal polynomial of w over $k\langle\langle t\rangle\rangle$.

Proposition 4.6. *If $p(y) \in k\langle\langle t\rangle\rangle[y]$ is the minimal polynomial of w over $k\langle\langle t\rangle\rangle$, then*

$$\mathcal{L}E(p(z)) = \Big(\frac{R}{r_m}\Big)\Big[r_m\Big(\sum_{j=0}^{m-1}\Big(\frac{1}{r_j}-\frac{1}{r_{j+1}}\Big)e_{j+1}\Big) + \mathcal{L}E(z-w)\Big].$$

Proof. By Notation 4.1, each conjugate of w agrees with z to an order of at most m. By Lemma 4.4, given $0 \le j \le m-1$, there are $R/r_j - R/r_{j+1}$ conjugates w_i that agree with z to order j, and for each of these conjugates, $\mathcal{L}E(z-w_i) = e_{j+1}$. By Lemma 4.5, there are R/r_m conjugates w_i that agree with z to order m, and for each of these conjugates, $\mathcal{L}E(z-w_i) = \mathcal{L}E(z-w)$. Thus

$$\begin{aligned}\mathcal{L}E(p(z)) &= \sum_{i=1}^{R}\mathcal{L}E(z-w_i)\\ &= \Big(\sum_{j=0}^{m-1}\Big(\frac{R}{r_j}-\frac{R}{r_{j+1}}\Big)e_{j+1}\Big) + \Big(\frac{R}{r_m}\Big)\mathcal{L}E(z-w)\\ &= \Big(\frac{R}{r_m}\Big)\Big[r_m\Big(\sum_{j=0}^{m-1}\Big(\frac{1}{r_j}-\frac{1}{r_{j+1}}\Big)e_{j+1}\Big) + \mathcal{L}E(z-w)\Big]. \qquad \square\end{aligned}$$

Using Proposition 4.6, we demonstrate that $\mathcal{L}E(p(z))$ lies in a discrete subset of $\mathbb{Q}$ that depends solely on m and the ramification sequence $\mathbf{r}$ of z.

Proposition 4.7. $\mathcal{L}E(p(z)) \in (1/(r_m r_{m+1}))\mathbb{Z}$.

Proof. Since z and w agree to order m, $\mathcal{L}E(z-w)$ must either be the $(m+1)$st exponent of z or the $(m+1)$st exponent of w. In the first case, $\mathcal{L}E(z-w) \in (1/r_{m+1})\mathbb{Z}$. In the second case, $\mathcal{L}E(z-w) \in (1/R)\mathbb{Z}$ since w has ramification index R. In either case, we have

$$\mathcal{L}E(z-w) \in (1/r_{m+1})\mathbb{Z} \cup (1/R)\mathbb{Z} \subset (1/(Rr_{m+1}))\mathbb{Z}.$$

Moreover, for $0 \le j \le m-1$, $e_{j+1} \in (1/r_m)\mathbb{Z} \subset (1/(Rr_{m+1}))\mathbb{Z}$, and since $r_m/r_j \in \mathbb{Z}$ for all $j \le m$, we have

$$r_m\Big(\sum_{j=0}^{m-1}\Big(\frac{1}{r_j}-\frac{1}{r_{j+1}}\Big)e_{j+1}\Big) + \mathcal{L}E(z-w) \in \Big(\frac{1}{Rr_{m+1}}\Big)\mathbb{Z}.$$

Thus by Proposition 4.6,

$$\mathcal{L}E(p(z)) \in (R/r_m)(1/(Rr_{m+1}))\mathbb{Z} = (1/(r_m r_{m+1}))\mathbb{Z}. \qquad \square$$

5 WELL-ORDERED SETS OF EXPONENTS

We are now in a position to state the main theorem which we prove in the next section.

Theorem 5.1. *Let k be an arbitrary field of characteristic zero, and let z be an infinite, simple, bounded series with exponent sequence* $\mathbf{e}$ *and ramification sequence* $\mathbf{r}$. *Define $u_0 = 0$ and for $m \geq 1$,*

$$u_m = r_m\Big(\sum_{j=0}^{m-1}\Big(\frac{1}{r_j} - \frac{1}{r_{j+1}}\Big)e_{j+1}\Big).$$

Suppose the following conditions hold:

(i) *For all $m \in \mathbb{N}$, $u_m + e_{m+1} \geq 0$,*
(ii) $\lim u_m = \infty$.

Then the subset $\{\mathcal{L}E(f(t,z)) : f(x,y) \in k[x,y]^{\star}\}$ of $\mathbb{Q}$ is well-ordered.

Since $\mathrm{Supp}(z)$ consists of an infinite, bounded, decreasing sequence of elements of $\mathbb{Q}$, the denominator sequence of z must be unbounded, and hence the ramification sequence must be unbounded, i.e.,

$$\lim r_m = \infty. \tag{5}$$

Thus z is not reverse Puiseux, and so it is transcendental over $k\langle\langle t\rangle\rangle$ (and hence transcendental over $k(t)$).

The following corollary states that series with positive support yield well-ordered sets. Questions of further exploration naturally arise concerning the necessity of the two conditions in Theorem 5.1. It is unlikely that these conditions are as general as possible, and it would be interesting to determine series that yield well-ordered sets despite the fact that they may fail to satisfy one or both of the conditions. Another related question is whether it is possible for a reverse Puiseux series $z \in k\langle\langle t^{\mathbb{Q}}\rangle\rangle$ that is transcendental over $k(t)$ to yield a well-ordered set.

Corollary 5.2. *Let k be an arbitrary field of characteristic zero, and let z be an infinite, simple series whose support is strictly positive. Then* $\{\mathcal{LE}(f(t,z)) : f(x,y) \in k[x,y]^\star\}$ *is well-ordered.*

Proof. Since each e_j is positive, it follows that u_j is positive for all j. Thus condition (i) of Theorem 5.1 holds.

For each $j \geq 0$, define $b_j = \left(\frac{1}{r_j} - \frac{1}{r_{j+1}}\right)e_{j+1}$. Since $r_{j+1} \geq r_j$, we have $b_j \geq 0$. Since $\lim r_m = \infty$ by (5), $r_M > r_{M-1}$ for some $M \in \mathbb{N}^\star$, in which case $b_M > 0$. Thus for all $m > M$,

$$u_m = r_m\Big(\sum_{j=0}^{m-1}\Big(\frac{1}{r_j} - \frac{1}{r_{j+1}}\Big)e_{j+1}\Big) = r_m\Big(\sum_{j=0}^{m-1} b_j\Big) \geq r_m b_M.$$

Since b_M is fixed and $\lim r_m = \infty$, condition (ii) of Theorem 5.1 must hold. □

Here is an example in which the series z has a mixture of positive and negative support, and yet well-ordereness still occurs.

Example 5.3. Let

$$z = t^{3/2} + \sum_{i=2}^{\infty} t^{-1+2^{-i}} = t^{3/2} + t^{-3/4} + t^{-7/8} + t^{-15/16} + \cdots.$$

The exponent sequence is $\mathbf{e} = (3/2, -1 + 1/4, -1 + 1/8, \ldots)$ and the ramification sequence is $\mathbf{r} = (1, 2, 4, 8, 16, \ldots)$. Clearly, condition (i) holds for $m = 0$. For $m \geq 1$, we compute:

$$\begin{aligned} u_m &= 2^m\Big(\sum_{j=0}^{m-1}\Big(\frac{1}{2^j} - \frac{1}{2^{j+1}}\Big)e_{j+1}\Big) \\ &= 2^m\Big(\frac{3}{4} + \sum_{j=1}^{m-1}\frac{e_{j+1}}{2^{j+1}}\Big) \\ &= 2^m\Big(\frac{3}{4} + \sum_{j=1}^{m-1}\frac{-1 + 2^{-(j+1)}}{2^{j+1}}\Big), \end{aligned}$$

which simplifies to

$$u_m = \Big(\frac{1}{3}\Big)2^m\Big(1 - 4^{-m}\Big) + 1.$$

Thus $u_m \geq 1$, and since $e_{m+1} \geq -1$, we have $u_m + e_{m+1} \geq 0$. Moreover, $\lim u_m = \infty$, and so by Theorem 5.1, $\{\mathcal{LE}(f(t,z)) : f(x,y) \in k[x,y]^\star\}$ is well-ordered.

6 THE PROOF OF THE MAIN THEOREM

If k is not algebraically closed, note that $\{\mathcal{LE}(f(t,z)) : f(x,y) \in k[x,y]^\star\} \subset \{\mathcal{LE}(f(t,z)) : f(x,y) \in \overline{k}[x,y]^\star\}$ (where $\overline{k}$ denotes the algebraic closure of k), in which case the smaller set is well-ordered whenever the larger set is well-ordered. Thus it suffices to prove Theorem 5.1 in case k is algebraically closed.

Notation 6.1. We adopt the following notation for this section.

- k is an algebraically closed field of characteristic zero.
- z is an infinite, simple, bounded series with limit L (see Definition 3.4).
- **e** and **r** are the exponent and ramification sequences of z.
- u_m is defined as in Theorem 5.1.

Definition 6.2. *Define $A_m(z)$ to be the collection of all $f(x,y) \in k[x,y]^\star$ such that the largest order to which any of the roots of $f(t,y) \in k(t)[y]$ agree with z is m.*

Example 6.3. Consider the series $z = t^{1/2} + t^{1/3} + t^{1/5} + \cdots$. Let $f_1(t,y) \in k\langle\langle t\rangle\rangle[y]$ be the minimal polynomial of $t^{1/2} + 2t^{1/3}$ over $k\langle\langle t\rangle\rangle$ and $f_2(t,y) \in k\langle\langle t\rangle\rangle[y]$ be the minimal polynomial of $-t^{1/2} + t^{1/3}$ over $k\langle\langle t\rangle\rangle$. Then $f_1(x,y) \in A_1(z)$ because none of the conjugates of $t^{1/2} + 2t^{1/3}$ agree with z to an order greater than 1, and $f_2(x,y) \in A_2(z)$ because $t^{1/2} + t^{1/3}$ is a conjugate of $-t^{1/2} + t^{1/3}$ that agrees with z to order 2.

Lemma 6.4. *If $u_m + e_{m+1} \geq 0$ for all $m \geq 0$, then $\{\mathcal{LE}(f(t,z)) : f(x,y) \in A_m(z)\}$ is well-ordered.*

Proof. Let $f(x,y) \in A_m(z)$. First factor $f(t,y) \in k[t,y]$ as $f(t,y) = g(t)p_1(y)\cdots p_s(y)$ where $g(t) \in k[t]$ and each $p_i(y)$ is an irreducible monic polynomial in $k\langle\langle t\rangle\rangle[y]$. Since no root of any $p_i(y)$ agrees with z to an order greater than m, by Proposition 4.7, $\mathcal{LE}(p_i(z)) \in (1/r_{m_i}r_{m_i+1})\mathbb{Z}$ for some $m_i \leq m$. Since $r_{m_i}|r_m$ by (2), it follows that $\mathcal{LE}(p_i(z)) \in (1/r_m r_{m+1})\mathbb{Z}$. Now

$$\mathcal{LE}(f(t,z)) = \mathcal{LE}(g(t)) + \sum \mathcal{LE}(p_i(z))$$

and $\mathcal{LE}(g(t)) \in \mathbb{N}$, and so $\mathcal{LE}(f(t,z)) \in (1/r_m r_{m+1})\mathbb{Z}$. Thus we have shown

$$\{\mathcal{LE}(f(t,z)) : f(x,y) \in A_m(z)\} \subset (1/(r_m r_{m+1}))\mathbb{Z}. \tag{6}$$

If $p_i(y)$ has degree R, then by Proposition 4.6 and (4),

$$\mathcal{L}E(p_i(z)) = (R/r_m)[u_m + \mathcal{L}E(z - w)] \geq (R/r_m)[u_m + e_{m+1}].$$

By the assumption $u_m + e_{m+1} \geq 0$, we have

$$\mathcal{L}E(p_i(z)) \geq 0. \tag{7}$$

Thus $\mathcal{L}E(f(t,z)) = \mathcal{L}E(g(t)) + \sum \mathcal{L}E(p_i(z)) \geq 0$, and so

$$\{\mathcal{L}E(f(t,z)) : f(x,y) \in A_m(z)\} \subset \mathbb{Q}^+. \tag{8}$$

Combining the inclusions in (6) and (8), we obtain $\{\mathcal{L}E(f(t,z)) : f(x,y) \in A_m(z)\} \subset (1/(r_m r_{m+1}))\mathbb{N}$. Since $(1/(r_m r_{m+1}))\mathbb{N}$ is a well-ordered set, $\{\mathcal{L}E(f(t,z)) : f(x,y) \in A_m(z)\}$ must also be a well-ordered set. □

We state the following lemma without proof.

Lemma 6.5. *Let $V_0, V_1, V_2, \ldots$ be well-ordered subsets of $\mathbb{Q}$, and let v_m be the smallest element of V_m. If $\lim v_m = \infty$, then $\bigcup_{m=0}^{\infty} V_m$ is well-ordered.*

We are now in a position to give a lower bound for $\mathcal{L}E(f(t,z))$ (where $f(x,y) \in A_m(z)$) in terms of u_m and the limit L of the series z.

Lemma 6.6. *If $u_m + e_{m+1} \geq 0$ for all $m \geq 0$, then for all $f(x,y) \in A_m(z)$, $\mathcal{L}E(f(t,z)) \geq u_m + L$.*

Proof. Given $f(x,y) \in A_m(z)$, let w be a root of $f(t,y) \in k(t)[y]$ that agrees with z to order m. Let $p_1(y) \in k\langle\langle t\rangle\rangle[y]$ be the minimal polynomial of w over $k\langle\langle t\rangle\rangle$. Factor $f(t,y)$ as

$$f(t,y) = g(t)p_1(y)\cdots p_s(y)$$

where $g(t) \in k[t]$ and each $p_i(y)$ is an irreducible monic polynomial in $k\langle\langle t\rangle\rangle[y]$. As in (7) in the proof of Lemma 6.4, $\mathcal{L}E(p_i(z)) \geq 0$. Moreover, $\mathcal{L}E(g(t)) \in \mathbb{N}$, and so $\mathcal{L}E(f(t,z))$ can be expressed as

$$\mathcal{L}E(g(t)) + \mathcal{L}E(p_1(z)) + \sum_{i=2}^{s} \mathcal{L}E(p_i(z)) \geq \mathcal{L}E(p_1(z)). \tag{9}$$

Let R be the ramification index of w. We know that $\mathcal{L}E(z - w) \geq e_{m+1}$ by (4), and so $\mathcal{L}E(z - w) \geq L$. Moreover, $R/r_m \geq 1$ by (2) and so we can obtain the desired lower bound for $\mathcal{L}E(p_1(z))$ (and hence for $\mathcal{L}E(f(t,z))$ via (9)) by replacing R/r_m by 1 and $\mathcal{L}E(z - w)$ by L in the expression for $\mathcal{L}E(p_1(z))$ given in Proposition 4.6. □

We now complete the proof of Theorem 5.1. To do this, we make the assumptions that (i) for all $m \in \mathbb{N}$, $u_m + e_{m+1} \geq 0$, and (ii) $\lim u_m = \infty$. By Lemma 6.4, $V_m = \{\mathcal{L}E(f(t,z)) : f(x,y) \in A_m(z)\}$ is well-ordered. By Lemma 6.6, it follows that for all $f(x,y) \in A_m(z)$, $\mathcal{L}E(f(t,z)) \geq u_m + L$. Thus if v_m denotes the smallest element of V_m, then $v_m \geq u_m + L$. Since we are assuming $\lim u_m = \infty$, it follows that $\lim v_m = \infty$. Thus by Lemma 6.5,

$$\bigcup_{m=0}^{\infty} \{\mathcal{L}E(f(t,z)) : f(x,y) \in A_m(z)\}$$

is well-ordered. Since $k[x,y]^\star = \bigcup A_m(z)$, the result follows.

REFERENCES

1. Cohn, P.M. *Algebraic Numbers and Algebraic Functions*; Chapman & Hall, 1991.
2. Duval, D. Rational Puiseux Series. Compositio Mathematica **1989**, *70*, 119–154.
3. Endler, E. *Valuation Theory*; Springer Verlag, 1972.
4. Hahn, H. Über Die Nichtarchimedischen Gr̈oßensysteme. Sitz. Akad. Wiss. Wien. **1907**, *116*, 601–655.
5. MacLane, S.; Schilling, O.F.G. Zero-Dimensional Branches on Algebraic Varieties. Annals of Mathematics **1939**, *40*, 507–520.
6. Mosteig, E. *A Valuation-Theoretic Approach to Polynomial Computations*; Doctoral Thesis, Cornell University, 2000.
7. Mosteig, E.; Sweedler, M. Valuations and Filtrations. Journal of Symbolic Computation, to appear.
8. Mosteig, E.; Sweedler, M. The Growth of Valuations on Rational Function Fields, preprint available at math.usask.ca/fvk/Valth.html.
9. Ribenboim, P. Rings of Generalized Power Series: Nilpotent Elements. Abh. Math. Sem. Univ. Hamburg **1991**, *61*, 15–33.
10. Ribenboim, P. Fields: Algebraically Closed and Others. Manuscripta Math. **1992**, *75*, 115–150.
11. Ribenboim, P.; Special Properties of Generalized Power Series. Journal of Algebra **1995**, *173*, 566–586.
12. Sweedler, M. Ideal Bases and Valuation Rings, available at math. usask.ca/fvk/Valth.html, 1986.
13. Zariski, O. The Reduction of the Singularities of an Algebraic Surface. Annals of Mathematics **1939**, *40*, 639–689.

Received August 2001
Revised October 2001