ÖAW AUSTRIAN ACADEMY OF SCIENCES

RICAM – JOHANN RADON INSTITUTE FOR COMPUTATIONAL AND APPLIED MATHEMATICS

The Newton-Puiseux algorithm and effective algebraic series

M. Buchacher

RICAM-Report 2023-31

WWW.RICAM.OEAW.AC.AT

ALTENBERGER STRASSE 69 | 4040 LINZ, AUSTRIA
T: +43 732 2468-5222 | F: +43 732 2468-5212 | OFFICE@RICAM.OEAW.AC.AT
IBAN: AT541100000262650519 | BIC: BKAUATWW | VAT: ATU37116303

RICAM

THE NEWTON-PUISEUX ALGORITHM AND EFFECTIVE ALGEBRAIC SERIES

Manfred Buchacher
RICAM
Austrian Academy of Sciences
manfredi.buchacher@gmail.com

Abstract. We explain how to encode an algebraic series by a finite amount of data, namely its minimal polynomial, a total order and its first terms with respect to this order, and how to do effective arithmetic on the level of these encodings. The reasoning is based on the Newton-Puiseux algorithm and an effective equality test for algebraic series. We also explain how to derive information about the support of an algebraic series, e.g. how to compute the vertices and bounded faces of the convex hull of its support.

1. Overview

Given a polynomial $p(x, y)$ in two variables x and y over an algebraically closed field $\mathbb{K}$ of characteristic zero, the classical Newton-Puiseux algorithm [20, 10] determines the first terms of a series ϕ in x over $\mathbb{K}$ that solves $p(x, \phi) = 0$. Finding a series solution of a polynomial equation is one and the most apparent aspect of the algorithm. However, it also permits to encode algebraic series by a finite amount of data and to effectively compute with them on the level of these encodings. While this is well-known for univariate algebraic series, this is not the case for algebraic series that are multivariate. We explain how to do effective arithmetic with multivariate algebraic series and complement the discussion of the Newton-Puiseux algorithm for (multivariate, not necessarily bivariate) polynomials over a field of characteristic zero in [16]. We also explain that the convex hull of the support of an algebraic series is a polyhedral set and explain how the Newton-Puiseux algorithm and an effective equality test for algebraic series can be used to compute its vertices and bounded faces. The article comes with a Mathematica implementation of the Newton-Puiseux algorithm and a Mathematica notebook that contains the examples presented here. Both can be found on https://github.com/buchacm/newtonPuiseuxAlgorithm.

Further literature related to the Newton-Puiseux algorithm, effective algebraic series or supports of algebraic series: a generalization of the Newton-Puiseux algorithm to systems of polynomial equations over a field of characteristic zero is presented in [17, 5, 4], see also the references therein, and to polynomials over a field of positive characteristic in [21]. Supports of series were also studied in [3, 6], though in the more general context of series algebraic over a certain ring of series. For a complexity analysis of (variants of) the Newton-Puiseux algorithm we refer to [22], in particular to [19] and the references therein. Finally, we point out that there are other computational models for algebraic (power) series based on the Implicit Function Theorem [2, 1], diagonals of rational functions [12], or closed-form formulas of their coefficients [13].

2. Preliminaries

We begin with introducing the objects this article is about: multivariate algebraic series and the Newton-Puiseux algorithm to constructively work with them.

We use multi-index notation: we denote by $\mathbf{x} = (x_1, \dots, x_n)$ a vector of variables, and we write $\mathbf{x}^I = x_1^{i_1} \cdots x_n^{i_n}$ for the monomial whose exponent vector is $I = (i_1, \dots, i_n) \in \mathbb{Q}^n$. We work over a (computable) algebraically closed field $\mathbb{K}$ of characteristic zero. A *series* ϕ in $\mathbf{x}$ over $\mathbb{K}$ is a formal sum

$$\phi = \sum_{I \in \mathbb{Q}^n} a_I \mathbf{x}^I$$

of terms in $\mathbf{x}$ whose coefficients a_I are elements of $\mathbb{K}$. Its *support* is defined by

$$\operatorname{supp}(\phi) = \{I \in \mathbb{Q}^n : a_I \neq 0\},$$

and we will assume throughout that there is a vector $v \in \mathbb{R}^n$, a strictly convex rational cone $C \subseteq \mathbb{R}^n$ and an integer $k \in \mathbb{Z}$ such that

$$\operatorname{supp}(\phi) \subseteq (v + C) \cap \frac{1}{k}\mathbb{Z}^n.$$

Recall that a *cone* C is a subset of $\mathbb{R}^n$ that is closed under multiplication with non-negative numbers. It is called *convex*, if for any two points of C, it also contains the line segment that joins them, and it

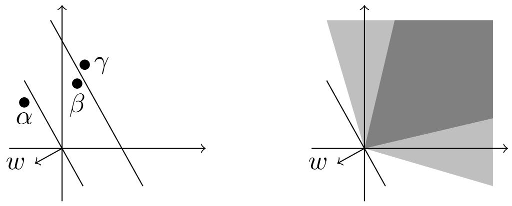

FIGURE 1. A vector $w \in \mathbb{R}^2$ that induces an additive total order $\preceq$ on $\mathbb{Q}^2$ such that $\alpha > \beta > \gamma$ and two cones that are compatible with it.

is said to be *strictly convex*, if it is convex and does not contain any lines. It is *rational*, if there are $v_1, \dots, v_k \in \mathbb{Z}^n$ such that

$$C = \operatorname{cone}\{v_1, \dots, v_k\} := \mathbb{R}_{\geq 0} \cdot v_1 + \cdots + \mathbb{R}_{\geq 0} \cdot v_k.$$

All cones appearing in this text will be strictly convex rational cones.

Without any restriction on their supports, the sum and product of two series is not well-defined.

Example 1. The geometric series

$$\phi_1 = 1 + x + x^2 + \dots \quad \text{and} \quad \phi_2 = -x^{-1} - x^{-2} - x^{-3} - \dots$$

are series in the above sense, but neither is their sum nor their product. Their product is not meaningful, since its coefficients involve infinite sums, and their sum is not well-defined, because its support is not contained in a shift of a strictly convex cone.

For any strictly convex rational cone $C \subseteq \mathbb{R}^n$ the set $\mathbb{K}_C[[x]]$ of series whose support is contained in C is a ring with respect to addition and multiplication [18, Theorem 10]. Yet, it is not a field [18, Theorem 12]. Any $w \in \mathbb{R}^n$ whose components are linearly independent over $\mathbb{Q}$ defines an additive total order $\preceq$ on $\mathbb{Q}^n$ by

$$\alpha \preceq \beta \quad :\Longleftrightarrow \quad \alpha \cdot w \leq \beta \cdot w,$$

where $v \cdot w$ denotes the Euclidean inner product of two vectors $v, w \in \mathbb{R}^n$. A cone $C \subseteq \mathbb{R}^n$ is *compatible* with $w \in \mathbb{R}^n$ and the induced total order $\preceq$ on $\mathbb{Q}^n$, if $C \cap \mathbb{Q}^n$ has a maximal element with respect to it. Given an additive total order $\preceq$ on $\mathbb{Q}^n$, we denote by $\mathscr{C}$ the set of strictly convex rational cones that are compatible with it, and we write

$$\mathbb{K}_{\preceq}((\mathbf{x})) := \bigcup_{C \in \mathscr{C}} \bigcup_{e \in \mathbb{Q}^n} x^e \mathbb{K}_C[[\mathbf{x}]]$$

for the set of series whose support is contained in a shift of such a cone. It is not only a ring but even a field [18, Theorem 15].

A series ϕ is said to be *algebraic*, if there is a non-zero polynomial $p \in \mathbb{K}[\mathbf{x}, y]$ such that

$$p(\mathbf{x}, \phi) = 0,$$

and it is said to be *D-finite* [15], if for every $i \in \{1, \dots, n\}$ there are polynomials $q_0, \dots, q_r \in \mathbb{K}[\mathbf{x}]$ such that

$$q_0 \phi + q_1 \frac{\partial}{\partial x_i} \phi + \cdots + q_r \frac{\partial^r}{\partial x_i^r} \phi = 0.$$

Every algebraic series is D-finite [14, Theorem 6.1], and just as algebraic series, D-finite series satisfy many closure properties. For instance, the sum $\phi_1 + \phi_2$ of two D-finite series ϕ_1 and ϕ_2 is D-finite [14, Theorem 7.2], and so is the restriction of a D-finite series ϕ to a rational cone C [8], i.e.

$$[\phi]_C(\mathbf{x}) := \sum_{I \in C \cap \mathbb{Q}^n} \left([\mathbf{x}^I]\phi \right) \mathbf{x}^I,$$

where $[\mathbf{x}^I]\phi$ denotes the coefficient of $\mathbf{x}^I$ in ϕ. These closure properties are effective in the sense that systems of differential equations for $\phi_1 + \phi_2$ and $[\phi]_C$ can be computed from the differential equations satisfied by ϕ_1, ϕ_2 and ϕ.

Having a univariate D-finite series $\phi(t) := \sum_{k \geq k_0} \phi_k t^k$ in a variable t and a differential equation satisfied by it, it can be checked effectively whether it is identically zero. The differential equation for ϕ translates into a recurrence relation for its coefficients,

$$p_0(k)\phi_k + p_1(k)\phi_{k+1} + \cdots + p_r(k)\phi_{k+r} = 0, \quad p_0, \dots, p_r \in \mathbb{K}[k],$$

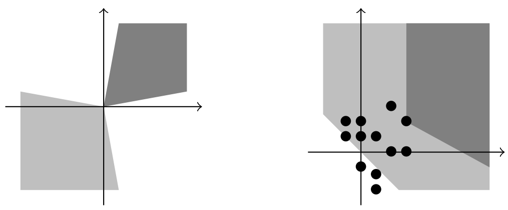

FIGURE 2. Two strictly convex cones that are dual to each other, and the support of the first terms of a series and a shifted cone that contains the remaining (non-depicted) support.

so that $\phi = 0$ if and only if $\phi_k = 0$ for finitely many k, the number of terms which have to be compared to zero depending on the order of the recurrence and the largest integer root of p_r.

Given $p \in \mathbb{K}[\mathbf{x}, y]$ and a total order $\preceq$ on $\mathbb{Q}^n$ induced by some $w \in \mathbb{R}^n$, the Newton-Puiseux algorithm [16] determines the first terms of the series solutions of $p(\mathbf{x}, y) = 0$ in $\mathbb{K}_{\preceq}((\mathbf{x}))$. We collect some definitions before we present it. The *Newton polytope* of p is the convex hull of the support of p,

$$\mathrm{NP}(p) := \mathrm{conv}(\mathrm{supp}(p)).$$

If e is an edge of $\mathrm{NP}(p)$ that connects two vertices v_1 and v_2, we write $e = \{v_1, v_2\}$. It is called *admissible*, if $v_{1,n+1} \neq v_{2,n+1}$. If $v_{1,n+1} < v_{2,n+1}$, we call v_1 and v_2 the minor and major vertex of e, respectively, and denote them by $\mathrm{m}(e)$ and $\mathrm{M}(e)$. An *edge path* on $\mathrm{NP}(p)$ is a sequence $e_1, \ldots, e_k$ of edges such that $\mathrm{m}(e_{i+1}) = \mathrm{M}(e_i)$ for $i = 1, \ldots, k-1$. Let P_e be the projection on $\mathbb{R}^{n+1}$ that projects on $\mathbb{R}^n \times \{0\}$ along lines parallel to an (admissible) edge e. The *barrier cone* of e is the smallest cone that contains $P_e(\mathrm{NP}(p)) - P_e(e)$, the projection of the Newton polytope of p shifted by the projection of its edge e. It is denoted by $C(e)$. We occasionally identify $\mathbb{R}^n$ and $\mathbb{R}^n \times \{0\} \subseteq \mathbb{R}^{n+1}$, and consider $C(e)$ as a subset of $\mathbb{R}^n$. Its *dual* is

$$C(e)^* := \{w \in \mathbb{R}^n : v \cdot w \leq 0 \text{ for all } v \in C(e)\}.$$

A vector $w \in \mathbb{R}^n$ that defines a total order on $\mathbb{Q}^n$ is said to be *compatible* with e, if $w \in C(e)^*$, and an edge path is called *coherent*, if there is a $w \in \mathbb{R}^n$ that is compatible with all of its edges.

Given an admissible edge $e = \{v_1, v_2\}$, we denote its *slope* with respect to its last coordinate by

$$\mathrm{S}(e) := \frac{1}{v_{2,n+1} - v_{1,n+1}}(v_{2,1} - v_{1,1}, \ldots, v_{2,n} - v_{1,n}).$$

The edge polynomial $p_e(t)$ of an edge e of the Newton polytope of p is

$$p_e(t) = \sum_I a_I t^{I_{n+1} - \mathrm{m}(e)_{n+1}},$$

where $a_I = [(\mathbf{x}, y)^I]p$ and the sum runs over all I in $e \cap \mathrm{supp}(p)$.

We now present the Newton-Puiseux algorithm. We comment on it after the statement of the algorithm. For details, in particular for a proof of its correctness, we refer to [16, Theorem 3.5].

Algorithm 1 (Newton-Puiseux Algorithm)**.** *Input: A square-free and non-constant polynomial* $p \in \mathbb{K}[\mathbf{x}, y]$*, an admissible edge* e *of its Newton polytope, an element* w *of the dual of its barrier cone* $C(e)$ *defining a total order on* $\mathbb{Q}^n$*, and a (non-negative) integer* k*.*
Output: A list of $\mathrm{M}(e)_{n+1} - \mathrm{m}(e)_{n+1}$ *many pairs* $(c_1\mathbf{x}^{\alpha_1} + \cdots + c_N\mathbf{x}^{\alpha_N}, C)$ *with* $c_1\mathbf{x}^{\alpha_1}, \ldots, c_N\mathbf{x}^{\alpha_N}$ *being the first* N *terms of a series solution* ϕ *of* $p(\mathbf{x}, \phi) = 0$*, ordered with respect to* w *in decreasing order, and* C *being a strictly convex rational cone such that* $\mathrm{supp}(\phi) \subseteq \{\alpha_1, \ldots, \alpha_{N-1}\} \cup (\alpha_N + C)$*, where* N *is the smallest integer greater than or equal to* k *such that the series solutions can be distinguished by their first* N *terms.*

Compute the roots c *of the edge polynomial* $p_e(t)$ *associated with* e*, let* L_1 *be equal to the set of (pairwise different!) pairs* (ϕ, e) *with* $\phi = c\mathbf{x}^{-\mathrm{S}(e)}$ *and set* $L_{\mathrm{finite}} = \emptyset$ *and* $N = 1$*.*
While $|L_{\mathrm{finite}}| + |L_1| < \mathrm{M}(e)_{n+1} - \mathrm{m}(e)_{n+1}$ *or* $(|L_{\mathrm{finite}}| < \mathrm{M}(e)_{n+1} - \mathrm{m}(e)_{n+1}$ *and* $N < k)$*, do:*
Set $L_2 = \emptyset$ *and* $N = N + 1$*.*
While there is a $(\phi, e) \in L_1$ *with* ϕ *not having* k *terms or* $p_e(t)$ *not having only simple roots, do for each* $(\phi, e) \in L_1$*:*
If ϕ *satisfies* $p(\mathbf{x}, \phi) = 0$*, append* (ϕ, e) *to* L_{finite}*, otherwise compute the Newton polytope of* $p(\mathbf{x}, \phi + y)$ *and determine its unique edge path* $e_1, \ldots, e_l$ *such that* $\mathrm{m}(e_1)_{n+1}$ *equals zero, and* $\mathrm{M}(e_l)$*, but not* $\mathrm{m}(e_l)$*, lies on the line through* e*, and* $w \in \bigcap C^*(e_i)$*.*

6 *For each edge e of the edge path, do:*
7 *Compute the roots c of the edge polynomial $p_e(t)$ associated with the edge e of the Newton polytope of $p(\mathbf{x}, \phi + y)$, and append to L_2 all pairs $(\phi + c\mathbf{x}^{-\mathrm{S}(e)}, e)$.*
8 *Set $L_1 = L_2$.*
9 *Replace each pair $(\phi + c\mathbf{x}^{-\mathrm{S}(e)}, e)$ in $L_{\mathrm{finite}} \cup L_1$ by $(\phi + c\mathbf{x}^{-S(e)}, C)$, where C is the barrier cone of e with respect to $p(\mathbf{x}, \phi + y)$, and return $L_{\mathrm{finite}} \cup L_1$.*

Remark 1. *The input of the Newton-Puiseux algorithm as stated here are a square-free polynomial p, an edge e of its Newton polytope, some vector w inducing a total order and an integer k, and outputs the first terms of series roots of p, sufficiently many to distinguish them from each other on the basis of this output. The order in which the terms of these series are computed is given by the total order induced by w. The integer k is a lower bound on the number of terms computed, the actual number can be greater if k is too small to distinguish the series solutions by their first k terms. It is the minimal number not smaller than k for which this is the case. The algorithm proceeds similarly as the classical Newton-Puiseux algorithm: it starts with computing a term $c_1\mathbf{x}^{\alpha_1}$ for which the highest order terms with respect to w in the expansion of $p(\mathbf{x}, c_1\mathbf{x}_1^{\alpha} + y)$ cancel. Choosing $\alpha_1 = -\mathrm{S}(e_1)$ for $e_1 = e$, these terms come from those terms of p which are supported on e_1. The choice of c_1 guarantees that they sum up to zero. See step 1. Having computed the first N terms $c_1\mathbf{x}^{\alpha_1}, \ldots, c_N\mathbf{x}^{\alpha_N}$, the next term is computed analogously, starting with some edge e_{N+1} of the Newton polytope of $p(c_1\mathbf{x}^{\alpha_1} + \cdots + c_N\mathbf{x}^{\alpha_N} + y)$, chosen such that the order of the corresponding term is smaller than the order of the previously computed terms. See step 5 and step 7. If an edge polynomial $p_e(t)$ has several pairwise different roots, or if there is more than one possible choice for the edge used in the construction of the next term, an approximate series solution splits into several different approximate solutions. The while-loop which starts in step 2 stops when the number of approximate solutions constructed reaches $|\mathrm{M}(e)_{n+1} - \mathrm{m}(e)_{n+1}|$ and the first N terms of each solution have been computed. It eventually terminates because p is square-free and $\mathbb{K}$ has characteristic zero, see* [16, Theorem 3.6]. *Clearly, as soon as an edge polynomial $p_{e_N}(t)$ has only simple roots the corresponding solutions constructed can be distinguished by their first N terms. In this case, the support of the corresponding series are contained in a shift of the barrier cone $C(e_N)$, see* [16, Section 3.10].

The following statement is an immediate consequence of the correctness of Algorithm 1 and will be helpful later. See [16, Corollary 4.1] for a similar statement.

Proposition 1. *Let $p \in \mathbb{K}[\mathbf{x}, y]$ and let $w \in \mathbb{R}^n$ define a total order $\preceq$ on $\mathbb{Q}^n$. Then $\mathbb{K}_{\preceq}((\mathbf{x}))$ contains $\deg_y(p)$ many series roots of p all of which can be computed by Algorithm 1.*

Proof. We assume that p is square-free and not a multiple of y. If p were not square-free, we could instead consider its square-free part $p/\gcd(p, \frac{\partial}{\partial y}p)$. This does not affect the set of roots but only their multiplicities. We show that there is a unique edge path $e_1, \ldots, e_k$ on the Newton polytope of p such that $w \in \bigcap C^*(e_i)$ and $\mathrm{m}(e_1)_{n+1} = 0$ and $\mathrm{M}(e_k)_{n+1} = \deg_y(p)$. Algorithm 1 then implies that these edges give rise to $\deg_y(p)$ many pairwise different series roots of p all of which are elements of $\mathbb{K}_{\preceq}((\mathbf{x}))$: the number of (pairwise different) series roots in $\mathbb{K}_{\preceq}((\mathbf{x}))$ coming from an edge e_i is $\mathrm{M}(e_i)_{n+1} - \mathrm{m}(e_i)_{n+1}$, series roots coming from different edges e_i and e_j are different since they can be distinguished by their leading exponents $-\mathrm{S}(e_i)$ and $-\mathrm{S}(e_j)$, and $\mathrm{M}(e_i)_{n+1} - \mathrm{m}(e_i)_{n+1}$ telescopes to $\deg_y(p)$ when summed over all edges of the edge path. To construct such an edge path, let v_1 be the vertex of the Newton polytope of p which maximizes $v \cdot w$ among all vertices in $\mathbb{R}^n \times \{0\}$ and let $e_1 = \{v_1, v_2\}$ be the admissible edge whose major vertex v_2 maximizes $v \cdot w$ among all vertices v that are adjacent to v_1 by an admissible edge. Then $w \in C^*(e_1)$. The latter holds because the hyperplane which contains e_1 and which is spanned by $v_2 - v_1$ and the orthogonal complement of w in $\mathbb{R}^n \times \{0\}$ is a supporting hyperplane for the Newton polytope of p. If $v_{2,n+1} = \deg_y(p)$ we are finished as e_1 is already the edge path we are looking for. If this is not the case we can extend e_1 by an admissible edge e_2 whose minor vertex equals the major vertex of e_1 which maximizes $\mathrm{M}(e_2) \cdot w$ among all such edges. Extending the edge path until it cannot be extended any further by an admissible edge results in an edge path with the claimed property. The uniqueness of this path is immediate: if it were not unique, then $\mathbb{K}_{\preceq}((\mathbf{x}))$ would contain more than $\deg_y(p)$ many series solutions, contradicting $\mathbb{K}_{\preceq}((\mathbf{x}))$ being a field. □

3. Finite encodings

The Newton-Puiseux algorithm determines the series solutions of a polynomial equation term by term. The next proposition implies that it can also be used to represent a series by a finite amount of data: its minimal polynomial (or more generally: an annihilating square-free polynomial), a total order, and its first few terms with respect to this order.

Proposition 2. *Let $p \in \mathbb{K}[\mathbf{x}, y]$ be a square-free and non-constant polynomial, e an admissible edge of its Newton polytope, w an element of $C^*(e)$ inducing a total order $\preceq$ on $\mathbb{Q}^n$ and $a_1\mathbf{x}^{\alpha_1}, \dots, a_N\mathbf{x}^{\alpha_N}$ the first few terms of a series solution ϕ as output by Algorithm 1 when applied to p, e, w and $k = 0$. Then ϕ is the only series solution in $\mathbb{K}_{\preceq}((\mathbf{x}))$ whose first terms are $a_1\mathbf{x}^{\alpha_1}, \dots, a_N\mathbf{x}^{\alpha_N}$.*

Proof. The proof of Proposition 1 shows that e can be extended to an edge path on the Newton polytope of p that gives rise to $\deg_y(p)$ many series solutions in $\mathbb{K}_{\preceq}((\mathbf{x}))$. By design of the algorithm, the first N terms of any series solution constructed from e different from ϕ differ from $a_1\mathbf{x}^{\alpha_1}, \dots, a_N\mathbf{x}^{\alpha_N}$. If e' is any other edge of the edge path, then the leading exponent of any series solution resulting from it is $-\mathrm{S}(e')$ and different from the leading exponent $-\mathrm{S}(e)$ of ϕ, see the proof of [16, Lemma 3.7]. □

We illustrate the Newton-Puiseux algorithm and Proposition 2 with a first example.

Example 2. We determine the first terms of a series solution of the equation

$$p(x, y, z) := 4x^2y + (x^2y + xy^2 + xy + y)^2 - z^2 = 0$$

when solved for z. The Newton polytope of p has four admissible edges, one of which is the edge $e = \{(0, 2, 0), (0, 0, 2)\}$. Its barrier cone is $C(e) = \mathrm{cone}\{(1, 1), (2, -1)\}$, and $w := (-\sqrt{2}, -1)$ is an element of its dual $C^*(e)$. Its components are linearly independent over $\mathbb{Q}$, therefore it defines a total order $\preceq$ on $\mathbb{Q}^2$. By [16, Theorem 3.5], and because the projection of e on its last coordinate has length 2, there are two series solutions ϕ_1 and ϕ_2 of $p(x, y, z) = 0$ in $\mathbb{K}_{\preceq}((x, y))$. We determine their first terms using Algorithm 1. The slope of e is $\mathrm{S}(e) = (0, -1)$, so the solutions have a term of the form cy, for some $c \in \mathbb{K}$. The coefficients c are the solutions to $-1 + t^2 = 0$. Hence, y is the first term of one series solution, say ϕ_1, and $-y$ the first term of ϕ_2. Furthermore, their support is contained in $(0, 1) + \mathrm{cone}\{(1, 1), (2, -1)\}$, because $-1 + t^2$ has only simply roots. To compute the next term of ϕ_1, for instance, we consider the polynomial $p(x, y, y + z)$. The edge path on its Newton polytope mentioned in Algorithm 1 consists of the single edge $e = \{(1, 2, 0), (0, 1, 1)\}$. Its slope with respect to the last coordinate is $(-1, -1)$, so its next term is of the form cxy, where c is the root of $-2 + 2t$. By Proposition 2 the series ϕ_1 and ϕ_2 can be encoded by $(p, (-\sqrt{2}, -1), y)$ and $(p, (-\sqrt{2}, -1), -y)$, respectively.

4. An effective equality test

The encoding of an algebraic series by its minimal polynomial, a total order, and its first terms is not unique, and so it is natural to ask if it is possible to decide whether two encodings represent the same series. We clarify this in this section. We begin with explaining how to compare the initial terms of two series when they are given with respect to different total orders. Let ϕ_1 and ϕ_2 be two series solutions of $p(\mathbf{x}, y) = 0$ encoded by (p, w_1, q_1) and (p, w_2, q_2) where w_1 and w_2 are elements of $\mathbb{R}^n$ inducing total orders $\preceq_1$ and $\preceq_2$ on $\mathbb{Q}^n$ and $q_1 = a_1\mathbf{x}^{\alpha_1} + \cdots + a_N\mathbf{x}^{\alpha_N}$ and $q_2 = b_1\mathbf{x}^{\beta_1} + \cdots + b_M\mathbf{x}^{\beta_M}$ are Puiseux polynomials in $\mathbf{x}$ which represent the sum of the first terms of ϕ_1 and ϕ_2 with respect to $\preceq_1$ and $\preceq_2$, respectively. Based on q_1, q_2 alone we cannot decide whether ϕ_1 equals ϕ_2 or not, even when $q_1 \neq q_2$, since there might be a term of q_2 which does not appear in q_1 because it has not been computed yet. To make sure that this is not the case, we assume that the order of the lowest order term of q_1 is at least the order of the lowest order term of q_2 with respect to w_1. Let $\sigma = (\sigma_1, \dots, \sigma_N) \in \mathfrak{S}_N$ be a permutation such that $(a_{\sigma_1}\mathbf{x}^{\alpha_{\sigma_1}}, \dots, a_{\sigma_N}\mathbf{x}^{\alpha_{\sigma_N}})$ is the sequence of terms of q_1 when ordered with respect to w_2. If $(b_1\mathbf{x}^{\beta_1}, \dots, b_M\mathbf{x}^{\beta_M})$ does not equal $(a_{\sigma_1}\mathbf{x}^{\alpha_{\sigma_1}}, \dots, a_{\sigma_M}\mathbf{x}^{\alpha_{\sigma_M}})$, then the series ϕ_1 and ϕ_2 cannot be the same. The next example demonstrates that we can also prove the equality of two series by comparing (only finitely many of) their initial terms and estimating their supports.

Example 3. The Newton polytope of

$$p(x, y, z) := x + y - (1 + x + y)z$$

has four admissible edges from each of which we can compute the first terms of a series solution of $p(x, y, z) = 0$. These series can be encoded by

$$(p, (-1 + 1/\sqrt{2}, 1), 1) \quad \text{and} \quad (p, (-1 + 1/\sqrt{2}, -1), 1), \quad \text{and}$$
$$(p, (-1 + 1/\sqrt{2}, -2), x) \quad \text{and} \quad (p, (-2 + 1/\sqrt{2}, -1), y).$$

We claim that the series ϕ_1 represented by $(p, (-1 + 1/\sqrt{2}, -2), x)$ and ϕ_2 represented by $(p, (-2 + 1/\sqrt{2}, -1), y)$ are equal. The order of y with respect to $(-1+1/\sqrt{2}, -2)$ is -2, and the terms of ϕ_1 whose

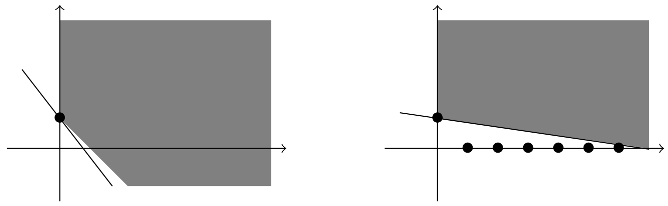

FIGURE 3. The leading exponent of the series encoded by $(p, (-2+1/\sqrt{2}, -1), y)$, the support of the first terms of $(p, (-1+1/\sqrt{2}, -2), x)$ up to the order of y with respect to $(-1+1/\sqrt{2}, -2)$, and the (shifted) cones which contain their remaining (non-depicted) supports.

order with respect to $(-1+1/\sqrt{2}, -2)$ is at least -2 are

$$x, -x^2, x^3, -x^4, x^5, -x^6, y.$$

Ordering these terms with respect to $(-2+1/\sqrt{2}, -1)$ results in the sequence

$$y, x, -x^2, x^3, -x^4, x^5, -x^6,$$

whose first term equals the first term of ϕ_2. Algorithm 1 shows that the support of ϕ_1 is contained in a shift of $\operatorname{cone}\{(0,1),(7,-1)\}$ and that the support of ϕ_2 is contained in a shift of $\operatorname{cone}\{(0,1),(1,-1)\}$. These cones are compatible in the sense that their sum is a strictly convex cone. Consequently, there is a total order $\preceq$ on $\mathbb{Q}^2$ that is compatible with both of them, and so $\mathbb{K}_{\preceq}((x,y))$ contains both ϕ_1 and ϕ_2. Since, by construction, ϕ_1 and ϕ_2 are roots of p, and since p has degree 1 with respect to z and $\mathbb{K}_{\preceq}((x,y))$ is a field and therefore can contain at most one solution of $p(x,y,z)=0$, the series ϕ_1 and ϕ_2 have to be the same. The series represented by the other encodings turn out to be different from ϕ_1 and different from each other. (Figure 3).

The reasoning in Example 3 relied on the cones output by Algorithm 1 not being too big. Although they are not always minimal, we believe that they are always in certain situations. We will have more to say about this at the end of this section and in Section 5. For the moment we just state the following conjecture.

Definition 1. A polynomial $p \in \mathbb{K}[x][y]$ is said to be content-free if the greatest common divisor of its coefficients in $\mathbb{K}[x]$ is 1.

Conjecture 1. *Let $c_1\mathbf{x}^{\alpha_1} + \cdots + c_N\mathbf{x}^{\alpha_N}$ be the sum of the first terms of a series solution ϕ of $p(\mathbf{x},\phi)=0$ output by Algorithm 1, and let C be the cone that goes with it. If $p \in \mathbb{K}[\mathbf{x}][y]$ is content-free and if N is sufficiently large, then C is minimal in the sense that there is no smaller cone satisfying*

$$\operatorname{supp}(\phi) \subseteq \{\alpha_1, \ldots, \alpha_{N-1}\} \cup (\alpha_N + C).$$

We now prove the main theorem of this section.

Theorem 1. *The equality of two algebraic series can be decided effectively.*

Proof. Let ϕ_1 and ϕ_2 be two series solutions of $p(\mathbf{x},y)=0$ encoded by (p,w_1,q_1) and (p,w_2,q_2) as above, and assume that the terms of q_2 equal the first few terms of q_1 when ordered with respect to w_2. (If this were not the case, then $\phi_1 \neq \phi_2$ and there is nothing left to show). Furthermore, assume that the lowest order term β_M of q_2 with respect to w_2 equals the lowest order term α_N of q_1 with respect to w_1. (Otherwise we extend q_2 by additional terms of ϕ_2 until it involves a term which does not appear in q_1 and extend q_1 by additional terms of ϕ_1 until again all terms of q_2 appear in q_1). Let C_1 be the cone output by Algorithm 1 such that $\operatorname{supp}(\phi_1) \subseteq \{\alpha_1,\ldots,\alpha_{N-1}\} \cup (\alpha_N + C_1)$, and let C_2 be the corresponding cone such that $\operatorname{supp}(\phi_2) \subseteq \{\beta_1,\ldots,\beta_{M-1}\} \cup (\beta_M + C_2)$. There are now two situations: either C_1 is a subset of C_2 or not. If $C_1 \subseteq C_2$, we have $w_2 \in C_1^*$, hence $\phi_1 \in \mathbb{K}_{\preceq_2}((\mathbf{x}))$, and it follows that $\phi_1 = \phi_2$ as in Example 3: the terms of q_2 being equal to the first terms of q_1 when ordered with respect to w_2 implies that ϕ_1 needs to be different from the series roots of p in $\mathbb{K}_{\preceq_2}((\mathbf{x}))$ different from ϕ_2. However, it cannot be different from ϕ_2 as $\mathbb{K}_{\preceq_2}((\mathbf{x}))$ cannot contain more than $\deg_y(p)$ many roots of p. If we assume that C_1 is the minimal cone for which $\operatorname{supp}(\phi_1) \subseteq \{\alpha_1,\ldots,\alpha_{N-1}\} \cup (\alpha_N + C_1)$, then we can also conclude that $\phi_1 \neq \phi_2$, if $C_1 \nsubseteq C_2$.

Since we do not know how to determine an N for which the cone output by Algorithm 1 is minimal (if such an N exists at all), we have to argue differently. We explain how to prove (or disprove) that $\operatorname{supp}(\phi_1) \subseteq \{\alpha_1,\ldots,\alpha_{N-1}\} \cup (\alpha_N + C_2)$ using basic properties of D-finite series. To simplify the argument we explain how to decide whether the support of an algebraic series ϕ is contained in a given rational cone C. Wlog assume that $\mathrm{supp}(\phi) \subseteq \frac{1}{k}\mathbb{Z}$. Let $\omega = (\omega_1, \dots, \omega_n) \in \mathbb{Z}^n$ be such that for each $i \in \mathbb{Z}$ there are only finitely many $\alpha \in \mathrm{supp}(\phi)$ for which $\alpha \cdot \omega = i$ and none if $i < i_0$ for some $i_0 \in \mathbb{Z}$, and consider the series

$$\tilde{\phi}(\mathbf{x}, t) := \phi(x_1 t^{\omega_1}, \dots, x_n t^{\omega_n})$$

Since ϕ is algebraic, so is $\tilde{\phi}$, and because every algebraic series is D-finite, this is also the case for $\tilde{\phi}$. Let

$$[\phi]_C(\mathbf{x}) := \sum_{I \in C \cap \mathbb{Z}^n} \left([\mathbf{x}^I]\phi\right) \mathbf{x}^I$$

be the restriction of ϕ to C, and let us denote the restriction of $\tilde{\phi}$ to $C \times \mathbb{R}_{\geq 0}$ by $[\tilde{\phi}]_C(\mathbf{x}, t) := [\phi]_C(x_1 t^{\omega_1}, \dots, x_n t^{\omega_n})$. By closure properties of D-finite functions $[\tilde{\phi}]_C$ is D-finite, and so is the difference $\tilde{\phi} - [\tilde{\phi}]_C$. In particular, when viewed as a series in t, the coefficients of $\tilde{\phi} - [\tilde{\phi}]_C$ satisfy a linear recurrence relation of the form

$$q_0(k)c_k + q_1(k)c_{k+1} + \cdots + q_r(k)c_{k+r} = 0 \tag{1}$$

with $q_0, \dots, q_r \in \mathbb{K}[\mathbf{x}][k]$, which can be explicitly computed. Whether $\mathrm{supp}(\phi) \subseteq C$ can therefore be verified by checking if $\tilde{\phi} - [\tilde{\phi}]_C = 0$, which can be done by comparing finitely many of its initial terms to zero, the number of terms which have to be computed depending on the order r of the recurrence and the largest integer root of q_r. □

Remark 2. *The equality test for algebraic series is effective because the closure properties of D-finite functions it is based on can be performed effectively. However, as was explained in* [8]*, it can be computationally quite expensive to do so. Note that it can be avoided to compute the recurrence relation* (1) *explicitly by deriving an upper bound for its order and the largest integer root of its leading coefficient polynomial and then check the equation which is to be verified for sufficiently many initial terms. However, in general these bounds are so high that this is not practible. It is therefore preferable to have an equality test based on the correctness of Conjecture 1.*

We end this section with an example that illustrates Conjecture 1.

Example 4. Let

$$p(x, y, z) := a_{000} + a_{010}y + z\left(a_{001} + a_{011}y + a_{101}x + a_{111}xy\right)$$

be a polynomial in x, y and z, and assume that its coefficients a_{ijk} are undetermined and non-zero. We apply Algorithm 1 to p, the edge $e = \{(0,0,0), (0,0,1)\}$, and any $w \in C^*(e)$ that induces a total order on $\mathbb{Q}^2$ and construct the first terms of a series solution ϕ of $p(x, y, \phi) = 0$. The slope of e with respect to the last coordinate is $-\mathrm{S}(e) = (0, 0)$, its edge polynomial is $p_e(t) = a_{000} + t a_{001}$, and so the first term of ϕ is

$$\phi_1 = -\frac{a_{000}}{a_{001}}.$$

To construct the next term of ϕ we consider

$$\begin{aligned} p(x, y, z + \phi_1) =& y\left(a_{010} - \frac{a_{000}a_{011}}{a_{001}}\right) - x\left(\frac{a_{000}a_{101}}{a_{001}} + y\frac{a_{000}a_{111}}{a_{001}}\right) \\ &+ z\left(a_{001} + a_{011}y + a_{101}x + a_{111}xy\right). \end{aligned}$$

Before we do so, we note that the algorithm implies that

$$\mathrm{supp}(\phi) \subseteq \mathrm{cone}\{(1, 0), (0, 1)\}.$$

The condition for no term other than ϕ_1 having its exponent on $\mathbb{R}_{\geq 0} \cdot (0, 1)$ is that the coefficient of y in $p(x, y, z + \phi_1)$ is zero, i.e

$$a_{010} - \frac{a_{000}a_{011}}{a_{001}} = 0,$$

or equivalently

$$\frac{a_{010}}{a_{000}} = \frac{a_{011}}{a_{001}}. \tag{2}$$

We assume that equation (2) is satisfied. Then $e_2 = \{(1,0,0), (0,0,1)\}$ is the edge of the Newton polytope of $p(x, y, z + \phi_1)$ that is used to construct the next term of ϕ. Its slope is $-\mathrm{S}(e_2) = (1, 0)$, and the corresponding edge polynomial is $p_{e_2}(t) = -\frac{a_{000}a_{101}}{a_{001}} + t a_{001}$, and so

$$\phi_2 = \frac{a_{000}a_{101}}{a_{001}^2} x.$$

Again, the algorithm predicts that

$$\operatorname{supp}(\phi) \subseteq \{(0,0)\} \cup ((1,0) + \operatorname{cone}\{(1,0),(0,1)\}),$$

and again, the condition for no term other than ϕ_2 having its exponent on $(1,0) + \mathbb{R}_{\geq 0} \cdot (0,1)$ is that the coefficient of xy in

$$p_2(x,y,z+\phi_1+\phi_2) = xy\frac{a_{000}\left(a_{011}a_{101} - a_{001}a_{111}\right)}{a_{001}^2} + x^2\left(\frac{a_{000}a_{101}^2}{a_{001}^2} + y\frac{a_{000}a_{101}a_{111}}{a_{001}^2}\right) + z\left(a_{001} + a_{011}y + a_{101}x + a_{111}xy\right)$$

equals zero. Assuming that a_{000} is different from zero, this is the case if and only if

$$\frac{a_{011}}{a_{001}} = \frac{a_{111}}{a_{101}}. \tag{3}$$

We assume that in addition to equation (2) also equation (3) holds and define

$$\lambda := \frac{a_{010}}{a_{000}} = \frac{a_{011}}{a_{001}} = \frac{a_{111}}{a_{101}}.$$

Then

$$\begin{aligned} p(x,y,z) &= a_{000} + a_{010}y + z\left(a_{001} + a_{011}y + a_{101}x + a_{111}xy\right) \\ &= a_{000} + \lambda a_{000}y + z\left(a_{001} + \lambda a_{001}y + a_{101}x + \lambda a_{101}xy\right) \\ &= a_{000}(1+\lambda y) + z\left(a_{001}(1+\lambda y) + a_{101}x(1+\lambda y)\right) \\ &= (1+\lambda y)\left(a_{000} + z\left(a_{001} + a_{101}x\right)\right), \end{aligned}$$

so p is not content-free.

5. The support

In Example 3 we saw that the number of admissible edges of the Newton polytope of a polynomial equation is not necessarily bounded by the number of series solutions the equation has. It can happen that different edges give rise to the same series solution. For the purpose of encoding a series, any edge is as good as any other edge as long as it gives rise to the same series. However, when interested in information about the support of a series solution, it is advisable to inspect all the edges which give rise to this series solution. We explain how Algorithm 1 and our effective equality test for algebraic series can be used to derive information about the convex hull of the support of an algebraic series.

Example 5. In Example 3 we saw that the Newton polytope of

$$p(x,y,z) = x + y - (1+x+y)z$$

has two admissible edges,

$$e_1 = \{(0,0,1),(1,0,0)\} \quad \text{and} \quad e_2 = \{(0,0,1),(0,1,0)\},$$

that give rise to two encodings,

$$(p, (-1+1/\sqrt{2}, -2), x) \quad \text{and} \quad (p, (-2+1/\sqrt{2}, -1), y),$$

of one and the same series solution ϕ of $p(x,y,z) = 0$. The barrier cones of these edges are

$$C(e_1) = \operatorname{cone}\{(1,0),(-1,1)\} \quad \text{and} \quad C(e_2) = \operatorname{cone}\{(0,1),(1,-1)\},$$

so that, by Algorithm 1, we have

$$\operatorname{supp}(\phi) \subseteq (1,0) + C(e_1) \quad \text{as well as} \quad \operatorname{supp}(\phi) \subseteq (0,1) + C(e_2).$$

The next proposition shows that the convex hull of the support of an algebraic series has only finitely many vertices (and hence bounded faces) and indicates how they can be found.

Proposition 3. *For every series root ϕ of a non-zero square-free polynomial $p \in \mathbb{K}[\mathbf{x}, y]$, there is a surjection from the set of edges of the Newton polytope of p which give rise to ϕ to the set of vertices of the convex hull of its support. In particular, the convex hull of the support of an algebraic series has only finitely many vertices and, as a consequence, also only finitely many bounded faces.*

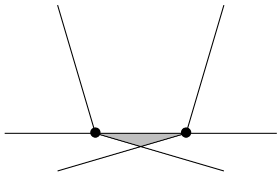

FIGURE 4. The (only) two vertices v_1, v_2 of a (not depicted) convex set $P \subseteq \mathbb{R}^2$, and two strictly-convex cones C_1, C_2 attached to them such that $P \subseteq (v_1 + C_1) \cap (v_2 + C_2)$. The complement of the line going through v_1, v_2 is the union of two open half-planes. The lower half-plane has bounded intersection with $(v_1 + C_1) \cap (v_2 + C_2)$ and does not contain any vertices of P. So $\operatorname{conv}(\{v_1, v_2\}$ is a bounded face of P.

Proof. We claim that the function that maps an edge e to the negative of its slope $-\mathrm{S}(e)$ has the required properties. If e is an edge that gives rise to the series solution ϕ, then $-\mathrm{S}(e)$ is necessarily a vertex of its support as it is the maximal element with respect to a total order induced by some irrational vector. Therefore, the function is well-defined. The function is also surjective, because for every vertex α of the convex hull of $\operatorname{supp}(\phi)$ there is some $w \in \mathbb{R}^n$ that induces a total order $\preceq$ on $\mathbb{Q}^n$ with respect to which α is the maximal element of $\operatorname{supp}(\phi)$. In particular, ϕ is an element of $\mathbb{K}_{\preceq}((\mathbf{x}))$. Since all series solutions of $p(\mathbf{x}, y) = 0$ in $\mathbb{K}_{\preceq}((\mathbf{x}))$ can be constructed by the Newton-Puiseux algorithm, see Proposition 1, there is also an edge e that gives rise to ϕ. The last statement of the proposition follows immediately as a bounded face is the convex hull of the set of vertices which are adjacent to it. □

The vertices of the convex hull of the support of ϕ can consequently be determined by identifying the admissible edges e of the Newton polytope of p that give rise to it. To determine also its bounded faces, it is helpful to be able to compute, for each of its vertices v, a strictly convex cone C_v such that $\operatorname{supp}(\phi) \subseteq v + C_v$. For each edge e that gives rise to ϕ and for every $w \in C^*(e)$ that defines a total order, Algorithm 1 provides its first N terms $a_1\mathbf{x}^{\alpha_1}, \ldots, a_N\mathbf{x}^{\alpha_N}$ with respect to w and a strictly convex cone C compatible with w such that $\operatorname{supp}(\phi) \subseteq \{\alpha_1, \ldots, \alpha_{N-1}\} \cup (\alpha_N + C)$. The cone C_{α_1} generated by C and $\{\alpha_2 - \alpha_1, \ldots, \alpha_N - \alpha_1\}$ has the property that $\operatorname{supp}(\phi) \subseteq \alpha_1 + C_{\alpha_1}$. It is also strictly convex since it is compatible with w.

Example 6. We continue Example 5. Proposition 3 implies that the vertices of the convex hull of the support of ϕ are $v_1 = (1, 0)$ and $v_2 = (0, 1)$. Apart from the vertices v_1 and v_2 itself, the only possible bounded face is the convex hull of v_1 and v_2. Since $\operatorname{supp}(\phi) \subseteq v_1 + \operatorname{cone}\{(1, 0), (-1, 1)\}$ and $\operatorname{supp}(\phi) \subseteq v_2 + \operatorname{cone}\{(0, 1), (1, -1)\}$, the line through v_1 and v_2 supports $\operatorname{conv}(\operatorname{supp}(\phi))$, and so $\operatorname{conv}(\{v_1, v_2\})$ is a face of it. See also Figure 4 (for an illustration of a slightly different example).

The candidates for the bounded faces of $\operatorname{conv}(\operatorname{supp}(\phi))$ are the convex hulls of subsets of its set of vertices. Whether such a convex hull is indeed a face can be decided based on the following proposition.

Proposition 4. *Let V be a subset of the set of vertices of* $\operatorname{conv}(\operatorname{supp}(\phi))$*, and for each $v \in V$, let C_v be a strictly convex cone such that* $\operatorname{supp}(\phi) \subseteq v + C_v$*. Assume that there is a hyperplane which contains V but no other vertices of* $\operatorname{conv}(\operatorname{supp}(\phi))$*. Furthermore, assume that its complement is the union of two half-spaces one of which has bounded intersection with $\bigcap_{v \in V}(v + C_v)$ and does not contain any vertices of* $\operatorname{conv}(\operatorname{supp}(\phi))$*. Then* $\operatorname{conv}(V)$ *is a bounded face of* $\operatorname{conv}(\operatorname{supp}(\phi))$*.*

Proof. If $\operatorname{conv}(V)$ were not a (bounded) face of $\operatorname{conv}(\operatorname{supp}(\phi))$, neither of the two (open) half-spaces would have a trivial intersection with $\operatorname{conv}(\operatorname{supp}(\phi))$. In particular, the bounded intersection of one of them with $\bigcap_{v \in V}(v + C_v)$ would be non-empty, and hence it would contain a vertex of $\operatorname{conv}(\operatorname{supp}(\phi))$. A contradiction to the assumption that this is not the case, so the hyperplane supports $\operatorname{conv}(\operatorname{supp}(\phi))$, and $\operatorname{conv}(V)$ is a bounded face of it. □

Conjecture 2. *The condition in Proposition 4 is not only a sufficient condition for* $\operatorname{conv}(V)$ *being a bounded face of* $\operatorname{conv}(\operatorname{supp}(\phi))$*. It is also a necessary one.*

Remark 3. *Note that if we can determine the bounded faces of the convex hull of the support of an algebraic series ϕ, we are able to check whether its support is bounded, i.e. whether ϕ is a Puiseux polynomial.*

We already pointed out that for deciding whether two algebraic series are equal or not, it is convenient that the cones output by Algorithm 1 are not too big. The following example shows that they do not need to be minimal.

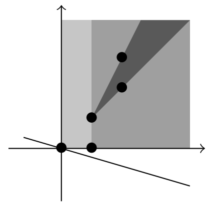

FIGURE 5. The first terms of the series ϕ from Example 9 and the (shifted) cones, as output by the Newton-Puiseux algorithm, that contain the support of the subsequent terms.

Example 7. One of the two series solutions of

$$p(x, y, z) = (1 - x)((1 - y)z - 1) = 0,$$

is the geometric series

$$\phi = 1 + y + y^2 + \dots$$

Though the convex hull of its support is the cone generated by $(1, 0)$, Algorithm 1 only shows that

$$\operatorname{supp}(\phi) \subseteq \operatorname{cone}\{(1, 0), (0, 1)\}.$$

The difference between the two cones is caused by the polynomial $p \in \mathbb{K}[x, y][z]$ not being content-free: first getting rid of its content, and then applying Algorithm 1 results in a cone that is minimal.

The non-primitivity is not the only possible reason for a cone output by Algorithm 1 not being minimal.

Example 8. One of the solutions of

$$p(x, y, z) = 1 + x + y + (1 + xy + 2y)z + yz^2 = 0$$

is

$$\frac{-1 - 2y - xy + \sqrt{1 - 2xy + 4xy^2 + x^2y^2}}{2y}.$$

It has a series expansion ϕ whose first terms with respect to $w = (-1 + 1/\sqrt{2}, -1)$ are

$$-1 - x + xy + x^2y^2 + \dots.$$

The closed form of ϕ together with Newton's binomial theorem implies that the minimal cone containing $\operatorname{supp}(\phi)$ is $\operatorname{cone}\{(1, 0), (1, 2)\}$, though Algorithm 1 only shows that it is contained in $\operatorname{cone}\{(1, 0), (0, 1)\}$. However, the algorithm also shows that

$$\operatorname{supp}(\phi) \subseteq \{(0, 0)\} \cup ((1, 0) + \operatorname{cone}\{(1, 1), (0, 1)\}),$$

where now $\operatorname{cone}\{(1, 1), (0, 1)\}$ is the minimal cone having this property, and computing another term and another cone, we find that

$$\operatorname{supp}(\phi) \subseteq \{(0, 0), (1, 0)\} \cup ((1, 1) + \operatorname{cone}\{(1, 1), (1, 2)\}),$$

where the cone $\operatorname{cone}\{(1, 1), (1, 2)\}$ is not only minimal but also has the property that its sides $(1, 1) + \mathbb{R}_{\geq 0} \cdot (1, 1)$ and $(1, 1) + \mathbb{R}_{\geq 0} \cdot (1, 2)$ contain infinitely many elements of $\operatorname{supp}(\phi)$.

For the series in the previous examples we could easily decide whether the corresponding cones given by the Newton-Puiseux algorithm were minimal or not, because the series were algebraic of degree 1 and 2, respectively, and therefore very explicit. It remains to clarify how this can be decided in general. Let $a_1\mathbf{x}^{\alpha_1}, \dots, a_N\mathbf{x}^{\alpha_N}$ be the first terms of ϕ, and let C be the cone output by Algorithm 1 such that $\operatorname{supp}(\phi) \subseteq \{\alpha_1, \dots, \alpha_{N-1}\} \cup (\alpha_N + C)$. If for each edge of $\alpha_N + C$ the exponent α_N is not the only element of $\operatorname{supp}(\phi)$ it contains, then C is minimal and its minimality can be verified simply by determining some of these elements.

Example 9. We continue Example 8. The cone $\operatorname{cone}\{(1, 1), (1, 2)\}$ for which $\operatorname{supp}(\phi) \subseteq \{(0, 0), (1, 0)\} \cup ((1, 1) + \operatorname{cone}\{(1, 1), (1, 2)\})$ is minimal because the first terms of ϕ with respect to $w = (-1 + 1/\sqrt{2}, -1)$ are

$$-1 - x + xy + x^2y^2 - x^2y^3 + \dots$$

and $(2, 2) \in (1, 1) + \mathbb{R}_{>0} \cdot (1, 1)$ and $(2, 3) \in (1, 1) + \mathbb{R}_{>0} \cdot (1, 2)$. See Figure 5.

Though this is obviously a sufficient condition, it is not a necessary one: it can happen that the cone C output by Algorithm 1 is minimal but α_N is the only element of $\operatorname{supp}(\phi)$ that lies on an edge of $\alpha_N + C$.

Example 10. Given the polynomial $p(x, y, z) = (1 - x)(z - y) - 1$, the edge $e = \{(0, 0, 1), (0, 1, 0)\}$ of its Newton polytope, the vector $w = (-1, \sqrt{2})$ and $k = 0$, Algorithm 1 returns y, the first term of the series root $\phi = y + \sum_{n=0}^{\infty} x^n$, and $C = \text{cone}\{(1, 0), (0, -1)\}$. Though C is minimal, the only element of the support of ϕ that lies on $(0, 1) + \mathbb{R} \cdot (1, 0)$ is $(0, 1)$.

Proving the minimality of a cone output by Algorithm 1 in such situations relates to the following open problem.

Problem 1. *Given an algebraic series in terms of its minimal polynomial, a total order and its first terms with respect to this order, determine the unbounded faces of the convex hull of its support.*

It is important to point out that not only the number of vertices and bounded faces of the convex hull of the support of an algebraic series is finite, but also the number of its unbounded faces. We refer the reader to [3, Theorem 1.5].

6. The number of series solutions

Part of the input of the Newton-Puiseux algorithm as specified in Section 2 are a polynomial, an admissible edge e of its Newton polytope and a vector w of the dual of its barrier cone inducing a total oder on $\mathbb{Q}^n$. It is natural to ask how the series constructed from e depend on w, i.e. whether w only affects the order in which the terms of the series are constructed. It turns out that in certain conditions the answer is affirmative.

Proposition 5. *Let e be an edge of the Newton polytope of a square-free polynomial $p \in \mathbb{K}[\mathbf{x}, y]$ whose associated edge polynomial $p_e(t)$ is square-free too. Then the set of series roots of p which result from e and an element $w \in C^*(e)$ that induces a total order on $\mathbb{Q}^n$ does not depend on the choice of w.*

Proof. Let w_1, w_2 be two elements of $C^*(e)$ whose components are linearly independent over $\mathbb{Q}$ and hence induce two total orders $\leq_1$ and $\leq_2$ on $\mathbb{Q}^n$. The field $\mathbb{K}_{\leq_1}((\mathbf{x}))$ contains $\deg_y(p)$ many series roots of which precisely the $\mathrm{M}(e)_{n+1} - \mathrm{m}(e)_{n+1}$ many series resulting from e and w_1 have the leading exponent $-\mathrm{S}(e)$. Since the edge polynomial $p_e(t)$ associated with e is square-free, the supports of these series are contained in the barrier cone $C(e)$ of e. The barrier cone is independent of w_1, so also the supports of the series roots constructed from e and w_2 are contained in $C(e)$, and therefore also these series are elements of $\mathbb{K}_{\leq_1}((\mathbf{x}))$. Since $\mathbb{K}_{\leq_1}((\mathbf{x}))$ cannot contain more than $\deg_y(p)$ many series solutions and because the leading exponents of the series roots constructed from e and w_2 are $-\mathrm{S}(e)$, the series roots constructed from e and w_1 and e and w_2 are the same. □

The following example[1] shows that the assumption of the Proposition cannot be weakened: if the edge polynomial associated with the edge e of the Newton polytope of a polynomial is not square-free, then the set of series constructed from e does not need to be independent of the choice of $w \in C^*(e)$.

Example 11. The series roots of $p(x, y, z) := 1 + x + y + 2z + z^2$ are

$$\phi_{1,2} = -1 \pm i x^{1/2} \sum_{k=0}^{\infty} \binom{1/2}{k} x^{-k} y^k \quad \text{and} \quad \phi_{3,4} = -1 \pm i y^{1/2} \sum_{k=0}^{\infty} \binom{1/2}{k} x^k y^{-k}.$$

The Newton polytope of p has three admissible edges one of which is $e = \{(0, 0, 2), (0, 0, 0)\}$. Its barrier cone is $C(e) = \text{cone}\{(1, 0), (0, 1)\}$, hence $C^*(e) = \text{cone}\{(-1, 0), (0, -1)\}$. The supports of the series roots of p imply that $C^*(e)$ decomposes into the union of $C_1 = \text{cone}\{(-1, -1), (0, -1)\}$ and $C_2 = \text{cone}\{(-1, 0), (-1, -1)\}$ such that the following holds: if $w \in C_1$, then the series constructed from e and w are ϕ_1 and ϕ_2, however, if $w \in C_2$, then these series are ϕ_3 and ϕ_4.

Remark 4. *Note that the observation made in the previous example has an unpleasant consequence concerning the computation of the vertices of the convex hull of a series root ϕ of a polynomial p: given an edge e of the Newton polytope of p, it is not enough to pick any $w \in C^*(e)$ that induces a total order on $\mathbb{Q}^n$ and to check whether e and w give rise to a series root of p that equals ϕ since the latter depend on w. It is not clear what the right choice of w is.*

Proposition 5 implies that under the condition that the edge polynomials of the admissible edges of the Newton polytope of a polynomial are square-free, the polynomial has only finitely many series roots. We believe that the latter is true in general and that the following conjecture holds.

---

[1] This example was pointed out by one of the reviewers to whom we express our sincere thanks.

Conjecture 3. *For each edge e of the Newton polytope of $p \in \mathbb{K}[\mathbf{x}, y]$, let w_e be any element of $C^*(e)$ which induces a total order on $\mathbb{Q}^n$. Then the list of series roots of p that results from e and w_e when e ranges over all admissible edges of the Newton polytope of p is exhaustive. In particular, p has only finitely many series roots.*

Having proven that a polynomial equation has only finitely many series solutions, at least in certain situations, it is natural to ask how to describe their number.

Problem 2. *Find a formula for the number of series solutions of a polynomial equation. Can it be related to any statistics of its Newton polytope?*

The next Proposition provides an answer to Problem 2 for polynomials of degree 1.

Proposition 6. *Let $p, q \in \mathbb{K}[\mathbf{x}]$ and let $\preceq$ be an additive total order. The series solution of*

$$p(\mathbf{x}) - q(\mathbf{x})y = 0$$

in $\mathbb{K}_{\preceq}((\mathbf{x}))$ depends on $\preceq$ only to the extent of what the leading term $\mathrm{lt}_{\preceq}(q)$ of q with respect to it is. It is

$$\frac{p}{\mathrm{lt}_{\preceq}(q)} \sum_{k=0}^{\infty} \left(1 - \frac{q}{\mathrm{lt}_{\preceq}(q)}\right)^k, \tag{4}$$

and its support is contained in a shift of the cone generated by the support of $q/\mathrm{lt}_{\preceq}(q)$. In particular, there is a bijection between the series solutions of the equation and the vertices of the Newton polytope of q.

Proof. Consider the Laurent polynomial $q/\mathrm{lt}_{\preceq}(q)$, and let C be the (strictly convex) cone generated by its support. Since $q/\mathrm{lt}_{\preceq}(q)$ is an element of $\mathbb{K}_C[[\mathbf{x}]]$, and because its constant term is different from zero, it has a multiplicative inverse in $\mathbb{K}_C[[\mathbf{x}]]$, see [18, Theorem 12]. Since $\mathbb{K}_C[[\mathbf{x}]]$ is an integral domain [18, Theorem 11], this multiplicative inverse is unique. As a consequence, the series solution of $p(\mathbf{x}) + q(\mathbf{x})y$ in $\mathbb{K}_{\preceq}((\mathbf{x}))$ depends on the total order $\preceq$ only to the extent of what $\mathrm{lt}_{\preceq}(q)$ is. The terms of q that appear as the leading term with respect to some additive total order are those whose exponent is a vertex of the Newton polytope of q. The number of series solutions is therefore bounded by the number of vertices the Newton polytope has. To see that these numbers are equal, it is sufficient to observe that the series solution in $\mathbb{K}_{\preceq}((\mathbf{x}))$ is the geometric series expansion of p/q given by (4), and to note that for an additive total order for which q has another leading term the corresponding series is different. The statement about the support is obvious from the explicit expression of the series. ☐

Example 12. The equation

$$x + y - (1 + x + y)z = 0$$

has three series solutions as the Newton polytope of $1 + x + y$ has three vertices: $(x + y)\sum_{k=0}^{\infty}(-1)^k(x + y)^k$, $\frac{x+y}{x}\sum_{k=0}^{\infty}(-1)^k\left(\frac{1+y}{x}\right)^k$ and $\frac{x+y}{y}\sum_{k=0}^{\infty}(-1)^k\left(\frac{1+x}{y}\right)^k$. Their supports are contained in shifts of $\mathrm{cone}\{(1, 0), (0, 1)\}$, $\mathrm{cone}\{(-1, 0), (-1, 1)\}$ and $\mathrm{cone}\{(0, -1), (1, -1)\}$, respectively.

7. Effective arithmetic

Given encodings of two series ϕ_1 and ϕ_2, we discuss how to decide whether their sum $\phi_1 + \phi_2$ and product $\phi_1\phi_2$ are well-defined and hence algebraic, and in case they are, how to determine finite encodings for them.

We first recall that in general the sum and product of two algebraic series do not need to be algebraic as they do not even need to be well-defined.

Example 13. The geometric series $\phi_1 = 1 + x + x^2 + \ldots$ and $\phi_2 = -x^{-1} - x^{-2} - x^{-3} - \ldots$ we have met in Example 1 are both algebraic as they are the series roots of

$$p(x, y) := (1 - x)y - 1,$$

but neither is their sum nor their product as none of them is well-defined.

The sum and product of two algebraic series ϕ_1 and ϕ_2 are algebraic if and only if there is a vector $w \in \mathbb{R}^n$ that induces a total order $\preceq$ on $\mathbb{Q}^n$ with respect to which both $\mathrm{supp}(\phi_1)$ and $\mathrm{supp}(\phi_2)$ have a maximal element. To decide whether such a vector exists, and in case it does, to find it, one would need to determine $\mathrm{conv}(\mathrm{supp}(\phi_1))$ and $\mathrm{conv}(\mathrm{supp}(\phi_2))$. However, we are only able to determine an estimate of the convex hull of the support of an algebraic series (see Section 5, in particular Problem 1), and so we can find such a vector only sometimes but not always when it exists. In particular, in case we cannot find one, it does not mean there is none. Yet, under the assumption that that the statement of Conjecture 3 holds, we can prove that the sum (and product) of ϕ_1 and ϕ_2 is not algebraic, by computing an annihilating polynomial p for the potentially algebraic series $\phi_1+\phi_2$ and observe that none of its series roots equals the sum of ϕ_1 and ϕ_2.

Example 14. Let

$$p_1 := (1+x+x^2-y)(x^2-(1-x)y) \quad \text{and} \quad p_2 := y(x^2-(x-1)y)$$

and consider the series

$$\phi_1 = x^2+x^3+x^4+\dots \quad \text{and} \quad \phi_2 = x+1+x^{-1}\dots$$

encoded by

$$(p_1, -\sqrt{2}, x^2) \quad \text{and} \quad (p_2, \sqrt{2}, x).$$

We can show that $\phi_1+\phi_2$ is not algebraic by computing the generator

$$p = \left(1+x+x^3-y\right) y \left(-1+x^2+x^4-(x-1)y\right) \left(x^3-(1-x)y\right)$$

of the elimination ideal $\langle p_1(x,y_1),\ p_2(x,y_2),\ y_1+y_2-y_3\rangle \cap \mathbb{K}(x)[y_3]$ and observing that none of its roots equals $\phi_1+\phi_2$. For instance, the series ϕ represented by $(p,-\sqrt{2},x^2)$ is different from $\phi_1+\phi_2$ because $\operatorname{supp}(\phi_1) \subseteq 2+\mathbb{R}_{\geq 0}$ and $\operatorname{supp}(\phi_2) \subseteq 1+\mathbb{R}_{\leq 0}$ and so $1 \in \operatorname{supp}(\phi_1+\phi_2)$ but $1 \notin \operatorname{supp}(\phi)$ as $\operatorname{supp}(\phi) \subseteq 2+\mathrm{R}_{\geq 0}$. The series ϕ encoded by $(p,\sqrt{2},x^2+2x)$ does not equal $\phi_1+\phi_2$ because the terms of ϕ_1 and ϕ_2 of order at least $-\sqrt{2}\cdot 2$ and $\sqrt{2}\cdot 1$ with respect to $-\sqrt{2}$ and $\sqrt{2}$ are x^2 and x, respectively, and their sum x^2+x differs from x^2+2x. Similar arguments apply for showing that the other series roots of p do not equal $\phi_1+\phi_2$, proving that the sum of ϕ_1 and ϕ_2 is not algebraic.

In the following we circumvent these difficulties simply by assuming that we know a $w \in \mathbb{R}^n$ that induces a total order $\preceq$ for which $\phi_1, \phi_2 \in \mathbb{K}_{\preceq}((\mathbf{x}))$ so that e.g. $\phi_1+\phi_2$ is algebraic and we can be sure to find it among the series roots of p. This assumption looks very restrictive, but it happens to be satisfied in applications, and it was satisfied in the context of the orbit-sum method, a method for solving discrete differential equations [11, 9, 7], which was the starting point of this work.

Assume that ϕ_1 and ϕ_2 are two series given by (p_1,w,q_1) and (p_2,w,q_2). We already noted that an annihilating polynomial p for $\phi_1+\phi_2$ can be derived from annihilating polynomials p_1 and p_2 of ϕ_1 and ϕ_2 by computing a generator of the elimination ideal of

$$\langle p_1(\mathbf{x},y_1),\ p_2(\mathbf{x},y_2),\ y_1+y_2-y_3\rangle \cap \mathbb{K}(\mathbf{x})[y_3].$$

Whether a series root of p represented by (p,w,q) equals $\phi_1+\phi_2$ can be decided by computing the truncations $\tilde{q}_1$ and $\tilde{q}_2$ of ϕ_1 and ϕ_2 up to order $\operatorname{ord}(q,w)$, where

$$\operatorname{ord}(q,w) := \min\{\alpha \cdot w \mid \alpha \in \operatorname{supp}(q)\}.$$

If $\tilde{q}_1+\tilde{q}_2$ does not equal q when ordered with respect to w, the series represented by (p,w,q) does not equal $\phi_1+\phi_2$. But if it does, then (p,w,q) is a finite encoding of $\phi_1+\phi_2$, and by assumption we can be sure that we find a finite encoding of it this way.

Similarly, an annihilating polynomial p for $\phi_1\phi_2$ can be determined by computing a generator of the elimination ideal

$$\langle p_1(\mathbf{x},y_1),\ p_2(\mathbf{x},y_2),\ y_1y_2-y_3\rangle \cap \mathbb{K}(\mathbf{x})[y_3].$$

To find a representation (p,w,q) of $\phi_1\phi_2$ compute the truncation $\tilde{q}_1$ of ϕ_1 up to order $\operatorname{ord}(q,w) - w \cdot \operatorname{lexp}_w(\phi_2)$ and the truncation $\tilde{q}_2$ of ϕ_2 up to order $\operatorname{ord}(q,w) - w \cdot \operatorname{lexp}_w(\phi_1)$, where $\operatorname{lexp}_w(\phi_i)$ denotes the leading exponent of ϕ_i with respect to the total order induced by w. If q does not equal the sum of the first terms of $\tilde{q}_1\tilde{q}_2$ when ordered with respect to w, the series represented by (p,w,q) does not equal $\phi_1\phi_2$. However, if it does, then (p,w,q) is a finite encoding of $\phi_1\phi_2$, and by assumption we can be sure that we find a finite encoding of it this way.

Other closure properties for algebraic series such as taking multiplicative inverses or derivatives can be performed similarly. We just refer to [14, Theorem 6.3] for an explanation of how the corresponding annihilating polynomials can be computed.

Acknowledgement

Thanks go to the Austrian FWF which supported part of this work with the grants F5004 and P31571-N32. Thanks also go to the author's colleagues Christoph Koutschan, Anton Ponomarchuk and Josef Schicho at the Austrian Academy of Sciences and Manuel Kauers and Thibaut Verron at the Johannes Kepler University Linz. Many thanks go to the reviewers who read the article very carefully and gave valuable feedback.

References

[1] Maria Emilia Alonso, Francisco J Castro-Jiménez, and Herwig Hauser. Encoding algebraic power series. *Foundations of Computational Mathematics*, 18(3):789–833, 2018.

[2] María Emilia Alonso, Teo Mora, and Mario Raimondo. A computational model for algebraic power series. *Journal of pure and applied algebra*, 77(1):1–38, 1992.

[3] Fuensanta Aroca, Julie Decaup, and Guillaume Rond. The minimal cone of an algebraic Laurent series. *Mathematische Annalen*, 382(3):1745–1773, 2022.

[4] Fuensanta Aroca and Giovanna Ilardi. A family of algebraically closed fields containing polynomials in several variables. *Communications in Algebra*, 37(4):1284–1296, 2009.

[5] Fuensanta Aroca, Giovanna Ilardi, and Lucía López de Medrano. Puiseux power series solutions for systems of equations. *International Journal of Mathematics*, 21(11):1439–1459, 2010.

[6] Fuensanta Aroca and Guillaume Rond. Support of Laurent series algebraic over the field of formal power series. *Proceeding of the London Mathematical Society*, 118(3):577–605, 2019.

[7] Alin Bostan, Mireille Bousquet-Mélou, and Stephen Melczer. Counting walks with large steps in an orthant. *Journal of the European Mathematical Society*, 23(7):2221–2297, 2021.

[8] Alin Bostan, Frédéric Chyzak, Mark Van Hoeij, Manuel Kauers, and Lucien Pech. Hypergeometric expressions for generating functions of walks with small steps in the quarter plane. *European Journal of Combinatorics*, 61:242–275, 2017.

[9] Mireille Bousquet-Mélou and Marni Mishna. Walks with small steps in the quarter plane. *Contemp. Math*, 520:1–40, 2010.

[10] Egbert Brieskorn and Horst Knörrer. *Plane Algebraic Curves*. Springer Science & Business Media, 2012.

[11] Manfred Buchacher and Manuel Kauers. The orbit-sum method for higher order equations. *arXiv preprint arXiv:2211.08175*, 2022.

[12] Jan Denef and Leonard Lipshitz. Algebraic power series and diagonals. *Journal of Number Theory*, 26(1):46–67, 1987.

[13] Michel Hickel and Mickaël Matusinski. About algebraic puiseux series in several variables. *Journal of Algebra*, 527:55–108, 2019.

[14] Manuel Kauers and Peter Paule. *The concrete tetrahedron*, volume 11. Springer, Wien, 2011.

[15] Leonard Lipshitz. D-finite power series. *Journal of algebra*, 122(2):353–373, 1989.

[16] John McDonald. Fiber polytopes and fractional power series. *Journal of Pure and Applied Algebra*, 104(2):213–233, 1995.

[17] John McDonald. Fractional power series solutions for systems of equations. *Discrete and Computational Geometry*, 27(4):501–530, 2002.

[18] Ainhoa Aparicio Monforte and Manuel Kauers. Formal Laurent series in several variables. *Expositiones Mathematicae*, 31(4):350–367, 2013.

[19] Adrien Poteaux and Marc Rybowicz. Improving complexity bounds for the computation of puiseux series over finite fields. In *Proceedings of the 2015 ACM on International Symposium on Symbolic and Algebraic Computation*, pages 299–306, 2015.

[20] Victor Puiseux. *Recherches sur les fonctions algébriques*. 1850.

[21] Victor Saavedra. The McDonald theorem in positive characteristic. *Journal of Algebra*, 491:219–240, 2017.

[22] P Walsh. A polynomial-time complexity bound for the computation of the singular part of a puiseux expansion of an algebraic function. *Mathematics of Computation*, 69(231):1167–1182, 2000.

[23] Güter M. Ziegler. *Lectures on Polytopes*. Springer-Verlag New York, 1994.