Effective power series computations[*]

by Joris van der Hoeven

CNRS, LIX, École polytechnique
91128 Palaiseau Cedex
France

Email: vdhoeven@lix.polytechnique.fr

Final version of June 15, 2019

Abstract

Let K be an effective field of characteristic zero. An effective tribe is a subset of $K[[z_1, z_2, \ldots]] = K \cup K[[z_1]] \cup K[[z_1, z_2]] \cup \cdots$ that is effectively stable under the K-algebra operations, restricted division, composition, the implicit function theorem, as well as restricted monomial transformations with arbitrary rational exponents. Given an effective tribe with an effective zero test, we will prove that an effective version of the Weierstrass division theorem holds inside the tribe, and that this can be used for the computation of standard bases.

Keywords: Power series, algorithm, Weierstrass preparation, standard basis, d-algebraic power series, tribe

A.M.S. subject classification: 68W30, 03C60

1 Introduction

There are two main aspects about effective computations with formal power series. On the one hand, we need fast algorithms for the computation of coefficients. There is an important literature on this subject and the asymptotically fastest methods either rely on Newton's method [4] or on relaxed power series evaluation [12].

On the other hand, there is the problem of deciding whether a given power series is zero. This problem is undecidable in general, since we need to check the cancellation of an infinite number of coefficients. Therefore, a related subject is the isolation of sufficiently large classes of power series such that most of the common operations on power series can be carried out inside the class, but such that the class remains sufficiently restricted such that we can design effective zero tests.

The abstract description of a suitable framework for power series computations is the subject of section 2. We first recall the most common operations on formal power series over a field K of characteristic zero: the K-algebra operations, restricted division, composition, the resolution of implicit equations, and so called restricted monomial transformations with arbitrary rational exponents. A subset L of $K[[z_1, z_2, \ldots]] = K \cup K[[z_1]] \cup K[[z_1, z_2]] \cup \cdots$ that is stable under each of these operations will be called a tribe. We will also specify effective counterparts of these notions.

The main results of this paper are as follows. Given an effective tribe with an effective zero test, we show in section 4 that the tribe also satisfies an effective version of the Weierstrass preparation theorem [23], and we give an algorithm for performing Weierstrass division with remainder. In section 5, we also introduce "Weierstrass bases" and a recursive version of Weierstrass division that works for ideals. For Archimedean monomial orderings, this can in turn be used for the computation of standard bases of ideals generated by series in the tribe in the sense of Hironaka [10].

[*]. This work has been supported by the ANR-10-BLAN 0109 LEDA project.

Our results can for instance be applied to the tribe of algebraic power series. In that particular case, various alternative algorithms have been developed. An algorithm for Weierstrass division was given in [2]. This algorithm has recently been extended to the computation of reduced standard bases of ideals that satisfy a suitable condition [1] (namely Hironaka's box condition). In the case that the ideals are generated by polynomials instead of power series, one may compute (non-reduced) standard bases using Mora's tangent cone algorithm [20] or Lazard's homogenization technique [17].

The main other example that motivated our work is the tribe of d-algebraic power series (see also [7, 8, 15]). The fact that the collection of all d-algebraic power series satisfies the Weierstrass preparation theorem was first proved in a more *ad hoc* way by van den Dries [9]. The notion of a tribe also shares some common properties with the notion of a Weierstrass system, as introduced by Denef and Lipshitz [6] and used in [9]. Our approach can be regarded as a simpler, effective and more systematic way to prove that certain types of power series form Weierstrass systems. Moreover, we show how to compute more general standard bases in this context.

The idea behind our main algorithm for the computation of Weierstrass polynomials is very simple: given a series $f \in L \cap K[[z_1, \ldots, z_n]]$ of Weierstrass degree d in z_1, we just compute the solutions $\varphi_1, \ldots, \varphi_d$ of the equation $f(z_1, \ldots, z_n) = 0$ in z_1 inside a sufficiently large field of grid-based power series. This allows us to compute the polynomial $P = (z_1 - \varphi_1) \cdots (z_1 - \varphi_d)$ which we *know* to be the Weierstrass polynomial associated to f. Using the stability of the tribe under restricted monomial transformations, we will be able to compute P as an element of L.

The algorithms rely on our ability to compute with the auxiliary grid-based power series $\varphi_1, \ldots, \varphi_d$. For this reason, we briefly recall some basic facts about grid-based power series in section 3, as well as the basic techniques that are needed in order to compute with them.

Weierstrass division is a precursor of the more general notion of Hironaka division in the particular case of a principal ideal in general position. For arbitrary ideals in general position (or, more precisely, in "Weierstrass position"), we introduce a recursive version of Weierstrass division in section 5. Assuming that such an ideal I is finitely generated by elements in the tribe L, this allows us to compute a "Weierstrass basis" for I and to decide ideal membership for other elements of I. Another application is the computation of the Hilbert function of I. The main ingredients in section 5 are the possibility to put ideals in Weierstrass position modulo a suitable linear change of variables and ordinary Weierstrass division in the principal ideal case. For tribes in which we have alternative algorithms for the Weierstrass preparation theorem, the techniques of section 5 can use these algorithms instead of the ones from section 4.

In the last section 6, we show how to compute more traditional standard bases of ideals I that are finitely generated by elements of L. The main difficulty with standard bases in the power series setting (in contrast to Gröbner bases in the polynomial setting) is termination. This difficulty is overcome by using the fact that we may compute the Hilbert function of the ideal using the techniques from section 5. During the construction of a standard basis, this essentially allows us to decide whether the S-series of two basis elements reduces to zero or whether it reduces to a series of high valuation. In general, our algorithm does not compute a reduced standard basis: it is actually known that such a reduced standard basis does not necessarily exist. An interesting open question is under which conditions our algorithm still does compute one. In the algebraic setting, we already mentioned above that [1] furnishes a conditional algorithm for the computation of reduced standard bases.

Our paper uses several notations from the theory of grid-based power series [13] that are uncommon in the area of standard bases. For instance, admissible orderings are replaced by monomial orderings, initial monomials by dominant monomials, and Weierstrass position is reminiscent of Hironaka's box condition that is essential in [1]. The general motivation behind our notations is their natural asymptotic meaning. They have been very useful for the development of asymptotic differential algebra and we refer the reader to [3] for a more extensive background and dictionary.

Acknowledgments. The author wishes to express his gratitude to the two referees for their careful reading and helpful comments, as well as to Alin Bostan and Lou van den Dries for historical references.

2 Common operations on power series

Let K be a field of characteristic zero and denote

$$K[[z_1, z_2, \ldots]] \;=\; K \cup K[[z_1]] \cup K[[z_1, z_2]] \cup \cdots,$$

where we understand that $K[[z_1, \ldots, z_n]]$ is naturally included in $K[[z_1, \ldots, z_{n+1}]]$ for each n. So each element $f \in K[[z_1, z_2, \ldots]]$ is a power series in a finite number of variables.

We say that K is *effective* if its elements can be represented by concrete data structures and if all field operations can be carried out by algorithms. We say that K *admits an effective zero test* if we also have an algorithm that takes $f \in K$ as input and that returns **true** if $f = 0$ and **false** otherwise.

If K is effective, then a power series $f \in K[[z_1, z_2, \ldots]]$ is said to be *computable* if we have an effective bound n for its dimension (so that $f \in K[[z_1, \ldots, z_n]]$), together with an algorithm that takes $i \in \mathbb{N}^n$ as input and produces the coefficient $f_i \in K$ of $z^i = z_1^{i_1} \cdots z_n^{i_n}$ on output. We will denote the set of computable power series by $K[[z_1, z_2, \ldots]]^{\mathrm{com}}$.

Basic operations on power series

Let L be a subset of $K[[z_1, z_2, \ldots]]$. We will denote $L_n = L \cap K[[z_1, \ldots, z_n]]$ for each n and say that L is *effective* if $L \subseteq K[[z_1, z_2, \ldots]]^{\mathrm{com}}$. In this section, we will give definitions of several operations on power series and the corresponding closure properties that L may satisfy. We say that L is a *power series algebra* if L is a K-algebra. From now on, we will always assume that this is the case. It is also useful to assume that L is *inhabited* in the sense that $z_i \in L$ for all i. For each i, we will denote $\partial_i = \partial / \partial z_i$ and $\delta_i = z_i \partial_i$. We say that L is *stable under differentiation* if $\partial_i L \subseteq L$ for all i (whence $\delta_i L \subseteq L$).

The above closure properties admit natural effective analogues. We say that L is an *effective power series algebra* if K is an effective field, if the elements of L can be represented by concrete data structures and the K-algebra operations can be carried out by algorithms. We say that L is *effectively inhabited* if there is an algorithm that takes $i \in \mathbb{N}$ as input and that computes $z_i \in L$. We say that L is *effectively stable under differentiation* if there exists an algorithm that takes $f \in L$ and $i \in \mathbb{N}$ as input and that computes $\partial_i f \in L$.

Restricted division

For any ring R, let $R^{\neq} = R \setminus \{0\}$. We say that L is *stable under restricted division* if $f / g \in L$ whenever $f \in L$ and $g \in L^{\neq}$ are such that $f / g \in K[[z_1, z_2, \ldots]]$. If L is effective, then we say that L is *effectively stable under restricted division* if we also have an algorithm that computes f / g as a function of $f, g \in L$, whenever $f / g \in K[[z_1, z_2, \ldots]]$. Here we do *not* assume the existence of a test whether $f / g \in K[[z_1, z_2, \ldots]]$ (the behaviour of the algorithm being unspecified if $f / g \notin K[[z_1, z_2, \ldots]]$). More generally, given $g \in L^{\neq}$, we say that L is *stable under restricted division by g* if $f / g \in L$ whenever $f / g \in K[[z_1, z_2, \ldots]]$, and that L is *effectively stable under restricted division by g* if this division can be carried out by an algorithm.

Composition

Given $f\in K[[z]]=K[[z_1,\ldots,z_n]]$, we let $f(0)\in K$ denote the evaluation of f at $0=(0,\ldots,0)$. Given $f\in K[[z]]$ and $g_1,\ldots,g_n\in K[[u]]=K[[u_1,\ldots,u_p]]$ with $g_1(0)=\cdots=g_n(0)=0$, we define the composition $f\circ g=f\circ(g_1,\ldots,g_n)$ of f and g to be the unique power series $f\circ g\in K[[u_1,\ldots,u_p]]$ with

$$(f\circ g)(u_1,\ldots,u_p)=f(g(u_1,\ldots,u_p),\ldots,g(u_1,\ldots,u_p)).$$

We say that a power series domain $L\subseteq K[[z_1,z_2,\ldots]]$ is *stable under composition* if $f\circ(g_1,\ldots,g_n)\in L$ for any $f\in L_n$ and $g_1,\ldots,g_n\in L$ with $g_1(0)=\cdots=g_n(0)=0$. If we also have an algorithm for the computation of $f\circ(g_1,\ldots,g_n)$, then we say that L is *effectively stable under composition*.

We notice that stability under composition implies stability under permutations of the z_i. In particular, it suffices that $z_1\in L$ for L to be inhabited. Stability under composition also implies stability under the projections π_i with

$$(\pi_i f)(z_1,\ldots,z_n)=f(z_1,\ldots,z_{i-1},0,z_{i+1},\ldots,z_n).$$

If L is also stable under restricted division by z_1 (whence under restricted division by any z_i), then this means that we may compute the coefficients $[z_i^k]\,f$ of the power series expansion of f with respect to z_i by induction over k:

$$[z_i^k]\,f=\pi_i\frac{f-[z_i^0]\,f-\cdots-([z_i^{k-1}]\,f)\,z_i^{k-1}}{z_i^k}.$$

Similarly, we obtain stability under the differentiation: for any $f\in L_n$ and $i\leqslant n$, we have

$$(\partial_i f)(z_1,\ldots,z_n)\;=\;\pi_{n+1}\frac{f(z_1,\ldots,z_{i-1},z_i+z_{n+1},z_{i+1},\ldots,z_n)-f(z_1,\ldots,z_n)}{z_{n+1}}.$$

Implicit functions

Let $\varphi_1,\ldots,\varphi_m\in K[[z_1,\ldots,z_n]]$ with $p=n-m>0$ and $\varphi_1(0)=\cdots=\varphi_m(0)=0$. Assume that the matrix formed by the first m columns of the scalar matrix

$$\frac{\partial\varphi}{\partial z}(0)\;=\;\begin{pmatrix}\frac{\partial\varphi_1}{\partial z_1}(0) & \cdots & \frac{\partial\varphi_1}{\partial z_n}(0)\\ \vdots & & \vdots\\ \frac{\partial\varphi_m}{\partial z_1}(0) & \cdots & \frac{\partial\varphi_m}{\partial z_n}(0)\end{pmatrix}$$

is invertible. Then the implicit function theorem implies that there exist unique power series $\psi_1,\ldots,\psi_m\in K[[z_1,\ldots,z_p]]$, such that the completed vector $\psi=(\psi_1,\ldots,\psi_n)$ with $\psi_{m+1}=z_1,\ldots,\psi_n=z_p$ satisfies $\varphi\circ\psi=0$. We say that a power series domain $L\subseteq K[[z_1,z_2,\ldots]]$ *satisfies the implicit function theorem* (for m implicit functions) if $\psi_1,\ldots,\psi_m\in L$ for the above solution of $\varphi\circ\psi=0$, whenever $\varphi_1,\ldots,\varphi_m\in L_n$. We say that L *effectively satisfies the implicit function theorem* if we also have an algorithm to compute $\psi_1,\ldots,\psi_m$ as a function of $\varphi_1,\ldots,\varphi_m$.

We claim that L satisfies the implicit function theorem for m implicit functions as soon as L satisfies the implicit function theorem for one implicit function and L is stable under restricted division and composition. We prove this by induction over m. For $m=1$ the statement is clear, so assume that $m>1$. Since the matrix formed by the first m columns of $(\partial\varphi/\partial z)(0)$ is invertible, at least one of the $(\partial\varphi_i/\partial z_1)(0)$ must be non-zero. Modulo a permutation of rows we may assume that $(\partial\varphi_1/\partial z_1)(0)\neq 0$. Applying the implicit function theorem to φ_1 only, we obtain a function $\xi\in L_{n-1}$ with $\varphi_1\circ(\xi,z_1,\ldots,z_{n-1})=0$. Differentiating this relation, we also obtain

$$\frac{\partial\xi}{\partial z_j} = -\frac{\partial\varphi_1/\partial z_{j+1}}{\partial\varphi_1/\partial z_1}\circ(\xi,z_1,\ldots,z_{n-1}),$$

for each j. Setting $\lambda:=1/(\partial\varphi_1/\partial z_1)(0)$, this yields in particular

$$\frac{\partial\xi}{\partial z_j}(0) = -\lambda\frac{\partial\varphi_1}{\partial z_{j+1}}(0).$$

Now consider the series $\varphi_i'=\varphi_{i+1}\circ(\xi,z_1,\ldots,z_{n-1})\in L$. For each $j\leqslant m-1$, we have

$$\begin{aligned}\frac{\partial\varphi_i'}{\partial z_j}(0) &= \frac{\partial\xi}{\partial z_j}(0)\frac{\partial\varphi_{i+1}}{\partial z_1}(0)+\frac{\partial\varphi_{i+1}}{\partial z_{j+1}}(0)\\ &= \frac{\partial\varphi_{i+1}}{\partial z_{j+1}}(0)-\lambda\frac{\partial\varphi_1}{\partial z_{j+1}}(0)\frac{\partial\varphi_{i+1}}{\partial z_1}(0).\end{aligned}$$

In particular,

$$\begin{vmatrix}\frac{\partial\varphi_1'}{\partial z_1}(0) & \cdots & \frac{\partial\varphi_1'}{\partial z_{m-1}}(0)\\ \vdots & & \vdots\\ \frac{\partial\varphi_{m-1}'}{\partial z_1}(0) & \cdots & \frac{\partial\varphi_{m-1}'}{\partial z_{m-1}}(0)\end{vmatrix} = \lambda\begin{vmatrix}\frac{\partial\varphi_1}{\partial z_1}(0) & \cdots & \frac{\partial\varphi_1}{\partial z_m}(0)\\ \vdots & & \vdots\\ \frac{\partial\varphi_m}{\partial z_1}(0) & \cdots & \frac{\partial\varphi_m}{\partial z_m}(0)\end{vmatrix}\neq 0.$$

By the induction hypothesis, we may thus compute series $\psi_2,\ldots,\psi_m\in L_p$ such that $\varphi_i'\circ(\psi_2,\ldots,\psi_m,z_1,\ldots,z_p)=0$ for all i. Setting $\psi_1=\xi\circ(\psi_2,\ldots,\psi_m,z_1,\ldots,z_p)\in L_p$, we conclude that $\varphi_1\circ(\psi_1,\ldots,\psi_m,z_1,\ldots,z_p)=\varphi_1\circ(\xi,z_1,\ldots,z_{n-1})\circ(\psi_2,\ldots,\psi_m,z_1,\ldots,z_p)=0$ and

$$\begin{aligned}\varphi_{i+1}\circ(\psi_1,\ldots,\psi_m,z_1,\ldots,z_p) &= \varphi_{i+1}\circ(\xi,z_1,\ldots,z_{n-1})\circ(\psi_2,\ldots,\psi_m,z_1,\ldots,z_p)\\ &= \varphi_i'\circ(\psi_2,\ldots,\psi_m,z_1,\ldots,z_p)\\ &= 0\end{aligned}$$

for all $i\leqslant m-1$.

Restricted monomial transformations

Consider an invertible $n\times n$ matrix $M\in\mathbb{Q}^{n\times n}$ with rational coefficients. Then the transformation

$$\begin{aligned}\cdot\circ z^M\colon z_1^{\mathbb{Q}}\cdots z_n^{\mathbb{Q}} &\longrightarrow z_1^{\mathbb{Q}}\cdots z_n^{\mathbb{Q}}\\ z^i &\longmapsto z^{M\cdot i}\end{aligned}$$

is called a monomial transformation, where $i\in\mathbb{Q}^n$ is considered as a column vector. For a power series $f\in K[[z_1,\ldots,z_n]]$ whose support $\operatorname{supp} f=\{i\in\mathbb{N}^n : f_i\neq 0\}$ satisfies $M\cdot\operatorname{supp} f\subseteq\mathbb{N}^n$, we may apply the monomial transformation to f as well:

$$f\circ z^M = \sum_{i\in\mathbb{N}^n} f_i\, z^{M\cdot i}.$$

We say that L is *stable under restricted monomial transformations* if for any $f \in L_n$ and invertible matrix $M \in \mathbb{Q}^{n \times n}$ with $M \cdot \operatorname{supp} f \subseteq \mathbb{N}^n$, we have $f \circ z^M \in L_n$. We say that L is *effectively stable under restricted monomial transformations* if we also have an algorithm to compute $f \circ z^M$ as a function of f and M. Notice that we do *not* require the existence of a test whether $M \cdot \operatorname{supp} f \subseteq \mathbb{N}^n$ in this case (the behaviour of the algorithm being unspecified whenever $M \cdot \operatorname{supp} f \nsubseteq \mathbb{N}^n$).

If $M \in \mathbb{N}^{n \times n}$ has non-negative integer coefficients, then we always have $M \cdot \operatorname{supp} f \subseteq \mathbb{N}^n$ and L is trivially stable under the monomial transformation $f \mapsto f \circ z^M$ whenever L is stable under composition.

Examples

We say that the K-algebra L with $z_1 \in L$ is a *local community* if L is stable under composition, the resolution of implicit equations, and restricted division by z_1. We say that L is a *tribe* if L is also stable under restricted division and restricted monomial transformations. Effective local communities and tribes are defined similarly.

A power series $f \in K[[z_1, z_2, \ldots]]$ is said to be *algebraic* if it satisfies a non-trivial algebraic equation over the polynomial ring $K[z_1, z_2, \ldots] = K \cup K[z_1] \cup K[z_1, z_2] \cup \cdots$. Setting $H = K(z_1, z_2, \ldots) = K \cup K(z_1) \cup K(z_1, z_2) \cup \cdots$, this is the case if and only if the module $H[f]$ is an H-vector space of finite dimension. Using this criterion, one can prove that the set $K[[z_1, z_2, \ldots]]^{\mathrm{alg}}$ of algebraic power series is a tribe (and actually the smallest tribe for inclusion). For convenience of the reader, let us state and prove an effective version of this result. Assume that K is an effective field. Then an effective algebraic power series $f \in K[[z_1, z_2, \ldots]]$ can be effectively represented as an effective power series together with an annihilator $P \in H[F]$. We claim that $K[[z_1, z_2, \ldots]]^{\mathrm{alg}}$ is an effective tribe for this representation.

Proposition 1. *The K-algebra $K[[z_1, z_2, \ldots]]^{\mathrm{alg}}$ forms an effective tribe.*

Proof. Let $f, g \in K[[z_1, z_2, \ldots]]^{\mathrm{alg}}$, so that $P(f) = Q(g) = 0$ for certain monic polynomials P, $Q \in K(z_1, \ldots, z_n)[u]$ of degrees d and e in u. For $i = 0, \ldots, d\,e$, these relations allow us to rewrite both $(f + g)^i$ and $(f\,g)^i$ as $K(z_1, \ldots, z_n)$-linear combinations of $f^k\,g^l$ with $0 \leqslant k < d$ and $0 \leqslant l < e$. Since these $f^k\,g^l$ span a vector space of dimension at most $d\,e$, this means that there exist monic polynomials $R, S \in K(z_1, \ldots, z_n)[u]$ of degree $\leqslant d\,e$ with $R(f + g) = S(f\,g) = 0$, and we may compute R and S using linear algebra. This shows that $K[[z_1, z_2, \ldots]]^{\mathrm{alg}}$ forms an effective power series algebra that is clearly inhabited.

With the above notations, let $\tilde{Q} = Q_e + Q_{e-1}\,u + \cdots + Q_1\,u^{e-1} + Q_0\,u^e$ and assume that $g \neq 0$. Then we notice that $Q(g) = 0 \Leftrightarrow \tilde{Q}(1/g) = 0$, so we can compute a polynomial $T \in K(z_1, \ldots, z_n)[u]$ with $T(f\,/\,g) = 0$ in a similar way as above. This shows that $K[[z_1, z_2, \ldots]]^{\mathrm{alg}}$ is effectively stable under restricted division by g.

Assume now that $g_1, \ldots, g_n \in K[[z_1, z_2, \ldots]]^{\mathrm{alg}}$ with $g_1(0) = \cdots = g_n(0) = 0$ and let $Q_i \in K(z_1, \ldots, z_m)[u]$ be a monic annihilator of g_i of degree e_i for $i = 1, \ldots, n$. Assume first that the annihilator P of f belongs to $K[z_1, \ldots, z_n, u]$. Given any $i \in \mathbb{N}$, we may then rewrite $(f \circ g)^i$ as a linear combination of $(f^j \circ g)\,g_1^{k_1} \cdots g_n^{k_n}$ with $j < d$, $k_1 < e_1, \ldots, k_n < e_n$. In a similar way as above, this allows us to compute a non trivial annihilator of degree $\leqslant d\,e_1 \cdots e_n$ of $f \circ g$. In general, the annihilator of f belongs to $D^{-1}\,K[z_1, \ldots, z_n, u]$ for some denominator $D \in K[z_1, \ldots, z_n]$. In that case, the annihilator of $D\,f$ belongs to $K[z_1, \ldots, z_n, u]$, whence $(D\,f) \circ g$ is algebraic, and so is $f \circ g = (D \circ g)^{-1}\,(D\,f) \circ g$. In other words, $K[[z_1, z_2, \ldots]]^{\mathrm{alg}}$ is effectively stable under composition. A similar argument shows the effective stability under restricted monomial transformations.

Let us finally assume that $f(0)=0$, but $(\partial f/\partial z_1)(0)\neq 0$, and let $\psi_1\in K[[z_1,\ldots,z_{n-1}]]$ and $\psi_2=z_1,\ldots,\psi_n=z_{n-1}$ be such that $f\circ\psi=0$. Let $P(z_1,\ldots,z_n,u)$ still be the annihilator of f. Then $P(f)\circ\psi=P(\psi_1,z_1,\ldots,z_{n-1},f\circ\psi)=P(\psi_1,z_1,\ldots,z_{n-1},0)=0$ yields a non trivial annihilator for ψ_1. This shows that $K[[z_1,z_2,\ldots]]^{\mathrm{alg}}$ is effectively stable under the implicit function theorem.

In order to conclude, we still need to prove the existence of an effective zero test for f (given by its annihilator P and an algorithm to compute its coefficients). Now the polynomial equation $P(f)=0$ admits at most d solutions. Using the Newton polygon method for a suitable valuation, it is possible to derive a bound for the maximal valuation of f in the case when $f\neq 0$. It then suffices to compute the coefficients of f up to this valuation bound. For more details, we refer to [15], where we proved a stronger result in a more general setting. □

A power series $f\in K[[z_1,\ldots,z_n]]$ is said to be *d-algebraic* if it satisfies an algebraic differential equation $P_i(f,\ldots,\delta_i^{r_i}f)=0$ for each $i\in\{1,\ldots,n\}$, where P_i is a non-zero polynomial in r_i+1 variables with coefficients in K. This is the case if and only if the differential field $H\langle f\rangle$ generated by f over $H=K(z_1,z_2,\ldots)$ admits a finite transcendence degree. We denote by $K[[z_1,z_2,\ldots]]^{\mathrm{dalg}}$ the set of d-algebraic power series. Using the finite transcendence degree criterion, and similar techniques as in the proof of Proposition 1, it can be shown that $K[[z_1,z_2,\ldots]]^{\mathrm{dalg}}$ forms a tribe.

If K is an effective field, then effective d-algebraic power series may again be represented through an effective power series and differential annihilators P_i of the above form. In [15], one may find more information on how to compute with d-algebraic power series, and a full proof of the fact that $K[[z_1,z_2,\ldots]]^{\mathrm{dalg}}$ is actually an effective tribe (the proof being based on earlier techniques from [7, 8]). Notice that the most intricate part of this kind of computations is zero testing.

3 Grid-based series

Monomial monoids

In what follows, we will only consider commutative monoids. A *monomial monoid* is a multiplicative monoid $\mathfrak{M}$ with a partial ordering $\preccurlyeq$ that is compatible with the multiplication (i.e. $\mathfrak{m}_1\preccurlyeq\mathfrak{n}_1\wedge\mathfrak{m}_2\preccurlyeq\mathfrak{n}_2\Rightarrow\mathfrak{m}_1\mathfrak{m}_2\preccurlyeq\mathfrak{n}_1\mathfrak{n}_2$ and $\mathfrak{m}_1\mathfrak{n}\preccurlyeq\mathfrak{m}_2\mathfrak{n}\Rightarrow\mathfrak{m}_1\preccurlyeq\mathfrak{m}_2$). The notation $\preccurlyeq$ generalizes Hardy's notation from asymptotic analysis, so we call $\preccurlyeq$ an *asymptotic ordering*. We denote by $\mathfrak{M}^{\prec}=\{\mathfrak{m}\in\mathfrak{M}:\mathfrak{m}\prec 1\}$ the set of *infinitesimal* elements in $\mathfrak{M}$ and by $\mathfrak{M}^{\preccurlyeq}=\{\mathfrak{m}\in\mathfrak{M}:\mathfrak{m}\preccurlyeq 1\}$ the set of *bounded* elements in $\mathfrak{M}$. We say that $\mathfrak{M}$ has $\mathbb{Q}$-powers if we also have a powering operation $(k,\mathfrak{m})\in\mathbb{Q}\times\mathfrak{M}\mapsto\mathfrak{m}^k\in\mathfrak{M}$ such that $(\mathfrak{m}\,\mathfrak{n})^k=\mathfrak{m}^k\mathfrak{n}^k$ and $(\mathfrak{m}^k)^l=\mathfrak{m}^{kl}$ for all $k,l\in\mathbb{Q}$ and $\mathfrak{m},\mathfrak{n}\in\mathfrak{M}$.

A monomial monoid $\mathfrak{M}$ is said to be *effective* if its elements can be represented by effective data structures and if we have algorithms for the multiplication and the asymptotic ordering $\preccurlyeq$. Since $\mathfrak{m}=\mathfrak{n}\Leftrightarrow\mathfrak{m}\preccurlyeq\mathfrak{n}\wedge\mathfrak{n}\preccurlyeq\mathfrak{m}$ this implies the existence of an effective equality test. A monomial group $\mathfrak{M}$ is said to be *effective* if it is an effective monomial monoid with an algorithm for the group inverse. We say that $\mathfrak{M}$ is an *effective monomial group with* $\mathbb{Q}$*-powers* if we also have a computable powering operation.

Grid-based sets

A subset $\mathfrak{G}\subseteq\mathfrak{M}$ is said to be *grid-based* if there exist finite sets $\{\mathfrak{m}_1,\ldots,\mathfrak{m}_m\}\subseteq\mathfrak{M}^{\prec}$ and $\{\mathfrak{n}_1,\ldots,\mathfrak{n}_n\}\subseteq\mathfrak{M}$ such that

$$\mathfrak{G}\;\subseteq\;\{\mathfrak{m}_1^{i_1}\cdots\mathfrak{m}_m^{i_m}\mathfrak{n}_j: i_1,\ldots,i_m\in\mathbb{N},1\leqslant j\leqslant n\}. \tag{1}$$

If $\mathfrak{M}$ is actually a monomial group that is generated (as a group) by its infinitesimal elements, then we may always take $n=1$.

If $\mathfrak{M}$ is an effective monomial monoid, then a grid-based subset $\mathfrak{G} \subseteq \mathfrak{M}$ is said to be *effective* if the predicate $\mathfrak{m} \in \mathfrak{M} \Rightarrow \mathfrak{m} \in \mathfrak{G}$ is computable and if finite sets $\{\mathfrak{m}_1, \ldots, \mathfrak{m}_m\} \subseteq \mathfrak{M}^{\prec}$ and $\{\mathfrak{n}_1, \ldots, \mathfrak{n}_n\} \subseteq \mathfrak{M}$ with (1) are explicitly given.

Grid-based series

Let K be a field of characteristic zero. Given a formal series $f = \sum_{\mathfrak{m} \in \mathfrak{M}} f_{\mathfrak{m}} \mathfrak{m}$ with $f_{\mathfrak{m}} \in K$, the set $\operatorname{supp} f = \{\mathfrak{m} \in \mathfrak{M} : f_{\mathfrak{m}} \neq 0\}$ will be called the *support* of f. We say that the formal series f is *grid-based* if its support is grid-based and we denote by $K[[\mathfrak{M}]]$ the set of such series. A grid-based series $f \in K[[\mathfrak{M}]]$ is said to be *infinitesimal* or *bounded* if $\operatorname{supp} f \subseteq \mathfrak{M}^{\prec}$ resp. $\operatorname{supp} f \subseteq \mathfrak{M}^{\preccurlyeq}$, and we denote by $K[[\mathfrak{M}]]^{\prec}$ resp. $K[[\mathfrak{M}]]^{\preccurlyeq}$ the sets of such series.

In [13, Chapter 2] elementary properties of grid-based series are studied at length. We prove there that $K[[\mathfrak{M}]]$ forms a ring in which all series f with $1 \in \operatorname{supp} f \subseteq \mathfrak{M}^{\preccurlyeq}$ are invertible. In particular, if $\mathfrak{M}$ is a totally ordered group, then $K[[\mathfrak{M}]]$ forms a field. Given a power series $f \in K[[z_1, \ldots, z_n]]$ and grid-based series $g_1, \ldots, g_n \in K[[\mathfrak{M}]]^{\prec}$, there is also a natural definition for the composition $f(g) = f \circ g = f(g_1, \ldots, g_n) = f \circ (g_1, \ldots, g_n)$.

Given a grid-based series $f \in K[[\mathfrak{M}]]$ the maximal elements of $\operatorname{supp} f$ for $\preccurlyeq$ are called *dominant monomials* for f. If f has a unique dominant monomial, then we say that f is *regular*, we write $\mathfrak{d}_f$ for the dominant monomial of f, and call $f_{\mathfrak{d}_f}$ the *dominant coefficient* of f. If $\mathfrak{M}$ is totally ordered, then any non-zero grid-based series in $K[[\mathfrak{M}]]$ is regular. Given $f, g \in K[[\mathfrak{M}]]^{\neq}$, this allows us to extend the relations $\preccurlyeq$ and $\prec$ by defining $f \preccurlyeq g \Leftrightarrow \mathfrak{d}_f \preccurlyeq \mathfrak{d}_g$ and $f \prec g \Leftrightarrow \mathfrak{d}_f \prec \mathfrak{d}_g$. By convention, we also define $0 \preccurlyeq g$ and $0 \prec g \Leftrightarrow g \neq 0$ for all $g \in K[[\mathfrak{M}]]$.

Assume that K and $\mathfrak{M}$ are effective. Then a grid-based series $f \in K[[\mathfrak{M}]]$ is said to be *effective* if its support is effective and if the map $\mathfrak{m} \in \mathfrak{M} \mapsto f_{\mathfrak{m}}$ is computable. It can be shown that the set $K[[\mathfrak{M}]]^{\mathrm{com}}$ of computable grid-based series forms an effective K-algebra.

Examples

Given an “infinitesimal” indeterminate z, the set $z^{\mathbb{N}} = \{z^i : i \in \mathbb{N}\}$ is a monomial monoid for the asymptotic ordering $z^i \preccurlyeq z^j \Leftrightarrow i \geqslant j$, and $K[[z^{\mathbb{N}}]]$ coincides with $K[[z]]$. Similarly, $K[[z^{\mathbb{Z}}]]$ coincides with the field of Laurent series $K((z))$. Notice that $f = \sum_{i \in \mathbb{N}} z^{-i}$ is *not* an element of $K[[z^{\mathbb{Z}}]]$, since its support $z^{-\mathbb{N}}$ admits no largest element for $\preccurlyeq$, whence it cannot be grid-based. Beyond Laurent series, it is easily verified that $K[[z^{\mathbb{Q}}]]$ coincides with the field of Puiseux series in z over K. If K is algebraically closed, then so is $K[[z^{\mathbb{Q}}]]$.

Given monomial monoids $\mathfrak{M}_1, \ldots, \mathfrak{M}_n$, one may form the product monomial monoid $\mathfrak{M}_1 \times \cdots \times \mathfrak{M}_n$ with $\mathfrak{m}_1 \cdots \mathfrak{m}_n \preccurlyeq \mathfrak{n}_1 \cdots \mathfrak{n}_n \Leftrightarrow \mathfrak{m}_1 \preccurlyeq \mathfrak{n}_1 \wedge \cdots \wedge \mathfrak{m}_n \preccurlyeq \mathfrak{n}_n$ for all $\mathfrak{m}_1, \mathfrak{n}_1 \in \mathfrak{M}_1, \ldots, \mathfrak{m}_n, \mathfrak{n}_n \in \mathfrak{M}_n$. Then $K[[z_1^{\mathbb{N}} \times \cdots \times z_n^{\mathbb{N}}]]$ coincides with the set of power series $K[[z_1, \ldots, z_n]]$, whereas $K[[z_1^{\mathbb{Z}} \times \cdots \times z_n^{\mathbb{Z}}]]$ coincides with the set of Laurent series that we denote by $K((z_1, \ldots, z_n))$. If $n \geqslant 2$, then we notice that $K((z_1, \ldots, z_n))$ is a strict subring of the quotient field of $K[[z_1, \ldots, z_n]]$.

Given monomial monoids $\mathfrak{M}_1, \ldots, \mathfrak{M}_n$, one may also form the set $\mathfrak{M}_1 \dot{\times} \cdots \dot{\times} \mathfrak{M}_n$ whose elements $\mathfrak{m}_1 \cdots \mathfrak{m}_n$ are ordered anti-lexicographically: $\mathfrak{m}_1 \cdots \mathfrak{m}_n \prec \mathfrak{n}_1 \cdots \mathfrak{n}_n$ if there exists an i with $\mathfrak{m}_i \prec \mathfrak{n}_i$ and $\mathfrak{m}_j = \mathfrak{n}_j$ for all $j > i$. The set $K[[z_1^{\mathbb{N}} \dot{\times} \cdots \dot{\times} z_n^{\mathbb{N}}]]$ should naturally be interpreted as $K[[z_1]] \cdots [[z_n]]$ (which is isomorphic to $K[[z_1, \ldots, z_n]]$). The set $K[[z_1^{\mathbb{Z}} \dot{\times} \cdots \dot{\times} z_n^{\mathbb{Z}}]]$ is a field that contains $K((z_1, \ldots, z_n))$, and this inclusion is strict if $n > 1$ (notice also that $K[[z_1^{\mathbb{Z}} \dot{\times} \cdots \dot{\times} z_n^{\mathbb{Z}}]] \subsetneq K((z_1)) \cdots ((z_n))$). If K is algebraically closed, then $K[[z_1^{\mathbb{Q}} \dot{\times} \cdots \dot{\times} z_n^{\mathbb{Q}}]]$ is again an algebraically closed field (and again, we have $K[[z_1^{\mathbb{Q}} \dot{\times} \cdots \dot{\times} z_n^{\mathbb{Q}}]] \subsetneq K[[z_1^{\mathbb{Q}}]] \cdots [[z_n^{\mathbb{Q}}]]$).

Asymptotic interpretation

Let $\mathfrak{M}$ be a totally ordered group. Given $f \in K[[z_1, \ldots, z_n]]$ and $g_1, \ldots, g_n \in K\llbracket\mathfrak{M}\rrbracket$, we have already observed that $f \circ g \in K\llbracket\mathfrak{M}\rrbracket$ whenever $g_1 \prec 1, \ldots, g_n \prec 1$. This means that we may regard $K[[z_1, \ldots, z_n]]$ as a space of "local functions" $(K\llbracket\mathfrak{M}\rrbracket^{\prec})^n \rightarrow K\llbracket\mathfrak{M}\rrbracket$. Similarly, $f \in K((z_1, \ldots, z_n))$ can be regarded as a function $(K\llbracket\mathfrak{M}\rrbracket^{\prec} \setminus \{0\})^n \rightarrow K\llbracket\mathfrak{M}\rrbracket$ and $f \in K\llbracket z_1^{\mathbb{Z}} \dot{\times} \cdots \dot{\times} z_n^{\mathbb{Z}}\rrbracket$ as a function $R \rightarrow K\llbracket\mathfrak{M}\rrbracket$ where $R = \{(g_1, \ldots, g_n) \in (K\llbracket\mathfrak{M}\rrbracket^{\prec} \setminus \{0\})^n : \forall i < j, \forall k, g_j \prec g_i^k\}$. More generally, for any monomial group $\mathfrak{N}$ with underlying group $z_1^{\mathbb{Z}} \cdots z_n^{\mathbb{Z}}$, the algebra $K\llbracket\mathfrak{N}\rrbracket$ can be regarded as a local function space on a subset of $(K\llbracket\mathfrak{M}\rrbracket^{\prec} \setminus \{0\})^n$.

Cartesian representations

From now on, we will assume that $\mathfrak{M}$ is a monomial group that is generated as a group by its infinitesimal elements. Given a series $f \in K\llbracket\mathfrak{M}\rrbracket$, a *Cartesian representation* for f is a Laurent series $\check{f} \in K((z_1, \ldots, z_k))$ together with monomials $\mathfrak{m}_1, \ldots, \mathfrak{m}_k \in \mathfrak{M}^{\prec}$ such that $f = \check{f}(\mathfrak{m}_1, \ldots, \mathfrak{m}_k)$. Given several series $f_1, \ldots, f_l \in K\llbracket\mathfrak{M}\rrbracket$, and Cartesian representations for each of the f_i, we say that these Cartesian representations are *compatible* if they are of the form $f_i = \check{f}_i(\mathfrak{m}_1, \ldots, \mathfrak{m}_k)$ for $\check{f}_i \in K((z_1, \ldots, z_k))$ and $\mathfrak{m}_1, \ldots, \mathfrak{m}_k \in \mathfrak{M}^{\prec}$. In [13, Proposition 3.12] we show that such compatible Cartesian representations always exist.

In [13, Chapter 3], we gave constructive proofs of several basic facts about Cartesian representations and L-based series to be introduced below. These constructive proofs can easily be transformed into algorithms, so we will only state the effective counterparts of the main results. First of all, in order to keep the number of variables k in Cartesian representations as low as possible, we may use the following effective variant of [13, Lemma 3.13]:

Lemma 2. *Let $\mathfrak{z}_1, \ldots, \mathfrak{z}_k, \mathfrak{m}_1, \ldots, \mathfrak{m}_l$ be infinitesimal elements of an effective totally ordered monomial group $\mathfrak{M}$ with $\mathbb{Q}$-powers, such that we have explicit expressions for $\mathfrak{m}_1, \ldots, \mathfrak{m}_l \in \mathfrak{z}_1^{\mathbb{Z}} \cdots \mathfrak{z}_k^{\mathbb{Z}}$ as power products. Then we may effectively compute infinitesimal $\mathfrak{z}_1', \ldots, \mathfrak{z}_k' \in \mathfrak{z}_1^{\mathbb{Q}} \cdots \mathfrak{z}_k^{\mathbb{Q}}$ with $\mathfrak{z}_1, \ldots, \mathfrak{z}_k, \mathfrak{m}_1, \ldots, \mathfrak{m}_l \in (\mathfrak{z}_1')^{\mathbb{N}} \cdots (\mathfrak{z}_k')^{\mathbb{N}}$.* □

L-based power series

Let L be a local community. We will say that $f \in K\llbracket\mathfrak{M}\rrbracket$ is *L-based* if f admits a Cartesian representation of the form $f = \check{f}(\mathfrak{m}_1, \ldots, \mathfrak{m}_k)$ with $\check{f} = \varphi\, z_1^{i_1} \cdots z_k^{i_k}$, $\varphi \in L_k$ and $i_1, \ldots, i_k \in \mathbb{Z}$. The set $K\llbracket\mathfrak{M}\rrbracket_L$ of all such series forms a K-algebra [13, Proposition 3.14]. If K, L and $\mathfrak{M}$ are effective, then any grid-based series in $K\llbracket\mathfrak{M}\rrbracket_L$ is computable. Moreover, we may effectively represent series in $K\llbracket\mathfrak{M}\rrbracket_L$ by Cartesian representations, and $K\llbracket\mathfrak{M}\rrbracket_L$ is an effective K-algebra for this representation.

A Cartesian representation $f = \check{f}(\mathfrak{m}_1, \ldots, \mathfrak{m}_k)$ of $f \in K\llbracket\mathfrak{M}\rrbracket$ is said to be *faithful* if for each dominant monomial $\check{\mathfrak{v}} = z_1^{i_1} \cdots z_k^{i_k}$ of f, there exists a dominant monomial $\mathfrak{w}$ of f with $\check{\mathfrak{v}}(\mathfrak{m}_1, \ldots, \mathfrak{m}_k) \preccurlyeq \mathfrak{w}$. We have the following effective counterpart of [13, Proposition 3.19]:

Proposition 3. *Assume that K, L and $\mathfrak{M}$ are effective. Then there exists an algorithm that takes a series in $K\llbracket\mathfrak{M}\rrbracket_L$ as input and computes a faithful Cartesian representation $f = \check{f}(\mathfrak{m}_1, \ldots, \mathfrak{m}_k)$ with $\check{f} = \varphi\, z_1^{i_1} \cdots z_k^{i_k}$, $\varphi \in L_k$ and $i_1, \ldots, i_k \in \mathbb{Z}$.* □

Faithful Cartesian representations are a useful technical tool for various computations. They occur for instance in the proof of the following effective counterpart of [13, Proposition 3.20]:

Proposition 4. *Assume that K, L and $\mathfrak{M}$ are effective. There exists an algorithm that takes an infinitesimal (or bounded, or regular) series $f \in K\llbracket\mathfrak{M}\rrbracket$ as input and that computes a Cartesian representation $f = \check{f}(\mathfrak{m}_1, \ldots, \mathfrak{m}_k)$ such that $\check{f}$ is again infinitesimal (or bounded, or regular, respectively).* □

Solving power series equations

Assume now that K is an effective field with an effective zero test and an algorithm for determining the roots in K of polynomials in $K[F]$, where F is a new indeterminate. Let L be an effective local community over K and $\mathfrak{M}$ an effective totally ordered monomial group. We notice that a grid-based series in $K[[\mathfrak{M} \times F^{\mathbb{N}}]]$ can also be regarded as an ordinary power series in $K[[\mathfrak{M}]][[F]]$. We are interested in finding all infinitesimal solutions of a power series equation

$$P_0 + P_1 f + P_2 f^2 + \cdots = 0,$$

where $P = P_0 + P_1 F + P_2 F^2 + \cdots \in K[[\mathfrak{M} \times F^{\mathbb{N}}]]_L$. The Newton polygon method from [13, Chapter 3] can be generalized in a straightforward way to power series equations instead of polynomial equations and the effective counterpart of [13, Theorem 3.21] becomes:

Theorem 5. *There exists an algorithm that takes $P \in K[[\mathfrak{M} \times F^{\mathbb{N}}]]_L \subseteq K[[\mathfrak{M}]][[F]]$ with $P \neq 0$ as input and that computes all solutions of the equation $P(f) = 0$ with $f \in K[[\mathfrak{M}]]^{\prec}$.* □

Given $P \in K[[\mathfrak{M} \times F^{\mathbb{N}}]]_L$ with $P \neq 0$, we may also consider P as an element of $K[[F^{\mathbb{N}} \times \mathfrak{M}]] \cong K[[F]][[\mathfrak{M}]]$. Let $N_P \in K[[F]]$ be the dominant coefficient of P for this latter representation. The valuation of N_P in F is called the *Weierstrass degree* of P. If K is algebraically closed, then it can be shown that the number of solutions to the equation in Theorem 5 coincides with the Weierstrass degree, when counting with multiplicities.

Scalar extensions

Let L be a tribe over K and let $\lambda_1, \ldots, \lambda_l$ be indeterminates. Then there exists a smallest tribe over $K(\lambda)$ that extends L. We will denote this tribe by $K(\lambda) \otimes L$. Setting

$$\mathfrak{L} = \lambda_1^{\mathbb{Z}} \dot{\times} \cdots \dot{\times} \lambda_l^{\mathbb{Z}} \dot{\times} (z_1^{\mathbb{N}} \times z_2^{\mathbb{N}} \times \cdots),$$

we notice that $K(\lambda) \subseteq K[[\lambda_1^{\mathbb{Z}} \dot{\times} \cdots \dot{\times} \lambda_l^{\mathbb{Z}}]]_L \subseteq K[[\mathfrak{L}]]_L$ and $L \subseteq K[[\mathfrak{L}]]_L$. This shows that any element in $K(\lambda) \otimes L$ can be represented by an element of $K[[\mathfrak{L}]]_L$. In particular, if L is effective, then so is $K(\lambda) \otimes L$.

4 Effective Weierstrass preparation

Effective algebraic closures

Let K be an effective field with an effective zero test. We may consider its algebraic closure K^{alg} as an effective field with an effective zero test, when computing non-deterministically (we refer to [5] for more details about this technique, which is also called dynamic evaluation).

Let L be an effective tribe over K with an effective zero test. It is convenient to represent elements of $K^{\text{alg}} \otimes L$ by evaluations of polynomials $P \in L[X]$ at $\alpha \in K^{\text{alg}}$. The algebraic number α is effectively represented using an annihilator $A \in K[X]$ and we may always take P such that $\deg P < \deg A$. We say that L is *algebraically stable* if $K^{\text{alg}} \otimes L$ forms again an effective tribe for this representation. This is the case for the tribes of algebraic and d-algebraic power series, but not for arbitrary tribes: if $K = \mathbb{R}$ and L is the smallest tribe that contains the exponential power series $\exp z_1$, then it follows from Wilkie's theorem [18] that L does not contain $\sin z_1$; on the other hand, any tribe that contains $\mathbb{C} \otimes L$ must contain $\sin z_1$.

Assume that L is algebraically stable. Consider a series $f \in (K^{\text{alg}} \otimes L) \cap K[[z_1, z_2, \ldots]]$, represented as $f = P(\alpha) = P_0 + \cdots + P_{k-1} \alpha^{k-1}$, where $\alpha \in K^{\text{alg}}$ is given by an annihilator of degree k, and $P_0, \ldots, P_{k-1} \in L$. Then we notice that we can compute a representation for f as a element of L. Indeed, whenever $P_j \neq 0$ for some $j > 0$, then this means that there exists a monomial $z^i \in z_1^{\mathbb{N}} z_2^{\mathbb{N}} \cdots$ such that the coefficient $[z^i] P \in K[\alpha]$ of z^i in P is a polynomial of non-zero degree in α. On the other hand, $[z^i] P \in K$, which means that we can compute an annihilator for α of degree $<k$. Repeating this reduction a finite number of times, we thus reach the situation in which $P_1 = \cdots = P_{k-1} = 0$, so that $f = P_0 \in L$.

Effective Weierstrass preparation

Let L still be an effective algebraically stable tribe over K with an effective zero test. Given $f \in L_n$, we recall that f is said to have *Weierstrass degree* d in z_1 if $f(0) = (\partial f / \partial z_1)(0) = \cdots = (\partial^{d-1} f / \partial z_1^{d-1})(0) = 0$, but $(\partial^d f / \partial z_1^d)(0) \neq 0$. In that case, the Weierstrass preparation theorem states that there exists a unit $u \in K[[z_1, \ldots, z_n]]$ and a monic polynomial $P = z_1^d + P_{d-1} z_1^{d-1} + \cdots + P_0 \in K[[z_2, \ldots, z_n]][z_1]$ of degree d such that $f = u\, P$. The polynomial P is called the *Weierstrass polynomial* associated to f (with respect to z_1). We claim that $P \in L_n$ and that there exists an algorithm to compute P (and therefore the corresponding unit u, since L_n is effectively stable under restricted division):

Theorem 6. *There exists an algorithm that takes a power series $f \in L_n$ of Weierstrass degree d in z_1 as input and computes its Weierstrass polynomial P as an element of L_n.*

Proof. Consider the effective totally ordered monomial group $\mathfrak{M} = z_2^{\mathbb{Q}} \dot{\times} \cdots \dot{\times} z_n^{\mathbb{Q}}$ with $\mathbb{Q}$-powers. We have a natural inclusion $L_n \subseteq K^{\text{alg}} [\![\mathfrak{M} \times z_1^{\mathbb{N}}]\!]_{K^{\text{alg}} \otimes L}$. Now consider $f \in K^{\text{alg}} [\![\mathfrak{M} \times z_1^{\mathbb{N}}]\!]_{K^{\text{alg}} \otimes L} \subseteq K^{\text{alg}} [\![\mathfrak{M}]\!] [[z_1]]$. By theorem 5, we may compute all infinitesimal solutions $\varphi_1, \ldots, \varphi_d \in K^{\text{alg}} [\![\mathfrak{M}]\!]_{K^{\text{alg}} \otimes L}$ to the equation $f(\varphi) = 0$ in z_1 (we recall that there are d such solutions, when counting with multiplicities, since K^{alg} is algebraically closed). Now consider

$$P = (z_1 - \varphi_1) \cdots (z_1 - \varphi_d) \in K^{\text{alg}} [\![\mathfrak{M} \times z_1^{\mathbb{N}}]\!]_{K^{\text{alg}} \otimes L}$$

and let $P^* \in K[[z_1, \ldots, z_n]]$ be the Weierstrass polynomial associated to f. Since P^* also admits the infinitesimal roots $\varphi_1, \ldots, \varphi_d$ when considered as an element of $K^{\text{alg}} [\![\mathfrak{M}]\!] [[z_1]]$, we have $P = P^*$ when considering P^* as an element of $K^{\text{alg}} [\![\mathfrak{M} \times z_1^{\mathbb{N}}]\!]$. It follows that

$$P \in K^{\text{alg}} [\![\mathfrak{M} \times z_1^{\mathbb{N}}]\!]_{K^{\text{alg}} \otimes L} \cap K[[z_1, \ldots, z_n]].$$

Now consider a Cartesian representation $P = \check{P}(\mathfrak{m}_1, \ldots, \mathfrak{m}_k)$ for P with $\check{P} \in L$. By Proposition 4, we may take $\check{P}$ to be infinitesimal. Since $\mathfrak{m}_1, \ldots, \mathfrak{m}_k$ are infinitesimal and $\mathfrak{m}_1, \ldots, \mathfrak{m}_k \in z_1^{\mathbb{Q}} \cdots z_n^{\mathbb{Q}}$, Lemma 2 also shows that we may assume without loss of generality that $k \leqslant n$. Completing the $\mathfrak{m}_1, \ldots, \mathfrak{m}_k$ with additional elements if necessary, this means that we may compute an invertible matrix $M \in \mathbb{Q}^{n \times n}$ such that $\mathfrak{m}_i = z_i \circ z^M$ for all i. In other words, $P = \check{P} \circ z^M$ with $\check{P} \in L_n$. Since $P \in K[[z_1, \ldots, z_n]]$ and L is effectively closed under restricted monomial transformations, we conclude that $P \in L_n$. □

Effective Weierstrass division

Recall that L is an effective algebraically stable tribe over K with an effective zero test. Assume that $f \in L_n$ has Weierstrass degree d in z_1 and let $g \in L_n$. The Weierstrass division theorem states that there exist unique $Q \in K[[z_1, \ldots, z_n]]$ and $R \in K[[z_2, \ldots, z_n]][z_1]$ with

$$g = Q f + R$$

and $\deg_{z_1} R < d$. We claim that the *quotient* Q and *remainder* R of this division once again belong to L_n and that there exists an algorithm to compute them:

Theorem 7. *There exists an algorithm that takes a power series $f \in L_n$ of Weierstrass degree d in z_1 and $g \in L_n$ as input and computes the quotient and remainder of the Weierstrass division of g by f as elements of L_n.*

Proof. Let $\mathfrak{M} = z_2^{\mathbb{Q}} \dot{\times} \cdots \dot{\times} z_n^{\mathbb{Q}}$ be as in the proof of Theorem 6. Let $\varphi_1, \ldots, \varphi_s$ be the distinct solutions of $f(\varphi) = 0$ when considered as an equation in z_1, and let μ_i be the multiplicity of each φ_i, so that $\mu_1 + \cdots + \mu_s = d$. For each i, we compute the multiplicity μ_i and the polynomials

$$\begin{aligned} A_i &= \sum_{j=0}^{\mu_i - 1} \frac{1}{j!} \frac{\partial^j g}{\partial z_1^j} \circ (\varphi_i, z_2, \ldots, z_n)\, z_1^j \in K^{\mathrm{alg}} [\![\mathfrak{M}]\!]_{K^{\mathrm{alg}} \otimes L} [z_1] \\ B_i &= (z_1 - \varphi_i)^{\mu_i} \in K^{\mathrm{alg}} [\![\mathfrak{M}]\!]_{K^{\mathrm{alg}} \otimes L} [z_1]. \end{aligned}$$

Using Chinese remaindering, we next compute the unique $R \in K^{\mathrm{alg}} [\![\mathfrak{M}]\!]_{K^{\mathrm{alg}} \otimes L} [z_1]$ such that $R \equiv A_i \bmod B_i$ for each i and $\deg_{z_1} R < d$. It is easily verified that R coincides with the remainder of the Weierstrass division of g by f. In particular, $R \in K[[z_1, \ldots, z_n]]$ and we may obtain R as an element of L_n in the same way as in the proof of Theorem 6. We obtain the quotient Q of the Weierstrass division by performing the restricted division of $g - R$ by f. □

The evaluation approach

Often, it is possible to regard or represent elements of the tribe L as functions. For instance, we may regard $f = z_1 + \exp z_2$ as a function $f: (t\, K[[t]])^2 \rightarrow K[[t]]$ that sends $(z_1(t), z_2(t))$ to $z_1(t) + \exp z_2(t)$. This point of view is very useful for heuristic zero testing: in order to test whether $f \in K[[z_1, \ldots, z_n]]_L$ vanishes, just pick random infinitesimal univariate series $z_1(t), \ldots, z_n(t) \in t\, K[[t]]$ and check whether the first N terms of $f(z_1(t), \ldots, z_n(t))$ vanish for some suitable large number N.

In this evaluation approach, we notice that Weierstrass preparation becomes far less expensive: instead of explicitly computing $\varphi_1, \ldots, \varphi_d \in K^{\mathrm{alg}} [\![\mathfrak{M}]\!]_{K^{\mathrm{alg}} \otimes L}$ as above, it suffices to show how to *evaluate* $\varphi_1, \ldots, \varphi_d$ (in terms of the evaluations of $z_2, \ldots, z_n$). For instance, if we evaluate $z_1, \ldots, z_n$ at infinitesimal ordinary power series in $t\, K[[t]]$, then the evaluations of $\varphi_1, \ldots, \varphi_d$ will be Puiseux series in $K [\![t^{\mathbb{Q}}]\!]$ that can be computed fast using the Newton polygon method.

Algebraic power series

In the special case of algebraic power series, we recall from the introduction that an alternative approach to Weierstrass division was proposed in [2]. In this approach, algebraic functions are represented in terms of unique power series solutions to certain systems of polynomial equations. Given an algebraic series $f \in K[[z_1, \ldots, z_n]]$ of Weierstrass degree d in z_1, the idea is then to represent the Weierstrass polynomial P associated to f as $P = z_1^d + u_{d-1}\, z_1^{d-1} + \cdots + u_0$ for certain undetermined coefficients. Next, it suffices to form a new system of equations in $u_0, \ldots, u_{d-1}$ for which the unique solution yields the actual Weierstrass polynomial. For instance, if f is a polynomial, then the relation $f \operatorname{rem}_{z_1} P = 0$ essentially provides us with such a system, where $f \operatorname{rem}_{z_1} P$ stands for the remainder of the Euclidean division of f by P as polynomials in z_1.

The efficiency of this approach from [2] highly depends on the way how the systems of equations that are satisfied by algebraic power series are represented. For instance, completely writing out the remainder $f \operatorname{rem}_{z_1} P$ as a polynomial in $K[u_0, \ldots, u_{d-1}, z_1, z_2, \ldots, z_n]$ typically leads to very large expressions. On the other hand, we expect the approach to be efficient in combination with the evaluation approach mentioned above. If we replace the variables $z_2, \ldots, z_n$ by infinitesimal power series in $t\, K[[t]]$, then one may solve the evaluated system of equations in $u_0, \ldots, u_{d-1}$ using the relaxed technique from [14].

D-algebraic power series

One attractive way to represent d-algebraic power series in $z_1, \ldots, z_n$ is as elements of a suitable type of finitely generated algebras $A \subseteq K[[z_1, \ldots, z_n]]$ over K that are stable under the derivations $\partial_1, \ldots, \partial_n$ with respect to $z_1, \ldots, z_n$. For instance, we might have $A = K\left[z_1, z_2, \mathrm{e}^{-z_1^2 z_2^2}, \operatorname{erf}(z_1 z_2)\right]$.

In order to compute with implicit functions, there are essentially two approaches. The traditional one procedes by the elimination of one or more coordinates, which may lead to expensive rewritings. An alternative strategy is to represent restrictions of functions in A to subvarieties by the same functions in A, and rather focus on the computation of the derivations that leave the subvariety invariant. Consider for instance the sphere $(z_1 + 1)^2 + z_2^2 + z_3^2 = 1$. We keep representing functions on the sphere using all three coordinates z_1, z_2, and z_3. On the other hand, for differential calculus, we only work with derivations that annihilate the equation of the sphere. In particular, the local coordinates z_2 and z_3 give rise to derivations $\tilde{\partial}_2 = \partial_2 - z_2 (1 + z_1)^{-1} \partial_1$ and $\tilde{\partial}_3 = \partial_3 - z_3 (1 + z_1)^{-1} \partial_1$ that do not commute. We refer to [15, Section 5] for more details on how to compute with respect to such curved coordinates and how to derive an implicit function theorem in this way.

The second, more geometric approach can be generalized to Weierstrass division, by regarding the implicit function theorem as division with respect to a series of Weierstrass degree one. For a d-algebraic series $f \in A \subseteq K[[z_1, \ldots, z_n]]$ of higher Weierstrass degree $d > 1$, we may again consider the restriction of the ambient space to the zero-set of f (recall that we may regard f as a local function $f: (K[\![\mathfrak{M}]\!]^{\prec})^n \to K[\![\mathfrak{M}]\!]^{\preccurlyeq}$ for any totally ordered monomial group $\mathfrak{M}$). Remainders of Weierstrass divisions by f then correspond to functions on this zero-set. It is likely that an alternative effective Weierstrass preparation theorem can be obtained by pursuing this line of thought.

5 Effective power series elimination

Throughout this section, we assume that K is an effective field with an effective zero test and that L is an effective algebraically stable tribe over K with an effective zero test. We will write $\mathbb{S} = K[[z_1, \ldots, z_n]] = K[\![\mathfrak{M}]\!]$ with $\mathfrak{M} = z_1^{\mathbb{N}} \cdots z_n^{\mathbb{N}}$ and assume that $\mathfrak{M}$ is endowed with the asymptotic ordering $\preccurlyeq$ that corresponds on the standard lexicographical ordering on the exponent vectors:

$$z^i \prec z^j \iff (\exists k, i_1 = j_1 \wedge \cdots \wedge i_{k-1} = j_{k-1} \wedge i_k > j_k).$$

For each $k \in \{1, \ldots, n\}$, we also define $\mathfrak{M}_k = z_k^{\mathbb{N}} \cdots z_n^{\mathbb{N}}$ and $\mathbb{S}_k = K[[z_k, \ldots, z_n]] = K[\![\mathfrak{M}_k]\!]$. Given an arbitrary subset $\mathfrak{S} \subseteq \mathfrak{M}$, we finally define $K[\![\mathfrak{S}]\!] := \{f \in \mathbb{S} : \operatorname{supp} f \subseteq \mathfrak{S}\}$.

Weierstrass systems

Consider a subset $\mathcal{B} \subseteq \mathbb{S}^{\neq}$ together with a mapping $\mathfrak{l}: \mathcal{B} \to \mathfrak{M}; b \mapsto \mathfrak{l}_{\mathfrak{m}}$ with $b_{\mathfrak{l}_b} \neq 0$ for each $b \in \mathcal{B}$ (intuitively speaking, $\mathfrak{l}_b$ should be interpreted as a "leading monomial" of b; it will play a similar role as the "dominant monomial" $\mathfrak{d}_b$ of b from before). Setting $\mathfrak{l}_b = z_1^{d_1} \cdots z_k^{d_k}$ with $d_k \neq 0$ (or $d_k = 0$ and $k = 1$), we call z_k the *Weierstrass variable* for b and d_k the corresponding *Weierstrass degree*. We also denote $k_b = k$, $d_b = d_k$, and

$$\begin{aligned}
\mathfrak{F}_b &= \mathfrak{l}_b \mathfrak{M}_k \\
\mathfrak{R}_b &= \mathfrak{M} \setminus \mathfrak{F}_b \\
\mathfrak{m}_b &= z_1^{d_1} \cdots z_{k-1}^{d_{k-1}} \\
\mathfrak{M}_b &= \{\mathfrak{m} \in \mathfrak{M} : \mathfrak{m} \preccurlyeq \mathfrak{m}_b\}.
\end{aligned}$$

Given any $f \in \mathbb{S}$, we define

$$\pi_b(f) \;=\; \sum_{\mathfrak{n} \in \mathfrak{M}_k} f_{\mathfrak{m}_b \mathfrak{n}} \, \mathfrak{n}.$$

We say that $\mathcal{B}$ is a *Weierstrass system* if $\operatorname{supp} b \subseteq \mathfrak{M}_b$, if $\pi_b(b)$ has valuation d_b (w.r.t. $z_1, \ldots, z_n$) for each $b \in \mathcal{B}$ and if $\mathfrak{F}_b \cap \mathfrak{F}_{b'} = \varnothing$ for all $b \neq b'$ in $\mathcal{B}$. In that case, the elements of $\mathcal{B}$ are totally ordered by $b \leqslant b' \Leftrightarrow (\mathfrak{M}_b \supsetneq \mathfrak{M}_{b'} \vee (\mathfrak{M}_b = \mathfrak{M}_{b'} \wedge k_b \leqslant k_{b'}))$.

Example 8. The set $\mathcal{B} = \{b_1, b_2\}$ with

$$\begin{aligned} b_1 &= z_1^2 - z_2^2 \, (1 + z_3) \\ b_2 &= z_2^2 - z_3^2 + z_1 \, z_2 \, z_3 \end{aligned}$$

forms a Weierstrass system with $b_1 < b_2$ and

$$\begin{aligned} \mathfrak{l}_{b_1} &= z_1^2 & \mathfrak{l}_{b_2} &= z_2^2 \\ \mathfrak{F}_{b_1} &= z_1^{2+\mathbb{N}} \, z_2^{\mathbb{N}} \, z_3^{\mathbb{N}} & \mathfrak{F}_{b_2} &= z_2^{2+\mathbb{N}} \, z_3^{\mathbb{N}} \\ \mathfrak{R}_{b_1} &= z_2^{\mathbb{N}} \, z_3^{\mathbb{N}} \cup z_1 \, z_2^{\mathbb{N}} \, z_3^{\mathbb{N}} & \mathfrak{R}_{b_2} &= z_3^{\mathbb{N}} \cup z_2 \, z_3^{\mathbb{N}} \cup z_1^{1+\mathbb{N}} \, z_2^{\mathbb{N}} \, z_3^{\mathbb{N}} \\ \mathfrak{m}_{b_1} &= 1 & \mathfrak{m}_{b_2} &= 1 \\ \mathfrak{M}_{b_1} &= z_1^{\mathbb{N}} \, z_2^{\mathbb{N}} \, z_3^{\mathbb{N}} & \mathfrak{M}_{b_2} &= z_1^{\mathbb{N}} \, z_2^{\mathbb{N}} \, z_3^{\mathbb{N}}. \end{aligned}$$

Weierstrass reduction

Let $\{b\}$ be a Weierstrass system and $k = k_b$. Given $f \in \mathbb{S}$, Weierstrass division of $\pi_b(f)$ by $\pi_b(b)$ yields a unique series a unique $u \in \mathbb{S}_k$ such that

$$\pi_b(f) - u \, \pi_b(b) \;\in\; K \, [\![z_k^{\{0, \ldots, d_b - 1\}} \, \mathfrak{M}_{k+1}]\!] \, .$$

It follows that $f - u \, b \in K \, [\![\mathfrak{R}_b]\!]$. Moreover, if $f \in K \, [\![\mathfrak{M}_b]\!]$, then $f - u \, b \in K \, [\![\mathfrak{M}_b]\!]$. We call $\operatorname{red}_b f := f - u \, b$ the *Weierstrass reduction* of f with respect to b. If $f, b \in \mathbb{S}_L$, then $\operatorname{red}_b f \in \mathbb{S}_L$ and we may compute $\operatorname{red}_b f$ as described in Section 4.

We notice that $\operatorname{red}_b \colon \mathbb{S} \rightarrow K \, [\![\mathfrak{R}_b]\!]$ is an $\mathbb{S}_{k+1}$-linear mapping. The mapping actually preserves *infinite summation* in the following sense: a family $(f_i)_{i \in I} \in \mathbb{S}^I$ is said to be *summable* if the set $\{i \in I : \mathfrak{m} \in \operatorname{supp} f_i\}$ is finite for each $\mathfrak{m} \in \mathfrak{M}$. In that case, the sum $f = \sum_{i \in I} f_i$ is well defined by taking $f_{\mathfrak{m}} = \sum_{i \in I} (f_i)_{\mathfrak{m}}$ for each $\mathfrak{m} \in \mathfrak{M}$. Linear mappings that preserve infinite summation are said to be *strongly linear*.

Now consider a Weierstrass system $\mathcal{B} = \{b_1, \ldots, b_p\}$ with $b_1 < \cdots < b_p$. Given $f \in \mathbb{S}$, we define its *Weierstrass reduction* with respect to $\mathcal{B}$ by

$$\operatorname{red}_{\mathcal{B}} f \;=\; (\operatorname{red}_{b_p} \circ \cdots \circ \operatorname{red}_{b_1})(f). \tag{2}$$

By induction over p, it can be checked that $\operatorname{red}_{\mathcal{B}} \colon \mathbb{S} \rightarrow K \, [\![\mathfrak{R}_{\mathcal{B}}]\!]$ is a strongly linear mapping, where $\mathfrak{R}_{\mathcal{B}} = \mathfrak{R}_{b_1} \cap \cdots \cap \mathfrak{R}_{b_p}$. If $f \in \mathbb{S}_L$, then we also have $\operatorname{red}_{\mathcal{B}}(f) \in K \, [\![\mathfrak{R}_{\mathcal{B}}]\!]_L$, and we may compute $\operatorname{red}_{\mathcal{B}}(f)$ using (2).

Example 9. Let us show how to reduce

$$f = z_1 \, b_2 = z_1^2 \, z_2 \, z_3 + (z_2^2 - z_3^2) \, z_1$$

with respect to the Weierstrass system $\mathcal{B}$ from Example 8. We start with the computation of

$$\operatorname{red}_{b_1} f \;=\; f - z_2 \, z_3 \, b_1 \;=\; z_2^3 \, z_3 \, (1 + z_3) + (z_2^2 - z_3^2) \, z_1.$$

Now $\pi_{b_2}(\operatorname{red}_{b_1} f) = z_2^3 \, z_3 \, (1 + z_3)$ and $\pi_{b_2}(b_2) = z_2^2 - z_3^2$. Abbreviating $b_2' := \pi_{b_2}(b_2)$, it follows that $u = z_2 \, z_3 \, (1 + z_3)$ satisfies $\operatorname{red}_{b_2'} \pi_{b_2}(\operatorname{red}_{b_1} f) = \operatorname{red}_{b_1} f - u \, b_2'$. Consequently,

$$\begin{aligned} \operatorname{red}_{\mathcal{B}} f &= \operatorname{red}_{b_1} f - u \, b_2 \\ &= z_2 \, z_3^3 \, (1 + z_3) + (z_2^2 - z_3^2 - z_2^2 \, z_3^2 \, (1 + z_3)) \, z_1. \end{aligned}$$

We indeed have $\operatorname{supp} \operatorname{red}_{\mathcal{B}} f \subseteq \mathfrak{R}_{\mathcal{B}} = z_3^{\mathbb{N}} \cup z_2 \, z_3^{\mathbb{N}} \cup z_1 \, z_2^{\mathbb{N}} \, z_3^{\mathbb{N}}$.

Remark 10. Weierstrass reduction is somewhat different in flavour than reduction with respect to a Gröbner basis in the sense that the variables $z_1, \ldots, z_n$ do not play a symmetric role. In particular, the notion of S-polynomials has no direct counterpart in our context. Despite these differences, Weierstrass reduction admits similar applications, such as the computation of Hilbert functions, checking ideal membership, etc. The set $\mathfrak{R}_{\mathcal{B}}$ also plays a similar role as the set of "boxes below a Gröbner staircase".

Remark 11. Rather than regarding Weierstrass bases as a power series analogue of Gröbner bases, it is actually more appropriate to consider them as a natural counterpart of so-called "Janet bases" [16, 22]. The theory of Janet bases was originally developed in the context of differential equations. Nevertheless, the theory in particular applies to linear partial differential equations in $\partial_1, \ldots, \partial_n$ with constant coefficients in K, in which case we are really working with polynomials in n indeterminates $\partial_1, \ldots, \partial_n$ over K.

Reduced Weierstrass systems

A Weierstrass system $\mathcal{B}$ is itself said to be *reduced* if for each $b \in \mathcal{B}$, we have $b - \mathfrak{l}_b \in K\llbracket \mathfrak{R}_{\mathcal{B}} \rrbracket$. Two Weierstrass systems $\mathcal{B}$ and $\mathcal{B}'$ are said to be *equivalent* if $\mathrm{red}_{\mathcal{B}}$ and $\mathrm{red}_{\mathcal{B}'}$ coincide.

Let $\mathcal{B}$ be an arbitrary Weierstrass system and consider $b \in \mathcal{B}$ with $k = k_b$ and $d = d_b$. We claim that there exists a unique $u = u_b \in \mathbb{S}_k$ with $u\, b - \mathfrak{l}_b \in K\llbracket \mathfrak{R}_b \rrbracket$. Indeed, the Weierstrass preparation theorem implies the existence of a series $u \in \mathbb{S}_{k_b}$ with $u\, \pi_b(b) \in z_k^d + \mathbb{S}_{k+1}\, z_k^{d-1} + \cdots + \mathbb{S}_{k+1}$. It follows that $u\, b - \mathfrak{l}_b \in K\llbracket \mathfrak{R}_b \rrbracket$. If $b \in \mathbb{S}_L$, then Theorem 6 shows how to compute u.

Replacing b by $u_b\, b$ for each $b \in \mathcal{B}$, we obtain an equivalent Weierstrass system such that $b - \mathfrak{l}_b \in K\llbracket \mathfrak{R}_b \rrbracket$ for each $b \in \mathcal{B}$. Let $\mathcal{B} = \{b_1, \ldots, b_p\}$ with $b_1 < \cdots < b_p$. Replacing b_i by $(\mathrm{red}_{b_p} \circ \cdots \circ \mathrm{red}_{b_{i+1}})(b_i)$ for $i = p, \ldots, 1$, we obtain an equivalent reduced Weierstrass system $\tilde{\mathcal{B}}$. If $\mathcal{B} \subseteq \mathbb{S}_L$, then this procedure is completely effective, and $\tilde{\mathcal{B}} \subseteq \mathbb{S}_L$.

Weierstrass position

Let I be an ideal of $\mathbb{S}$. In this subsection, we will define when I is in *Weierstrass position*. We proceed by induction over n. The ideals $I = 0$ and $I = \mathbb{S}$ are always in Weierstrass position, which deals in particular with the case when $n = 0$.

Assume that $n > 0$ and $I \neq 0$, and let d be the minimal valuation of a non-zero element of I. Given a power series $g \in \mathbb{S}$, let $g = g_0 + g_1\, z_1 + g_2\, z_1^2 + \cdots$ be its power series expansion with respect to z_1. For each $i \in \mathbb{N}$, the sets $I_{\geqslant i} := I \cap \{g \in \mathbb{S} : \mathrm{val}_{z_1} g \geqslant i\}$ and $I_{[i]} := \{g_i : g \in I_{\geqslant i}\}$ are ideals of $\mathbb{S}$ and $\mathbb{S}_2$. We say that I is in Weierstrass position if there exists an element $f \in I$ with $f_{z_1^d} \neq 0$ and such that the ideals $I_{[0]}, \ldots, I_{[d-1]}$ of $\mathbb{S}_2$ are in Weierstrass position.

Since we assumed K to be of charactersitic zero, it contains infinitely many elements. Given a finite number of ideals $I_1, \ldots, I_p$ of $\mathbb{S}$, let us show by induction over n that there exists a linear change of coordinates for which $I_1, \ldots, I_p$ are simultaneously in Weierstrass position. A linear change of coordinates is a mapping $\mathbb{S} \rightarrow \mathbb{S}$; $f \mapsto f \circ \varphi$ with $\varphi \in \mathbb{S}_{\mathrm{lin}}^n := (K\, z_1 + \cdots + K\, z_n)^n$

For $n = 0$, we have nothing to do, so assume that $n > 0$. For each $k \in \{1, \ldots, p\}$, let $f_k \in I_k$ be a non-zero element of minimal valuation d_k. Since K is infinite, there exist $\lambda_2, \ldots, \lambda_n \in K$ such that $(f_k \circ \varphi)_{z_1^{d_k}} \neq 0$, where $\varphi = (z_1, z_2 + \lambda_2\, z_1, \ldots, z_n + \lambda_n\, z_1)$. By the induction hypothesis, there exists a vector $\psi \in (\mathbb{S}_2)_{\mathrm{lin}}^{n-1} = (K\, x_2 + \cdots + K\, x_n)^{n-1}$ of linear series such that $(I_k \circ \varphi)_{[i]} \circ \psi$ are simultaneously in Weierstrass position for $k \in \{1, \ldots, p\}$ and $i < d_k$. Setting $\psi^{\#} = (z_1, \psi_1, \ldots, \psi_{n-1}) \in \mathbb{S}_{\mathrm{lin}}^n$, we notice that $(f_k \circ \varphi \circ \psi^{\#})_{z_1^{d_k}} \neq 0$ and $(I_k \circ \varphi)_{[i]} \circ \psi = (I_k \circ \varphi \circ \psi^{\#})_{[i]}$ for all $k \in \{1, \ldots, p\}$ and $i < d_k$. Consequently, the ideals $I_k \circ \varphi \circ \psi^{\#}$ are all in Weierstrass position.

From a practical point of view, a random linear change of variables puts an ideal into Weierstrass position with probability one. From a theoretical standpoint, it suffices to extend $\mathbb{K}$ with $\binom{n}{2}$ formal parameters and to perform a generic triangular linear change of coordinates. The adjunction of new formal parameters can be done effectively using the technique from the end of Section 3.

Weierstrass bases

Let I be an ideal of $\mathbb{S}$. A Weierstrass system $\mathcal{B}$ is said to be a *Weierstrass basis* for I if $I=\{f\in\mathbb{S}:\operatorname{red}_{\mathcal{B}} f=0\}$. Assuming that I is in Weierstrass position, an abstract way to construct a Weierstrass basis goes as follows.

If $I=\{0\}$, then we take $\mathcal{B}=\varnothing$. Otherwise, let f be an element of I of minimal valuation d with $f_{z_1^d}\neq 0$. For each $i\in\{0,\ldots,d-1\}$, the induction hypothesis yields a Weierstrass basis $\mathcal{B}_{[i]}$ for the ideal $I_{[i]}$. For each $b\in\mathcal{B}_{[i]}$, there exists an element $b'=b\,z_1^i+b'_{i+1}\,z_1^{i+1}+\cdots+b'_{d-1}\,z_1^{d-1}\in I_{\geqslant i}$. Let $\mathcal{B}'_{[i]}$ be the set of all such elements b' with $b\in\mathcal{B}_{[i]}$. Then the disjoint union $\{f\}\amalg\mathcal{B}'_{[0]}\amalg\cdots\amalg\mathcal{B}'_{[d-1]}$ is a Weierstrass basis for I.

Stable Weierstrass systems

Our next aim is to provide a more effective criterion for checking whether a reduced Weierstrass system $\mathcal{B}$ is in fact a Weierstrass basis of an ideal. Given $k\in\{1,\ldots,n\}$ we will denote

$$\begin{aligned}\mathcal{B}^{(k]} &= \{b\in\mathcal{B}:k_b\leqslant k\}\\ \mathcal{B}^{[k]} &= \{b\in\mathcal{B}:k_b=k\}\\ \mathcal{B}^{[k)} &= \{b\in\mathcal{B}:k_b\geqslant k\}.\end{aligned}$$

The Weierstrass system $\mathcal{B}$ is said to be *stable* if for all $k\in\{1,\ldots,n-1\}$ and $b\in\mathcal{B}$, we have

$$\operatorname{red}_{\mathcal{B}}(x_k\,b) = 0.$$

Notice that this relation automatically holds for $b\in\mathcal{B}^{(k]}$, so it suffices to prove the relation for all $k\in\{0,\ldots,n-1\}$ and $b\in\mathcal{B}^{[k+1)}$. The main goal of this subsection is to prove the following theorem:

Theorem 12. *Any stable reduced Weierstrass system $\mathcal{B}$ is a Weierstrass basis.*

Proof. Let $k\in\{0,\ldots,n-1\}$ and notice that $\mathbb{M}_k:=K\llbracket\mathfrak{R}_{\mathcal{B}^{(k]}}\rrbracket$ is an $\mathbb{S}_{k+1}$-module. Now consider

$$\begin{aligned}M_k &= \{f\in\mathbb{M}_k:\operatorname{red}_{\mathcal{B}} f=0\}\\ &= \{f\in\mathbb{M}_k:\operatorname{red}_{\mathcal{B}^{[k+1)}} f=0\}\\ N_k &= \mathbb{M}_k\cap\sum_{b\in\mathcal{B}^{[k+1)}}\mathbb{S}_{k+1}\,b.\end{aligned}$$

We claim that $M_k=N_k$ for all k. We clearly have $M_k\subseteq N_k$. For the inverse inclusion, it suffices to show that M_k is an $\mathbb{S}_{k+1}$-module. We will use induction over $n-k$. For $k=n$, we have $M_n=N_n=0$.

Assuming that $M_k=N_k$, let us now show that $M_{k-1}=N_{k-1}$. Notice that

$$\begin{aligned}\mathbb{M}_{k-1} &= \mathbb{M}_k\oplus\mathbb{E}_k\\ \mathbb{E}_k &= \bigoplus_{b\in\mathcal{B}^{[k]}}\mathbb{S}_k\,b\end{aligned}$$

and $\operatorname{red}_{\mathcal{B}^{(k]}}\colon \mathbb{M}_{k-1} \to \mathbb{M}_k$ is an $\mathbb{S}_{k+1}$-linear projection. Now $\mathbb{M}_k$ can be regarded as an $\mathbb{S}_k$-module by letting multiplication by $\varphi \in \mathbb{S}_k$ act as

$$\varphi \cdot f \; := \; \operatorname{red}_{\mathcal{B}^{(k]}}(\varphi f) \; = \; \operatorname{red}_{\mathcal{B}^{[k]}}(\varphi f).$$

Since $\mathcal{B}$ is stable, we have $x_k \cdot b \in M_k$ for all $b \in \mathcal{B}^{[k+1)}$. Since $\mathcal{B}^{[k+1)}$ generates the $\mathbb{S}_{k+1}$-module $N_k = M_k$, it follows that M_k is an $\mathbb{S}_{k+1}[x_k]$-submodule of $\mathbb{M}_k$. Using the fact that $\operatorname{red}_{\mathcal{B}}$ is strongly linear, M_k is actually an $\mathbb{S}_k$-submodule of $\mathbb{M}_k$. In other words, $\mathbb{S}_k \, M_k \subseteq M_k + \mathbb{E}_k$. Using that $M_{k-1} = M_k \oplus \mathbb{E}_k$, we conclude that $\mathbb{S}_k \, M_{k-1} = \mathbb{S}_k \, (M_k \oplus \mathbb{E}_k) \subseteq M_k \oplus \mathbb{S}_k \, \mathbb{E}_k = M_{k-1}$, whence M_{k-1} is an $\mathbb{S}_k$-module.

Having proved our claim, we finally observe that $\mathcal{B}$ is a Weierstrass basis for $N_0 = M_0$. □

Computing Weierstrass bases

Let $\mathcal{F}$ be a finite subset of $\mathbb{S}_L$. Assuming “general position”, we will show in this section how to compute a Weierstrass basis $\mathcal{B} \subseteq \mathbb{S}_L$ for the ideal $(\mathcal{F})$. The algorithm will proceed by the repeated replacement of elements of $\mathcal{B}$ by linear combinations of elements in $\mathcal{B}$. Consequently, along with the computations, we may calculate a matrix $M \in \mathbb{S}_L^{\mathcal{B} \times \mathcal{F}}$ with $\mathcal{B} = M \mathcal{F}$ (in the sense that $b = \sum_{f \in \mathcal{F}} M_{b,f} f$ for all $b \in \mathcal{B}$). The algorithm raises an error if the general position hypothesis is violated.

As usual, we proceed by induction over n. If $\mathcal{F} \subseteq \{0\}$, then we may take $\mathcal{B} = \varnothing$ and we have nothing to do. Otherwise, let $f \in \mathcal{F} \setminus \{0\}$ be of minimal valuation d. If $f_{x_1^d} = 0$, then we raise an error. Assuming that $f_{x_1^d} \neq 0$, we first replace f by $u \, f$, where $u \in \mathbb{S}_L$ is such that $u \, f - z_1^d \in K \llbracket \mathfrak{R}_f \rrbracket$. We next replace each other element $g \in \mathcal{F} \setminus \{f\}$ by $\operatorname{red}_f g$, so that $\mathcal{F} \setminus \{f\} \subseteq K \llbracket \mathfrak{R}_f \rrbracket$. For each $i \in \{0, \ldots, d-1\}$, let $\mathcal{F}_{[i]} = \{g \in \mathcal{F} : \operatorname{val}_{z_1} g = i\}$. The recursive application of the algorithm to $(\mathcal{F}_{[i]})_i$ yields a matrix M_i such that $M_i \, (\mathcal{F}_{[i]})_i$ is a Weierstrass basis of $((\mathcal{F}_{[i]})_i)$. Consequently, $\mathcal{B}_{[i]} = M_i \, \mathcal{F}_{[i]}$ yields a Weierstrass system such that $(\mathcal{B}_{[i]})_i$ is a Weierstrass basis. The disjoint union $\mathcal{B} = \{f\} \amalg \mathcal{B}_{[0]} \amalg \cdots \amalg \mathcal{B}_{[d-1]}$ is also a Weierstrass system and we may reduce it using the algorithm described above.

At this point, we have a reduced Weierstrass system with the property that $(\mathcal{B}_{[i]})_i$ is a Weierstrass basis for each i. We next compute $\mathcal{R} = \{\operatorname{red}_{\mathcal{B}}(x_k \, b) : 1 \leqslant k < n, b \in \mathcal{B}\}$. If $\mathcal{R} = \{0\}$, then $\mathcal{B}$ is a Weierstrass basis by Theorem 12. Otherwise, we replace $\mathcal{F}$ by $\mathcal{B} \cup \mathcal{R} \setminus \{0\}$ and recompute $\mathcal{B}$ in the same way above, while keeping the same f. During each iteration of this loop, the ideals $((\mathcal{B}_{[i]})_i)$ of $\mathbb{S}_2$ can only increase, and one of them must increase strictly. Since $\mathbb{S}_2$ is Noetherian, the loop therefore terminates.

Sufficiently “general position” for avoiding any errors can be forced in a similar way as described in the subsection about Weierstrass position. In that case, we systematically work with collections $\boldsymbol{\mathcal{F}}$ such that each $\mathcal{F} \in \boldsymbol{\mathcal{F}}$ is a finite subset of $\mathbb{S}_L$. Modulo a common linear change of coordinates $\varphi \in \mathbb{S}_{\operatorname{lin}}^n$ we then compute a Weierstrass basis for each ideal $(\mathcal{F} \circ \varphi)$ with $\mathcal{F} \in \boldsymbol{\mathcal{F}}$.

Hilbert functions

Let I be an ideal of $\mathbb{S}$. For each $d \in \mathbb{N}$, let J_d be the ideal generated by all monomials $z_1^{d_1} \cdots z_n^{d_n}$ with $d_1 + \cdots + d_n = d$. Setting $D(d) = \dim (\mathbb{S} / (I + J_d))$ and $\operatorname{HF}(d) = \operatorname{HF}_I(d) = D(d+1) - D(d)$, the function $\operatorname{HF} = \operatorname{HF}_I$ is called the *Hilbert function* of I. It is well known that there exists a degree $\delta \in \mathbb{N}$ and a polynomial $H = H_I \in \mathbb{Q}[t]$ such that $\operatorname{HF}(d) = H(d)$ for all $d \geqslant \delta$. This polynomial is called the *Hilbert polynomial* of I. Moreover, the *regularity* δ_I of I is the minimal $\delta' \in \mathbb{N}$ such that $\operatorname{HF}(d) = H(d)$ for all $d \geqslant \delta'$.

Now let $\mathcal{B}$ be a Weierstrass basis for I and denote

$$\mathfrak{R}_{\mathcal{B},<d} \; = \; \mathfrak{R}_{\mathcal{B}} \cap \mathfrak{M}_{<d} \tag{3}$$

$$\mathfrak{M}_{<d} \; = \; \{z_1^{d_1} \cdots z_n^{d_n} : d_1 + \cdots + d_n < d\}. \tag{4}$$

Given $f\in\mathbb{S}$, let $f_{<d}=\sum_{\mathfrak{m}\in\mathfrak{M}_{<d}} f_{\mathfrak{m}}\,\mathfrak{m}$, so that $f_{<d}$ is a natural representative of f modulo J_d. For some $(Q_b)_{b\in\mathcal{B}}\in\mathbb{S}^{\mathcal{B}}$, we have $f=\sum_{b\in\mathcal{B}} Q_b\,b+\operatorname{red}_{\mathcal{B}}(f)$, whence $f_{<d}=\sum_{b\in\mathcal{B}}(Q_b\,b)_{<d}+\operatorname{red}_{\mathcal{B}}(f)_{<d}$. It follows that $f \operatorname{mod}(I+J_d)=\operatorname{red}_{\mathcal{B}}(f)\operatorname{mod}(I+J_d)$, whence

$$\mathbb{S}/(I+J_d)\;\cong\;K\llbracket\mathfrak{R}_{\mathcal{B},<d}\rrbracket.$$

This simply means that

$$D(d)=|\mathfrak{R}_{\mathcal{B},<d}|=|\mathfrak{M}_{<d}\setminus\mathfrak{F}_{\mathcal{B}}|=|\mathfrak{M}_{<d}|-\sum_{b\in\mathcal{B}}|\mathfrak{F}_b\cap\mathfrak{M}_{<d}|.$$

Now given $b\in\mathcal{B}$ with $\mathfrak{l}_b=z_1^{d_1}\cdots z_k^{d_k}$, we have

$$|\mathfrak{F}_b\cap\mathfrak{M}_{<d}|=|x_k^{\mathbb{N}}\cdots x_n^{\mathbb{N}}\cap\mathfrak{M}_{<d-d_1-\cdots-d_k}|=\binom{n-k+d-d_1-\cdots-d_k}{n-k+1}$$

for all $d\geqslant d_1+\cdots+d_k$. These formulas allow us to explicitly compute the Hilbert polynomial of I and the corresponding regularity.

Generalization to modules

Using a fairly standard technique, let us briefly show how the results of this section generalize to finitely generated $\mathbb{S}$-modules instead of ideals.

Let $\mathbb{M}:=\mathbb{S}^r$ be the free $\mathbb{S}$-module with canonical basis $e_1,\ldots,e_r$. We may embed this module in the $\mathbb{S}$-submodule $\mathbb{M}'=\mathbb{S}\,z_{n+1}\oplus\cdots\oplus\mathbb{S}\,z_{n+r}$ of $\hat{\mathbb{S}}:=\mathbb{S}[[z_1,\ldots,z_n,z_{n+1},\ldots,z_{n+r}]]$ *via* the mapping $\Phi\colon\mathbb{M}\to\mathbb{M}'$ defined by

$$\Phi(a_1\,e_1+\cdots+a_r\,e_r)=a_1\,z_{n+1}+\cdots+a_r\,z_{n+r}.$$

Now consider an $\mathbb{S}$-submodule M of $\mathbb{M}$ and let $I(M)$ be the ideal of $\hat{\mathbb{S}}$ generated by $M':=\Phi(M)$ and Z^2, where $Z:=(z_{n+1},\ldots,z_{n+r})$. Then

$$M'\;=\;I(M)\cap\mathbb{M}'$$

and we have a natural isomorphism of $\mathbb{S}$-modules

$$\hat{\mathbb{S}}/I(M)\;\cong\;\mathbb{M}/M\oplus\hat{\mathbb{S}}/Z\;\cong\;\mathbb{M}/M\oplus\mathbb{S}.$$

This latter identity makes it possible to carry over the constructions from this section to the case of $\mathbb{S}$-modules. In particular, one may define and compute the Hilbert function of M using the formula

$$\mathrm{HF}_M(d)\;=\;\mathrm{HF}_{I(M)}(d+1)-\mathrm{HF}_Z(d+1),$$

and it can be checked that $\mathrm{HF}_M(d)=\dim(\mathbb{M}/(M+J_d\,e_1+\cdots+J_d\,e_r))$. The corresponding Hilbert polynomial and Hilbert regularity satisfy

$$\begin{aligned}H_M(d)&=H_{I(M)}(d+1)-H_Z(d+1)\\ \delta_M&\leqslant\max(\delta_{I(M)},\delta_Z)+1.\end{aligned}$$

6 Standard bases

Let K, $\mathbb{S}=K[[z_1,\ldots,z_n]]=K\llbracket\mathfrak{M}\rrbracket$ and L be as in the previous section, but the reader may forget about the other notations defined there. Let $\preccurlyeq$ be an arbitrary total monomial ordering on $\mathfrak{M}$ with $z_1\prec 1,\ldots,z_n\prec 1$. Given a series $f\in\mathbb{S}$ and a monomial $\mathfrak{m}\in\mathfrak{M}$, we denote $f_{\succ\mathfrak{m}}=\sum_{\mathfrak{n}\succ\mathfrak{m}} f_{\mathfrak{n}}\,\mathfrak{n}$. Given a subset $\mathcal{S}\subseteq\mathbb{S}$, we also denote $\mathcal{S}_{\succ\mathfrak{m}}=\{f_{\succ\mathfrak{m}}: f\in\mathcal{S}\}$. The notations $f_{\prec\mathfrak{m}}$, $f_{\preccurlyeq\mathfrak{m}}$, $\mathcal{S}_{\prec\mathfrak{m}}$, etc. are defined likewise.

In this section, we first very briefly recall the notions of Hironaka reduction and standard bases; for more details, we refer to [10, 11]. Given a finite subset $\mathcal{F}$ of $\mathbb{S}_L$, we next show how to compute a (not necessarily reduced) standard base for $(\mathcal{F})$, using the techniques from the previous section.

Hironaka reduction

Let $\mathcal{B}$ be a finite subset of $\mathbb{S}^{\neq}$. We define

$$\begin{aligned} \mathfrak{F}_{\mathcal{B}} &= \bigcup_{b \in \mathcal{B}} \mathfrak{d}_b \mathfrak{M} \\ \mathfrak{R}_{\mathcal{B}} &= \mathfrak{M} \setminus \mathfrak{F}_{\mathcal{B}}. \end{aligned}$$

Given $f \in \mathbb{S}$, we say that f is *reduced* with respect to $\mathcal{B}$ if $\operatorname{supp} f \subseteq \mathfrak{R}_{\mathcal{B}}$. There exists a $g \in (\mathcal{B})$ such that $f - g$ is reduced with respect to $\mathcal{B}$. Writing $\mathcal{B} = \{b_1, \ldots, b_r\}$ with $b_1 < \cdots < b_r$, there actually exist unique $q_1, \ldots, q_r \in \mathbb{S}$ such that $f - q_1 b_1 - \cdots - q_r b_r$ is reduced with respect to $\mathcal{B}$ and $\mathfrak{m} \in \operatorname{supp} q_i \Rightarrow \mathfrak{d}_{b_j} \nmid \mathfrak{m} \, \mathfrak{d}_{b_i}$ for all $1 \leqslant j < i \leqslant r$. We define $\operatorname{red}_{\mathcal{B}}(f) := f - q_1 b_1 - \cdots - q_r b_r$ to be the *Hironaka reduction* of f with respect to $\mathcal{B}$ and simply write $\operatorname{red}_b = \operatorname{red}_{\mathcal{B}}$ if $\mathcal{B} = \{b\}$ is a singleton. If $f \in \mathbb{S}_L$ and $\mathcal{B} \subseteq \mathbb{S}_L$, then we do not necessarily have $\operatorname{red}_{\mathcal{B}}(f) \in \mathbb{S}_L$. Nevertheless, for any $\mathfrak{m} \in \mathfrak{M}$ such that $\mathfrak{M}_{\succ \mathfrak{m}}$ is finite, we may compute $\operatorname{red}_{\mathcal{B}}(f)_{\succ \mathfrak{m}}$ from $f_{\succ \mathfrak{m}}$ and $\mathcal{B}_{\succ \mathfrak{m}}$ using a similar recursion (over $\mathfrak{M}_{\succ \mathfrak{m}}$) as in the case of Euclidean division. We say that $\mathcal{B}$ is *autoreduced* if b is reduced with respect $\mathcal{B} \setminus \{b\}$ for all $b \in \mathcal{B}$.

Example 13. Let L be the tribe of algebraic power series. If

$$\begin{aligned} f &= z_1 z_2 \\ b &= (z_1 - z_2^2)(z_2 - z_1^2), \end{aligned}$$

then it can be shown [11, p. 75] that

$$\operatorname{red}_b(f) = \sum_{k \geqslant 0} (-1)^k \left(z_1^{3 \cdot 2^k} + z_2^{3 \cdot 2^k} \right).$$

Since the power series $\Lambda(z) := \sum_{k \geqslant 0} (-1)^k z^{2^k}$ is lacunary, it cannot be algebraic, whence $\operatorname{red}_b(f)$ is transcendental. This means that $f, b \in \mathbb{S}_L$, but $\operatorname{red}_b(f) \notin \mathbb{S}_L$.

Example 14. For those readers who are familiar with differential algebra [21], it is not hard to see that the series $\Lambda(z)$ from the previous example is even d-transcendental (this fact was first proved using different techniques in [19]): assume the contrary and consider a d-algebraic equation $P(\Lambda(z)) = 0$ over $K(z^{\mathbb{Q}})$ of minimal Ritt rank. We have $\Lambda(z) = z - \Lambda(z^2)$, so $P(z - \Lambda(z^2)) = 0$ also yields an equation of the same Ritt rank for $\Lambda(z^2)$. But the change of variables $z^2 = z'$ then gives a second, different, d-algebraic equation for $\Lambda(z')$ of the same Ritt rank as P. Applying Ritt reduction with respect to P, this yields a new equation of smaller Ritt rank, which contradicts the minimality hypothesis. In other words, if we replace L by the tribe of d-algebraic power series in the above example, then we still have $f, b \in \mathbb{S}_L$, but $\operatorname{red}_b(f) \notin \mathbb{S}_L$.

Standard bases

Given an ideal $I \subseteq \mathbb{S}$, let

$$\begin{aligned} \mathfrak{F}_I &= \{\mathfrak{d}_f : f \in I \setminus \{0\}\} \\ \mathfrak{R}_I &= \mathfrak{M} \setminus \mathfrak{F}_I. \end{aligned}$$

We say that a finite subset $\mathcal{B}$ of $\mathbb{S}^{\neq}$ is a *standard basis* for I if $(\mathfrak{d}_b)_{b \in \mathcal{B}}$ is a set of generators of $(\mathfrak{F}_I)$. We say that $\mathcal{B}$ is *reduced* if $\mathcal{B}$ is autoreduced and $b - \mathfrak{d}_b \in K[[\mathfrak{R}_I]]$ for all $b \in \mathcal{B}$. Any ideal $I \subseteq \mathbb{S}$ admits a unique reduced standard basis.

Let f, $g\in\mathbb{S}^{\neq}$ be such that $\mathfrak{d}_f=z^i=z_1^{i_1}\cdots z_n^{i_n}$ and $\mathfrak{d}_g=z^j=z_1^{j_1}\cdots z_n^{j_n}$. Let $k=\sup(i,j)=(\max(i_1,j_1),\ldots,\max(i_n,j_n))$. We define the S-series $S(f,g)\in\mathbb{S}$ of f and g to be

$$S(f,g) = g_{\mathfrak{d}_g} z^{k-i} f - f_{\mathfrak{d}_f} z^{k-j} g.$$

In a similar way as in the case of Gröbner bases, it can be shown that a finite autoreduced subset $\mathcal{B}$ of $\mathbb{S}^{\neq}$ is a standard basis if and only if $\operatorname{red}_{\mathcal{B}}(S(b,b'))=0$ for all $b,b'\in\mathcal{B}$. For any pair $(b,b')\in\mathcal{B}^2$, the relation $\operatorname{red}_{\mathcal{B}}(S(b,b'))=0$ gives rise to an $\mathbb{S}$-linear relation between the elements of $\mathcal{B}$. Using standard Gröbner basis techniques it can be shown that the space of all $\mathbb{S}$-linear relations between elements of $\mathcal{B}$ (the module of syzygies) is generated by the relations of this special form.

Given a finite set $\mathcal{F}\subseteq\mathbb{S}$ and $I=(\mathcal{F})$, this characterization theoretically allows us to compute the reduced standard basis $\mathcal{B}$ for I using a suitable local adaptation of Buchberger's algorithm. However, such an "algorithm" relies on our ability to compute reductions and Examples 13 and 14 show that we do not have any general algorithm for doing so. Nevertheless, we will show next that it is still possible to compute suitable truncations of $\mathcal{B}$.

Truncated standard bases

Given an ideal $I\subseteq\mathbb{S}$ and a monomial $\mathfrak{m}\in\mathfrak{M}$, we have $I=I_{\succ\mathfrak{m}}\oplus I_{\preccurlyeq\mathfrak{m}}$, where $I_{\preccurlyeq\mathfrak{m}}=I\cap\mathbb{S}_{\preccurlyeq\mathfrak{m}}$ is again an ideal. Let $\mathcal{B}$ be the reduced standard basis for I and assume that I is generated by a finite subset $\mathcal{F}$ of $\mathbb{S}_L$.

If $\mathfrak{M}_{\succ\mathfrak{m}}$ is finite, then for any $f\in\mathbb{S}_{\succ\mathfrak{m}}$ and $\mathcal{S}\subseteq\mathbb{S}_{\succ\mathfrak{m}}$ we have an algorithm to compute the *truncated reduction* $\operatorname{red}_{\mathcal{S}}^{\top}(f):=\operatorname{red}_{\mathcal{S}}(f)_{\succ\mathfrak{m}}\in\mathbb{S}_{\succ\mathfrak{m}}$. Similarly, for f, $g\in\mathbb{S}_{\succ\mathfrak{m}}^{\neq}$, we can compute the *truncated S-polynomial* $S^{\top}(f,\,g):=S(f,\,g)_{\succ\mathfrak{m}}\in\mathbb{S}_{\succ\mathfrak{m}}$. When using these truncated variants of reduction and S-polynomials, the local analogue of Buchberger's algorithm terminates, since all computations take place in a finite dimensional vector space. This provides us with an algorithm to compute $\mathcal{T}=\mathcal{B}_{\succ\mathfrak{m}}\setminus\{0\}$, together with a matrix $M\in\mathbb{S}_L^{\mathcal{T}\times\mathcal{F}}$ such that $\mathcal{T}=(M\mathcal{F})_{\succ\mathfrak{m}}$.

Hilbert functions

Let $\mathcal{B}$ be a standard basis of an ideal I of $\mathbb{S}$, let $d\in\mathbb{N}$, and let $\mathfrak{R}_{\mathcal{B},<d}$ be defined as in (3). In a similar way as at the end of section 5, one can show that

$$\mathbb{S}/(I+J_d) \;\cong\; K[\![\mathfrak{R}_{\mathcal{B},<d}]\!].$$

Moreover, $\mathfrak{R}_{\mathcal{B}}=\mathfrak{R}_{\{\mathfrak{d}_b:b\in\mathcal{B}\}}$ and the dimension of $K[\![\mathfrak{R}_{\{\mathfrak{d}_b:b\in\mathcal{B}\},<d}]\!]$ can be computed by the familiar technique of counting boxes below a Gröbner staircase. In other words, if we know a standard basis $\mathcal{B}\subseteq\mathbb{S}_L$ of an ideal I of $\mathbb{S}$, then we can compute the Hilbert function of I.

Computing standard bases in the Archimedean case

In this subsection we show that the Hilbert function of I also provides us with information about the possible shapes of standard bases for I. We will assume that the monomial ordering $\preccurlyeq$ on $\mathfrak{M}$ is *Archimedean* in the sense that for any $\mathfrak{m}$, $\mathfrak{n}\in\mathfrak{M}\setminus\{1\}$, there exists a $k\in\mathbb{N}$ with $\mathfrak{m}^k\prec\mathfrak{n}$. In particular, the set $\mathfrak{M}_{\succ\mathfrak{m}}$ is finite for any $\mathfrak{m}\in\mathfrak{M}$.

Theorem 15. *Let $\mathcal{F}$ be a finite subset of $\mathbb{S}_L$ and assume that the monomial ordering $\preccurlyeq$ on $\mathfrak{M}$ is Archimedean. Then there exists an algorithm to compute a standard basis $\tilde{\mathcal{B}}$ for $I=(\mathcal{F})$, together with a matrix $M\in\mathbb{S}_L^{\tilde{\mathcal{B}}\times\mathcal{F}}$ with $\tilde{\mathcal{B}}=M\mathcal{F}$.*

Proof. Using the techniques from Section 5, we can compute the Hilbert function HF_I of I. Let $\mathcal{B}$ be the reduced standard basis of I and $\mathfrak{m} \in \mathfrak{M}$. Since $\preccurlyeq$ is Archimedean, the set $\mathfrak{M}_{\succ \mathfrak{m}}$ is finite. We have shown above that this allows us to compute $\mathcal{T} = \mathcal{B}_{\succ \mathfrak{m}} \setminus \{0\}$, as well as a matrix $M \in \mathbb{S}_L^{\mathcal{T} \times \mathcal{F}}$ with $\mathcal{T} = (M \mathcal{F})_{\succ \mathfrak{m}}$. Let $\tilde{\mathcal{B}} = M \mathcal{F}$. Given $\tilde{b} \in \tilde{\mathcal{B}}$, there exists a $b \in \mathcal{B}$ with $\tilde{b}_{\succ \mathfrak{m}} = b_{\succ \mathfrak{m}} \neq 0$ and $\mathfrak{d}_b = \mathfrak{d}_{b_{\succ \mathfrak{m}}} = \mathfrak{d}_{\tilde{b}_{\succ \mathfrak{m}}} = \mathfrak{d}_{\tilde{b}}$. Consequently, $\mathfrak{I}_{\tilde{\mathcal{B}}} \subseteq \mathfrak{I}_{\mathcal{B}}$. Now we may also compute the Hilbert function $\mathrm{HF}_{\tilde{J}}$ of the ideal $\tilde{J} = (\mathfrak{I}_{\tilde{\mathcal{B}}})$. We claim that $\tilde{\mathcal{B}}$ is a standard basis for I if and only if $\mathrm{HF}_I = \mathrm{HF}_{\tilde{J}}$. Indeed, we have $\mathfrak{I}_{\tilde{J}} = \mathfrak{I}_{\tilde{\mathcal{B}}} \subseteq \mathfrak{I}_{\mathcal{B}} = \mathfrak{I}_I$, so $\mathrm{HF}_I = \mathrm{HF}_{\tilde{J}}$ if and only if $\mathfrak{I}_{\tilde{\mathcal{B}}} = \mathfrak{I}_{\mathcal{B}}$. By definition, a subset $\mathcal{A} \subseteq I$ is a standard basis of I if and only $\mathfrak{I}_{\mathcal{A}} = \mathfrak{I}_I = \mathfrak{I}_{\mathcal{B}}$.

In order to compute a standard basis, we pick smaller and smaller elements $\mathfrak{m} \in \mathfrak{M}$ for $\preccurlyeq$, and perform the above computations until we have $\mathrm{HF}_I = \mathrm{HF}_{\tilde{J}}$. Since $\preccurlyeq$ is Archimedean, $\mathfrak{m}$ eventually becomes sufficiently small so that $\mathfrak{m} \prec \mathfrak{d}_b$ for all $b \in \mathcal{B}$. At that point, we necessarily have $\mathfrak{I}_{\tilde{\mathcal{B}}} = \mathfrak{I}_{\mathcal{B}}$ and $\mathrm{HF}_I = \mathrm{HF}_{\tilde{J}}$. This proves the termination of our algorithm. □

Standard bases for modules

Let $\mathbb{M} = \mathbb{S}^r$, $\hat{\mathbb{S}} = K[[z_1, \ldots, z_{n+r}]]$ be as at the end of section 5, as well as the further notations Z, Φ and $I(M)$. Assume also that the monomial ordering on $\mathfrak{M}$ has been extended to $\hat{\mathfrak{M}} := z_1^{\mathbb{N}} \cdots z_{n+r}^{\mathbb{N}}$ in such a way that $z_{n+1} \prec 1, \ldots, z_{n+r} \prec 1$.

Given an $\mathbb{S}$-submodule M of $\mathbb{M}$, a subset $\mathcal{B}$ of $\mathbb{M}$ is defined to be a *standard basis* for M if $\mathcal{B}' := \Phi(\mathcal{B}) \cup \{z_i z_j : n+1 \leqslant i \leqslant j \leqslant n+r\}$ is a standard basis for the ideal $I(M)$ of $\hat{\mathbb{S}}$. Given such a standard basis, we may compute the Hilbert function of M using $\mathrm{HF}_M(d) = \mathrm{HF}_{I(M)}(d+1) - \mathrm{HF}_Z(d+1)$, by counting boxes below the standard bases $\mathcal{B}'$ and $\{z_{n+1}, \ldots, z_{n+r}\}$ of $I(M)$ and Z.

Given a subset $\mathcal{S} \subseteq \mathbb{M}$ and a monomial $\mathfrak{m} \in \mathfrak{M}$, we denote $\mathcal{S}_{\succ \mathfrak{m}} = \{(f_1)_{\succ \mathfrak{m}} e_1 + \cdots + (f_r)_{\succ \mathfrak{m}} e_r : f_1 e_1 + \cdots + f_r e_r \in \mathcal{S}\}$, and we define $\mathcal{S}_{\prec \mathfrak{m}}$, etc. likewise. We again have $M = M_{\succ \mathfrak{m}} \oplus M_{\preccurlyeq \mathfrak{m}}$, where $M_{\preccurlyeq \mathfrak{m}} = M \cap \mathbb{M}_{\preccurlyeq \mathfrak{m}}$ is an $\mathbb{S}$-module. The notions of truncated reduction and truncated S-"polynomials" readily generalize to modules (the S-polynomial of $f e_i$ and $g e_j$ with $i \neq j$ being zero, by definition) and it can be shown that the same holds for Theorem 15. In fact, we are up to proving something even better.

Computing standard bases in the general case

Modulo a permutation of variables, we may assume without loss of generality that $z_1 \prec \cdots \prec z_n$. The *Archimedean rank* of $\mathfrak{M}$ is defined to be the number of indices $m \in \{1, \ldots, n\}$ such that $m = n$ or $m < n$ and $z_m \prec z_{m+1}^k$ for all $k \in \mathbb{N}$. Given a finite subset $\mathcal{F}$ of $\mathbb{M}_L := \mathbb{S}_L e_1 \oplus \cdots \oplus \mathbb{S}_L e_r$, we also denote by $\mathbb{S} \mathcal{F}$ the $\mathbb{S}$-module generated by $\mathcal{F}$.

Theorem 16. *Let $\mathcal{F}$ be a finite subset of $\mathbb{M}_L$. Then there exists an algorithm to compute a standard basis $\tilde{\mathcal{B}}$ for $M = \mathbb{S} \mathcal{F}$, together with a matrix $T \in \mathbb{S}_L^{\tilde{\mathcal{B}} \times \mathcal{F}}$ with $\tilde{\mathcal{B}} = T \mathcal{F}$.*

Proof. We proceed by induction over the Archimedean rank ϱ of $\mathfrak{M}$. If $\varrho = 0$, then the result is obvious. So assume that $\varrho > 0$ and let $m \leqslant n$ be maximal such that $\mathfrak{M}^\sharp = z_1^{\mathbb{N}} \cdots z_m^{\mathbb{N}}$ has Archimedean rank one. We denote $\mathbb{S}^\flat = K[[z_{m+1}, \ldots, z_n]]$ and notice that $\mathfrak{M}^\flat = z_{m+1}^{\mathbb{N}} \cdots z_n^{\mathbb{N}}$ has Archimedean rank $\varrho - 1$.

Given $\mathfrak{m} \in \mathfrak{M}^\sharp$, we notice that the truncation $\mathbb{M}_{\succ \mathfrak{m}}$ is a free finite dimensional $\mathbb{S}^\flat$-module. By the induction hypothesis, it follows that we can compute a standard basis for the $\mathbb{S}^\flat$-submodule generated by any finite subset $\mathcal{G}$ of $\mathbb{M}_{\succ \mathfrak{m}}$. Given $f \in \mathbb{M}_{\succ \mathfrak{m}}$, we can also check whether $f \in \mathbb{S}^\flat \mathcal{G}$: it suffices to decide whether the Hilbert functions of $\mathbb{S}^\flat \mathcal{G}$ and $\mathbb{S}^\flat (\mathcal{G} \cup \{f\})$ coincide.

Given a finite subset $\mathcal{G}$ of $\mathbb{M}_{\succ \mathfrak{m}}$ as above, we say that $\mathcal{G}$ is *stable* if for all $i \in \{1, \ldots, r\}$, $f, g \in \mathbb{S}^\flat$, and $\mathfrak{v}, \mathfrak{w} \in \mathfrak{M}^\sharp$ with $\mathfrak{v} \succ \mathfrak{m}$ and $\mathfrak{w} \succ \mathfrak{m}$, we have

1. If $f \mathfrak{v} e_i \in \mathcal{G}$ and $\mathfrak{w} \in \mathfrak{v} \mathfrak{M}^\sharp$, then $(f \mathfrak{w} e_i)_{\succ \mathfrak{m}} \in \mathbb{S}^\flat \mathcal{G}$.

2. If $f\,\mathfrak{v}\,e_i, g\,\mathfrak{w}\,e_i \in \mathcal{G}$ and $\mathfrak{v} \neq \mathfrak{w}$, then $S(f\,\mathfrak{v}, g\,\mathfrak{w})_{\succ\mathfrak{m}}\,e_i \in \mathbb{S}^{\flat}\,\mathcal{G}$.

By what precedes, we have an algorithm to check whether $\mathcal{G}$ is stable. If not, then we may keep enlarging $\mathcal{G}$ with elements of the form $(f\,\mathfrak{w}\,e_i)_{\succ\mathfrak{m}}$ or $S(f\,\mathfrak{v}, g\,\mathfrak{w})_{\succ\mathfrak{m}}\,e_i$ until stabilization takes place. Due to the Noetherianity of $\mathbb{M}_{\succ\mathfrak{m}}$, this happens after a finite number of steps.

In other words, given $\mathfrak{m} \in \mathfrak{M}^{\sharp}$, the above procedure allows us to compute a stable standard basis $\mathcal{G}$ for the $\mathbb{S}^{\flat}$-module $(\mathbb{S}\,\mathcal{F})_{\succ\mathfrak{m}}$ together with the matrix $T \in \mathbb{S}_L^{\mathcal{B}\times\mathcal{F}}$ for which $\mathcal{G} = (T\,\mathcal{F})_{\succ\mathfrak{m}}$. Let $\tilde{\mathcal{B}} = T\,\mathcal{F}$. Since $\mathfrak{M}^{\sharp}$ is Archimedean, a similar reasoning as in the proof of Theorem 15 shows that the Hilbert functions of $\mathbb{S}\,\tilde{\mathcal{B}}$ and M coincide for a sufficiently small $\mathfrak{m} \in \mathfrak{M}^{\sharp}$. At that point, $\tilde{\mathcal{B}} = T\,\mathcal{F}$ contains the desired standard basis of M. □

Bibliography

[1] M. E. Alonso, F. J. Castro-Jiménez, and H. Hauser. Encoding algebraic power series. Technical report, ArXiv, 2014. http://arxiv.org/abs/1403.4104.

[2] M. E. Alonso, T. Mora, and R. Raimondo. A computational model for algebraic power series. *J. Pure and Appl. Alg.*, 77:1–38, 1992.

[3] M. Aschenbrenner, L. van den Dries, and J. van der Hoeven. *Asymptotic Differential Algebra and Model Theory of Transseries*. Number 195 in Annals of Mathematics studies. Princeton University Press, 2017.

[4] R. P. Brent and H. T. Kung. Fast algorithms for manipulating formal power series. *Journal of the ACM*, 25:581–595, 1978.

[5] J. Della Dora, C. Dicrescenzo, and D. Duval. A new method for computing in algebraic number fields. In G. Goos and J. Hartmanis, editors, *Eurocal'85 (2)*, volume 174 of *Lect. Notes in Comp. Science*, pages 321–326. Springer, 1985.

[6] J. Denef and L. Lipshitz. Ultraproducts and approximation in local rings. *Math. Ann.*, 253:1–28, 1980.

[7] J. Denef and L. Lipshitz. Power series solutions of algebraic differential equations. *Math. Ann.*, 267:213–238, 1984.

[8] J. Denef and L. Lipshitz. Decision problems for differential equations. *The Journ. of Symb. Logic*, 54(3):941–950, 1989.

[9] L. van den Dries. On the elementary theory of restricted elementary functions. *J. Symb. Logic*, 53(3):796–808, 1988.

[10] H. Hironaka. Resolution of singularities of an algebraic variety over a field of characteristic zero. *Annals of Math.*, 79:109–326, 1964.

[11] H. Hironaka. Idealistic exponents of singularity. In *Algebraic geometry, The Johns Hopkins Centennial Lectures*. John Hopkins University Press, 1975.

[12] J. van der Hoeven. Relax, but don't be too lazy. *JSC*, 34:479–542, 2002.

[13] J. van der Hoeven. *Transseries and real differential algebra*, volume 1888 of *Lecture Notes in Mathematics*. Springer-Verlag, 2006.

[14] J. van der Hoeven. From implicit to recursive equations. Technical report, HAL, 2011. http://hal.archives-ouvertes.fr/hal-00583125.

[15] J. van der Hoeven. Computing with D-algebraic power series. Technical report, HAL, 2014. http://hal.archives-ouvertes.fr/hal-00979367.

[16] M. Janet. *Sur les systèmes d'équations aux dérivées partielles*. PhD thesis, Faculté des sciences de Paris, 1920. Thèses françaises de l'entre-deux-guerres. Gauthiers-Villars.

[17] D. Lazard. Gröbner bases, gaussian elimination and resolution of systems of algebraic equations. In J. A. van Hulzen, editor, *Proc. EUROCAL'83*, number 162 in Lect. Notes in Computer Sc., pages 146–156. Springer Berlin Heidelberg, 1983.

[18] A. J. Macintyre and A. J. Wilkie. On the decidability of the real exponential field. Technical report, Oxford University, 1994.

[19] K. Mahler. Arithmetische Eigenschaften einer Klasse transzendental-transzendenter Funktionen. *Math. Z.*, 32:545–585, 1930.

[20] F. Mora. An algorithm to compute the equations of tangent cones. In *Proc. EUROCAM '82*, number 144 in Lect. Notes in Computer Sc., pages 158–165. Springer Berlin Heidelberg, 1982.

[21] J. F. Ritt. *Differential algebra*. Amer. Math. Soc., New York, 1950.

[22] D. Robertz. *Formal Algorithmic Elimination for PDEs*, volume 2121 of *Lecture Notres in Mathematics*. Springer, Cham, 2014.

[23] K. Weierstrass. *Mathematische Werke II, Abhandlungen 2*, pages 135–142. Mayer und Müller, 1895. Reprinted by Johnson, New York, 1967.