# Effective power series computations*

by Joris van der Hoeven

CNRS, LIX, École polytechnique
91128 Palaiseau Cedex
France

*Email:* vdhoeven@lix.polytechnique.fr

*October 22, 2014*

**Abstract**

Let $K$ be an effective field of characteristic zero. An effective tribe is a subset of $K[[z_1, z_2, ...]] = K \cup K[[z_1]] \cup K[[z_1, z_2]] \cup \cdots$ which 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.

**Keywords:** Power series, algorithm, Weierstrass preparation, 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 [1] or on relaxed power series evaluation [7].

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.

In 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 $K[[z_1, z_2, ...]] = K \cup K[[z_1]] \cup K[[z_1, z_2]] \cup \cdots$ which is stable under each of these operations will be called a tribe. We will also specify effective counterparts of these notions.

The main result of this note is presented in section 4: given an effective tribe with an effective zero test, we show that the tribe also satisfies an effective version of the Weierstrass preparation theorem [10], and we give an algorithm for performing Weierstrass division with remainder. Our result can for instance be applied to the tribes of algebraic power series and D-algebraic power series (see also [4, 5, 9]).

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 [6]. The notion of a tribe also shares some common properties with the notion of a Weierstrass system, as introduced by Denef and Lipshitz [3] and used in [6]. Our main theorem can be regarded as a simpler, effective and more systematic way to prove that certain types of power series form Weierstrass systems.

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

The idea behind our main algorithm is very simple: given a series $f \in L \cap K[[z_1, ..., z_n]]$ of Weierstrass degree $d$ in $z_1$, we just compute the solutions $\varphi_1$, ..., $\varphi_d$ of the equation $f(z_1, ..., z_n) = 0$ in $z_1$ inside a sufficiently large field of grid-based power series. This allows us to compute the polynomial $P = (z_1 - \varphi_1) \cdots (z - \varphi_d)$ 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 $\varphi_1, ..., \varphi_d$. For this reason, we briefly recall some basic facts about grid-based power series in section 3, as well as the basic techniques which are needed in order to compute with them.

# 2 Common operations on power series

Let $K$ be a field of characteristic zero and denote

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

where we understand that $K[[z_1, ..., z_n]]$ is naturally included in $K[[z_1, ..., z_{n+1}]]$ for each $n$. So each element $f \in K[[z_1, z_2, ...]]$ 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 which takes $f \in K$ on input and which returns **true** if $f = 0$ and **false** otherwise.

If $K$ is effective, then a power series $f \in K[[z_1, z_2, ...]]$ is said to be *computable* if we have an effective bound $n$ for its dimension (so that $f \in K[[z_1, ..., z_n]]$), together with an algorithm which takes $i \in \mathbb{N}^n$ on 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 $K[[z_1, z_2, ...]]^{\mathrm{com}}$.

### Basic operations on power series

Let $L$ be a subset of $K[[z_1, z_2, ...]]$. We will denote $L_n = L \cap K[[z_1, ..., z_n]]$ for each $n$ and say that $L$ is *effective* if $L \subseteq K[[z_1, z_2, ...]]^{\mathrm{com}}$. In this section, we will give definitions of several operations on power series and the corresponding closure properties that $L$ may satisfy. From now on, we will always assume that $L$ is at least a $K$-algebra. 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 $K$-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 which takes $i \in \mathbb{N}$ on input and which computes $z_i \in L$. We say that $L$ is *effectively stable under differentiation* if there exists an algorithm which takes $f \in L$ and $i \in \mathbb{N}$ on input and which computes $\partial_i f \in L$.

### Restricted division

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

### Composition

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

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

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

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

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 $k$:

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

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

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

### Implicit functions

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

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 $(\partial \varphi / \partial z)(0)$ 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 $\varphi_1$ only, we obtain a function $\xi \in L_{n-1}$ with $\varphi_1 \circ (\xi, z_1, ..., z_{n-1}) = 0$. Differentiating this relation, we also obtain

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

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 $\varphi_i' = \varphi_{i+1}\circ(\xi, z_1, ..., z_{n-1}) \in L$. 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 $\psi_2$, ..., $\psi_m \in L_p$ such that $\varphi_i'\circ(\psi_2, ..., \psi_m, z_1, ..., z_p) = 0$ for all $i$. Setting $\psi_1 = \xi\circ(\psi_2, ..., \psi_m, z_1, ..., z_p) \in L_p$, we conclude that $\varphi_1\circ(\psi_1, ..., \psi_m, z_1, ..., z_p) = \varphi_1\circ(\xi, z_1, ..., z_{n-1})\circ(\psi_2, ..., \psi_m, z_1, ..., z_p) = 0$ and

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

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

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

is called a monomial transformation, where $i \in \mathbb{Q}^n$ is considered as a column vector. For a power series $f \in K[[z_1, ..., z_n]]$ 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 $M\cdot\operatorname{supp} f \not\subseteq \mathbb{N}^n$).

If $M \in \mathbb{N}^{n\times n}$ has positive 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 $f \in K[[z_1, z_2, ...]]$ is said to be *algebraic* if it satisfies a non trivial algebraic equation over the polynomial ring $K[z_1, z_2, ...] = K \cup K[z_1] \cup K[z_1, z_2] \cup \cdots$. Setting $H = K(z_1, z_2, ...) = K \cup K(z_1) \cup K(z_1, z_2) \cup \cdots$, this is the case if and only if the module $H[f]$ is a $H$-vector space of finite dimension. Using this criterion, it is not hard to prove that the set $K[[z_1, z_2, ...]]^{\text{alg}}$ of algebraic power series is a tribe (and actually the smallest tribe for inclusion). Assume that $K$ is an effective field. Then an effective algebraic power series $f \in K[[z_1, z_2, ...]]$ can be effectively represented as an effective power series together with an annihilator $P \in K[z_1, z_2, ...][F]$. It can be shown that $K[[z_1, z_2, ...]]^{\text{alg}}$ is an effective tribe for this representation.

A power series $f \in K[[z_1, ..., z_n]]$ is said to be *D-algebraic* if it satisfies a non trivial algebraic differential equation $P_i(f, ..., \delta_i^{r_i} f) = 0$ for each $i \in \{1, ..., n\}$, where $P_i$ is a non zero polynomial in $r_i + 1$ variables with coefficients in $K$. We denote by $K[[z_1, z_2, ...]]^{\text{dalg}}$ the set of D-algebraic power series. 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 [9], one may find more information on how to compute with D-algebraic power series, and a full proof of the fact that $K[[z_1, z_2, ...]]^{\text{dalg}}$ is an effective tribe (the proof being based on earlier techniques from [4, 5]).

## 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 an asymptotic partial ordering $\preccurlyeq$ which 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 $\mathfrak{m}_1 \mathfrak{n} \preccurlyeq \mathfrak{m}_2 \mathfrak{n} \Rightarrow \mathfrak{m}_1 \preccurlyeq \mathfrak{m}_2$). 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 $\{\mathfrak{m}_1, ..., \mathfrak{m}_m\} \subseteq \mathfrak{M}^{\prec}$ and $\{\mathfrak{n}_1, ..., \mathfrak{n}_n\} \subseteq \mathfrak{M}$ such that

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

If $\mathfrak{M}$ is actually a group which 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 $\mathfrak{m} \in \mathfrak{M} \mapsto \mathfrak{m} \in \mathfrak{G}$ is computable and if finite sets $\{\mathfrak{m}_1, ..., \mathfrak{m}_m\} \subseteq \mathfrak{M}^{\prec}$ and $\{\mathfrak{n}_1, ..., \mathfrak{n}_n\} \subseteq \mathfrak{M}$ 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 [8, 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 $f \in K[[z_1, ..., z_n]]$ and grid-based series $g_1, ..., g_n \in K[\![\mathfrak{M}]\!]^{\prec}$, there is also a natural definition for the composition $f(g) = f \circ g = f(g_1, ..., g_n) = f \circ (g_1, ..., g_n)$.

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.

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 $z^{\mathbb{N}} \in \{z^i : i \in \mathbb{N}\}$ 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 $K((z))$ and $K[\![z^{\mathbb{Q}}]\!]$ 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 $\mathfrak{M}_1$, ..., $\mathfrak{M}_n$, 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 $\mathfrak{m}_1, \mathfrak{n}_1 \in \mathfrak{M}_1$, ..., $\mathfrak{m}_n, \mathfrak{n}_n \in \mathfrak{M}_n$. Then $K[\![z_1^{\mathbb{N}} \times \cdots \times z_n^{\mathbb{N}}]\!]$ coincides with the set of power series $K[[z_1, ..., z_n]]$, whereas $K[\![z_1^{\mathbb{Z}} \times \cdots \times z_n^{\mathbb{Z}}]\!]$ coincides with the set of Laurent series $K((z_1, ..., z_n))$.

Given monomial monoids $\mathfrak{M}_1$, ..., $\mathfrak{M}_n$, one may also form the set $\mathfrak{M}_1 \mathbin{\dot\times} \cdots \mathbin{\dot\times} \mathfrak{M}_n$ 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 $K[\![z_1^{\mathbb{N}} \mathbin{\dot\times} \cdots \mathbin{\dot\times} z_n^{\mathbb{N}}]\!]$ should naturally be interpreted as $K[[z_1]] \cdots [[z_n]]$ (which it is isomorphic to $K[[z_1, ..., z_n]]$). The set $K[\![z_1^{\mathbb{Z}} \mathbin{\dot\times} \cdots \mathbin{\dot\times} z_n^{\mathbb{Z}}]\!]$ is a field which contains $K((z_1, ..., z_n))$, and this inclusion is strict if $n > 1$ (notice also that $K[\![z_1^{\mathbb{Z}} \mathbin{\dot\times} \cdots \mathbin{\dot\times} z_n^{\mathbb{Z}}]\!] \subsetneq K((z_1)) \cdots ((z_n))$). If $K$ is algebraically closed, then $K[\![z_1^{\mathbb{Q}} \mathbin{\dot\times} \cdots \mathbin{\dot\times} z_n^{\mathbb{Q}}]\!]$ is again an algebraically closed field (and again, we have $K[\![z_1^{\mathbb{Q}} \mathbin{\dot\times} \cdots \mathbin{\dot\times} z_n^{\mathbb{Q}}]\!] \subsetneq K[\![z_1^{\mathbb{Q}}]\!] \cdots [\![z_n^{\mathbb{Q}}]\!]$).

### Cartesian representations

From now on, we will assume that $\mathfrak{M}$ is a monomial group which is generated as a group by its infinitesimal elements. Given a series $f \in K[\![\mathfrak{M}]\!]$, a *Cartesian representation* for $f$ is a Laurent series $\check{f} \in K((z_1, ..., z_k))$ together with monomials $\mathfrak{m}_1, ..., \mathfrak{m}_k \in \mathfrak{M}^{\prec}$ such that $f = \check{f}(\mathfrak{m}_1, ..., \mathfrak{m}_k)$. Given several series $f_1, ..., f_l \in K[\![\mathfrak{M}]\!]$, and Cartesian representations for each of the $f_i$, we say that these Cartesian representations are *compatible* if they are of the form $f_i = \check{f}_i(\mathfrak{m}_1, ..., \mathfrak{m}_k)$ for $\check{f}_i \in K((z_1, ..., z_k))$ and $\mathfrak{m}_1, ..., \mathfrak{m}_k \in \mathfrak{M}^{\prec}$. In [8, Proposition 3.12] we show that such compatible Cartesian representations always exist.

In [8, Chapter 3], we give 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 [8, Lemma 3.13]:

**Lemma 1.** *Let $\mathfrak{z}_1, ..., \mathfrak{z}_k, \mathfrak{m}_1, ..., \mathfrak{m}_l$ be infinitesimal elements of an effective totally ordered monomial group $\mathfrak{M}$ with $\mathbb{Q}$-powers, such that we have explicit expressions for $\mathfrak{m}_1, ..., \mathfrak{m}_l \in \mathfrak{z}_1^{\mathbb{Z}} \cdots \mathfrak{z}_k^{\mathbb{Z}}$ as power products. Then we may effectively compute infinitesimal $\mathfrak{z}_1', ..., \mathfrak{z}_k' \in \mathfrak{z}_1^{\mathbb{Q}} \cdots \mathfrak{z}_k^{\mathbb{Q}}$ with $\mathfrak{z}_1, ..., \mathfrak{z}_k, \mathfrak{m}_1, ..., \mathfrak{m}_l \in (\mathfrak{z}_1')^{\mathbb{N}} \cdots (\mathfrak{z}_k')^{\mathbb{N}}$.* □

### $L$-based power series

Let $L$ be a local community. We will say that $f \in K[\![\mathfrak{M}]\!]$ is *$L$-based* if $f$ admits a Cartesian representation of the form $f = \check{f}(\mathfrak{m}_1, ..., \mathfrak{m}_k)$ with $\check{f} = \varphi\, z_1^{i_1} \cdots z_k^{i_k}$, $\varphi \in L_k$ and $i_1, ..., i_k \in \mathbb{Z}$. The set $K[\![\mathfrak{M}]\!]_L$ of all such series forms a $K$-algebra [8, Proposition 3.14]. If $K$, $L$ and $\mathfrak{M}$ are effective, then any grid-based series in $K[\![\mathfrak{M}]\!]_L$ is computable. Moreover, we may effectively represent series in $K[\![\mathfrak{M}]\!]_L$ by Cartesian representations, and $K[\![\mathfrak{M}]\!]_L$ is an effective $K$-algebra for this representation.

A Cartesian representation $f = \check{f}(\mathfrak{m}_1, ..., \mathfrak{m}_k)$ of $f \in K[\![\mathfrak{M}]\!]$ 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 $\check{\mathfrak{v}}(\mathfrak{m}_1, ..., \mathfrak{m}_k) \preccurlyeq \mathfrak{w}$. We have the following effective counterpart of [8, Proposition 3.19]:

**Proposition 2.** *Assume that $K$, $L$ and $\mathfrak{M}$ are effective. Then there exists an algorithm which takes a series in $K[\![\mathfrak{M}]\!]_L$ on input and computes a faithful Cartesian representation $f = \check{f}(\mathfrak{m}_1, ..., \mathfrak{m}_k)$ with $\check{f} = \varphi\, z_1^{i_1} \cdots z_k^{i_k}$, $\varphi \in L_k$ and $i_1, ..., i_k \in \mathbb{Z}$.* □

Faithful Cartesian representations are a useful technical tool for various computations. They occur for instance in the proof of the following effective counterpart of [8, Proposition 3.20]:

**Proposition 3.** *Assume that $K$, $L$ and $\mathfrak{M}$ are effective. There exists an algorithm which takes an infinitesimal (or bounded, or regular) series $f \in K[\![\mathfrak{M}]\!]$ on input and which computes a Cartesian representation $f = \check{f}(\mathfrak{m}_1, ..., \mathfrak{m}_k)$ 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 $K[F]$. 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 solution 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 [8, Chapter 3] can be generalized in a straightforward way to power series equations instead of polynomial equations and the effective counterpart of [8, Theorem 3.21] becomes:

**Theorem 4.** *There exists an algorithm which takes $P \in K[\![\mathfrak{M} \times F^{\mathbb{N}}]\!]_L \subseteq K[\![\mathfrak{M}]\!][[F]]$ with $P \neq 0$ on input and which 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 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 4 coincides with the Weierstrass degree, when counting with multiplicities.

# 4 Effective Weierstrass preparation

### Effective algebraic closures

Let $K$ be an effective field with an effective zero test. We may consider its algebraic closure $K^{\mathrm{alg}}$ as an effective field with an effective zero test, when computing non deterministically (we refer to [2] 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 $K^{\mathrm{alg}} \otimes L$ by polynomials $P \in L[\alpha]$, where $\alpha \in K^{\mathrm{alg}}$. The algebraic number $\alpha$ is effectively represented using an annihilator $A \in L[X]$ and we may always take $P$ such that $\deg P < \deg A$. It is a routine verification that $K^{\mathrm{alg}} \otimes L$ forms again an effective tribe for this representation.

Consider a series $f \in K^{\mathrm{alg}} \otimes L \cap K[[z_1, z_2, ...]]$, represented as $f = P(\alpha) = P_0 + \cdots + P_{k-1}\, \alpha^{k-1}$, where $\alpha \in K^{\mathrm{alg}}$ is given by an annihilator of degree $k$. 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 $\alpha$. On the other hand, $[z^i]\, P \in K$, which means that we can compute an annihilator for $\alpha$ 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 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 unit $u \in K[[z_1, ..., z_n]]$ and a monic polynomial $P = z^d + P_{d-1}\, z_1^{d-1} + \cdots + P_0 \in K[[z_2, ..., z_n]][z_1]$ of degree $d$ such that $f = u\, P$. The polynomial $P$ is called the *Weierstrass polynomial* associated to $f$. 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 5.** *There exists an algorithm which takes a power series $f \in L_n$ of Weierstrass degree $d$ on input and computes its Weierstrass polynomial $P$ as an element of $L_n$.*

**Proof.** Consider the effective totally ordered monomial group $\mathfrak{M} = z_2^{\mathbb{Q}} \dot{\times} \cdots \times z_n^{\mathbb{Q}}$ with $\mathbb{Q}$-powers. We have a natural inclusion $L_n \subseteq K^{\mathrm{alg}}[\![\mathfrak{M} \times z_1^{\mathbb{N}}]\!]_{K^{\mathrm{alg}} \otimes L}$. Now consider $f \in K^{\mathrm{alg}}[\![\mathfrak{M} \times z_1^{\mathbb{N}}]\!]_{K^{\mathrm{alg}} \otimes L} \subseteq K^{\mathrm{alg}}[\![\mathfrak{M}]\!][[z_1]]$. By theorem 4, we may compute all infinitesimal solutions $\varphi_1, ..., \varphi_d \in K^{\mathrm{alg}}[\![\mathfrak{M}]\!]_{K^{\mathrm{alg}} \otimes L}$ to the equation $f(\varphi) = 0$ in $z_1$ (we recall that there are $d$ such solutions, when counting with multiplicities, since $K^{\mathrm{alg}}$ is algebraically closed). Now consider

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

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

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

Now consider a Cartesian representation $P = \check{P}(\mathfrak{m}_1, ..., \mathfrak{m}_k)$ for $P$ with $\check{P} \in L$. By Proposition 3, we may take $\check{P}$ to be infinitesimal. Since $\mathfrak{m}_1, ..., \mathfrak{m}_k$ are infinitesimal and $\mathfrak{m}_1, ..., \mathfrak{m}_k \in z_1^{\mathbb{Q}} \cdots z_n^{\mathbb{Q}}$, Lemma 1 also shows that we may assume without loss of generality that $k \leqslant n$. Completing the $\mathfrak{m}_1, ..., \mathfrak{m}_k$ 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 $P \in K[[z_1, ..., z_n]]$ and $L$ is effectively closed under restricted monomial transformations, we conclude that $P \in L_n$. □

**Effective Weierstrass division**

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 exists a quotient $Q$ and a remainder $R$ in $K[[z_2, ..., z_n]][z_1]$ with

$$g = Q f + R$$

and $\deg_{z_1} R < d$. We claim that $Q$ and $R$ once again belong to $L_n$ and that there exists an algorithm to compute them:

**Theorem 6.** *There exists an algorithm which takes a power series $f \in L_n$ of Weierstrass degree $d$ and $g \in L_n$ on input and computes the quotient and remainder of the Weierstrass division of $g$ by $f$ as elements of $L_n$.*

**Proof.** Let $\varphi_1, ..., \varphi_s$ be the distinct solutions of $f(\varphi) = 0$ when considered as an equation in $z_1$, and let $\mu_i$ be the multiplicity of each $\varphi_i$, so that $\mu_1 + \cdots + \mu_s = d$. For each $i$, we compute the polynomials

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

Using Chinese remaindering, we next compute the unique $R \in K^{\mathrm{alg}}[\![\mathfrak{M}]\!]_{K^{\mathrm{alg}} \otimes L}[z]$ such that $R \equiv A_i \bmod B_i$ for each $i$ and $\deg_z R < d$. It is easily verified that $R$ coincides with the remainder of the Weierstrass division of $g$ by $f$. In particular, $R \in K[[z_1, ..., z_n]]$ and we may obtain $R$ as an element of $L_n$ in the same way as in the proof of Theorem 5. We obtain the quotient $Q$ of the Weierstrass division by performing the restricted division of $g - R$ by $f$. □

# Bibliography


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

**[2]** 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.

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

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

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

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

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

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

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

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