# Computing with D-algebraic power series

Joris van der Hoeven

# Computing with D-algebraic power series*

by Joris van der Hoeven

CNRS, LIX, École polytechnique
91128 Palaiseau Cedex
France

*Email:* vdhoeven@lix.polytechnique.fr

*April 15, 2014*

**Abstract**

In this paper, we will present several algorithms for computing with D-algebraic power series. Such power series are specified by one or more algebraic differential equations and a sufficient number of initial conditions. The emphasis is not on the efficient computation of coefficients of such power series (various techniques are known for that), but rather on the ability to decide whether expressions involving D-algebraic power series are zero. We will both consider univariate and multivariate series and, besides the usual ring operations and differentiation, we will also consider composition, implicitly determined power series and monomial transformations.

**Keywords:** D-algebraic power series, algorithm, zero-test, implicit function
**A.M.S. subject classification:** 68W30, 34A09, 34A12

# 1 Introduction

## General introduction

Let $K$ be a field of characteristic zero. A power series $f \in K[[z]]$ is said to be *D-algebraic* if it satisfies a non trivial differential equation $P(f(z), f'(z), ..., f^{(r)}(z)) = 0$, where $P$ is a polynomial with coefficients in $K$. The set of D-algebraic power series contains many classical transcendental functions, such as $\exp z$, $\log z$, $\wp(z)$, etc., and it is closed under the ring operations, restricted division, differentiation and composition. This makes the differential ring of D-algebraic power series suitable as a framework for exact computations with mathematical expressions which involve transcendental functions.

The notion of D-algebraic power series admits a straightforward generalization to the multivariate context. In this case, we require the satisfaction of a non trivial algebraic differential equation with respect to each of the partial derivatives. The multivariate context allows for some additional operations, such as the resolution of implicit power series equations and general monomial transformations with rational powers. Again, the set of D-algebraic power series is stable under such operations.

There are two main aspects about 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 [2, 1, 9] or on relaxed power series evaluation [8, 6, 10].

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

On the other hand, there is the problem of deciding whether a given power series is zero. This problem is hard in the sense that we need to check the cancellation of an infinite number of coefficients. Therefore, a related question is how to represent power series in such a way that we can design such zero tests. We also notice the asymmetric aspect of the problem: given a non zero series $f$, it is usually easy to prove that $f \neq 0$: it suffices to compute a non zero coefficient. However, if $f$ vanishes, then it is potentially difficult to establish a formal proof of this fact.

In this paper, we will focus on the second aspect. We will consider various representations for D-algebraic power series, show how to perform common operations on power series when using these representations, and also present several zero tests. All representations are based on a combination of differential equations satisfied by the power series and initial conditions. However, depending on additional properties of these equations, some representations are more suitable for performing common operations and zero testing.

For global computations with algebraic differential equations, it is convenient to use the classical framework of differential algebra [17, 14]. In addition, we need some technology in order to deal with initial conditions. One key ingredient is the determination of the number of initial conditions which are needed in order to guarantee that a power series solution of a system of differential equations is unique. For this, we will use a similar technique as the one introduced by Denef and Lipshitz in [4, 5], and develop this technique in further detail.

## Structure of the paper and main results

Apart from a first section 2 with some reminders from differential algebra, the paper is subdivided into three main parts. In section 3, we first focus on the univariate case and the representation of a D-algebraic series $f$ by a single differential polynomial which annihilates $f$ together with a sufficient number of initial conditions. In section 4, we remain in the univariate setting, but switch to more flexible representations of D-algebraic series as solutions to systems of algebraic differential equations with sufficiently many initial conditions. In section 5, we generalize our results to the multivariate setting and also consider the additional operations of solving implicit equations, composition, and monomial transformations.

In section 3, we effectively represent D-algebraic power series by a pair $(f, P)$, where $f \in K[[z]]$ is a computable power series (meaning that the function $n \mapsto f_n$ is computable) and a non zero differential polynomial $P \in K\{F\}$ such that $P(f) = 0$. Specializing a more general result from [4, 5], we will show how to compute a number $\sigma \in \mathbb{N}$ (called a root separation bound for $P$ at $f$) with the property that the equation $P(g) = 0$ admits no other solutions $g$ with $v(g - f) \,\square\, \sigma$. Moreover, if $f$ is a "non degenerate root" of $P$ (in the sense that $S_P(f) \neq 0$, where $S_P$ is a simpler non zero differential polynomial, called the separant of $P$), then we actually obtain an explicit recurrence relation for $f_n$ in terms of $f_0, \ldots, f_{n-1}$ for $n \,\square\, \sigma$.

In section 3.3, we will exploit the existence of such a recurrence relation in the non degenerate case, by giving a first zero test for series in the differential field $K\langle f \rangle$ generated by $f$. We will next strengthen the root separation bound by not only looking for other solutions of $P(g) = 0$ in $K[[z]]$, but also in $K[\log z][[z]]$. In section 3.4, this allows us to simplify the zero test (along similar lines as in [7]) and also widen its scope to power series which depend on a finite number of parameters (Remark 10). We finally consider the case when $f$ is ill specified as a degenerate root of $P$. In sections 3.5 and 3.6, we give algorithms for computing root separation bounds in this case, as well as non degenerate annihilators.

In principle, annihilators of complex D-algebraic series (such as large expressions in other D-algebraic series) can be computed using brute force (Proposition 14). However, this technique is deemed to be very inefficient. For this reason, we introduce the more flexible framework of D-domains in section 4. In this framework, we express D-algebraic series as rational functions in a finite number of D-algebraic series which satisfy a special kind of system of algebraic differential equations with initial conditions. We will show how to adopt the major results from section 3 to this setting.

In section 5, we turn our attention to multivariate D-algebraic series. We will start by showing how to interpret a multivariate D-algebraic series in $K[[z_1, ..., z_n]]$ as a D-algebraic series in $z_n$ whose coefficients are D-algebraic series in $K[[z_1, ..., z_{n-1}]]$. We next generalize the notion of a D-domain and show that the above reduction to the univariate case can be done at the level of D-domains. We conclude by giving some algorithms for some typical multivariate operations: the resolution of implicit equations, composition, and monomial transformations. In each of these cases, we will show how to avoid the computation of differential annihilators as much as possible, by remaining in the framework of multivariate D-domains.

## Comparison with previous work

There are several approaches to the zero test problem for D-algebraic power series [16, 4, 5, 13, 18, 19, 15, 12] and we refer to [7] for a brief discussion. From a logical point of view, the most important decision problems for power series solutions to algebraic differential equations with initial conditions were settled in [4, 5]. One essential tool in this paper is the computation of a generalization of root separation bounds for more general decision problems. In a sense, this paper merely consists of specializations of these results to more specific problems. Nevertheless, we think that we introduced some noteworthy improvements which we will point out now.

It should first be emphasized that the papers [4, 5] are based on a more general decision procedure for testing whether systems of differential equations and inequations with initial conditions admit solutions. Efficiency is not the major concern here. The authors also do not attempt to state their results in terms of classical differential algebra, even though they are aware of this possibility. From our point of view, one main contribution of this paper is to isolate the part of the problem which can be dealt with classical differential algebra techniques from the part where initial conditions and root separation bounds come in (notice that [15] provides an interesting alternative way to achieve this goal). As a consequence, we can explicitly state our zero test algorithms, which we also believe to be more efficient.

Our approach also contains a few theoretical improvements. First of all, we mainly work over a so called "effective power series domain" $A \subseteq K[[z]]$ instead of the constant field $K$. For instance, we may take $A = K\langle\varphi\rangle \cap K[[z]]$, where

$$\varphi = \sum_{n \geqslant 2} \frac{(-1)^n B_n}{n\,(n-1)}\, z^{n-1}$$

is the differentially transcendental power series involved in the Euler-Maclaurin formula for the $\Gamma$-function. Similarly, the conditions on the constant field $K$ are slightly weaker: we merely require an effective constant field $K$ with an algorithm for the computation of all positive integer roots of polynomials in $K[N]$. The improved zero test from section 3.4 also allows for power series which depend on parameters.

These theoretical improvements were actually introduced in [7], but the current presentation is a bit simpler and more systematic. In particular, we only need to consider logarithmic power series instead of logarithmic transseries in the correctness proof of the improved zero test from section 3.4. Furthermore, we added algorithms for the computation of non degenerate annihilators and root separation bounds in the degenerate case.

Section 4 contains no theoretical improvements, but we expect the more flexible framework of D-domains to be most suitable for practical computations. It is interesting to see that the root separation bounds and both zero tests from section 3 can be generalized to this setting. In particular, for the computation of root separation bounds, we introduced the dominant Hermite normal form, which seems interesting in its own right.

As we show in section 5, a multivariate D-algebraic series in $K[[z_1, ..., z_n]]$ can always be regarded as a D-algebraic series in $z_n$ whose coefficients are D-algebraic series in $K[[z_1, ..., z_{n-1}]]$. From the logical point of view, decision problems for such series therefore reduce to their univariate counterparts. However, there are a few additional operations, such as solving implicit equations, extraction of coefficients and monomial transformations. Not only do we present algorithms for carrying out such operations, but we also discuss ways to make this efficient, in the framework of multivariate D-domains.

# 2 Reminders from differential algebra

## 2.1 Ritt reduction

Let us recall some standard notations from differential algebra. Let $K$ be a field of characteristic zero and let $A$ be a differential $K$-algebra which is also an integral domain. We will mainly work with respect to a single derivation $\delta$. Given a finite number of indeterminates $F_1, ..., F_k$, we will denote by $A\{F_1, ..., F_k\}$ or simply by $A\{F\}$ the differential ring of differential polynomials in $F_1, ..., F_k$ and by $A\langle F_1, ..., F_k\rangle$ or $A\langle F\rangle$ its fraction field.

We will assume an admissible ranking $\square$ on the set $\mathcal{V} = \{\delta^j F_i : i \in \{1, ..., k\}, j \in \mathbb{N}\}$. For instance, we may take $\delta^j F_i \square \delta^{j'} F_{i'}$ whenever $j < j'$ or $j = j'$ and $i < i'$. Given such a ranking, the *leader* of a differential polynomial $P \in A\{F\} \setminus A$ is the highest variable $\delta^j F_i$ occurring in $P$ when $P$ is considered as a polynomial in $\mathcal{V}$. We will denote by $\ell_P$ the leader of $P$. Considering $P$ as a polynomial in $\ell_P$, the leading coefficient $I_P$ is called the *initial* of $P$, $S_P = \partial P / \partial \ell_P$ the *separant*, and we will denote $H_P = I_P S_P$. If $P$ has degree $d$ in $\ell_P$, then the pair $\operatorname{rank} P = (\ell_P, d)$ is called the *Ritt rank* of $P$ and such pairs are ordered lexicographically. We will also denote $\ell_P^* = \ell_P^d$ in that case.

Given $P, Q_1, ..., Q_l \in A\{F\} \setminus A$, we say that $P$ is *reducible* with respect to $Q_1, ..., Q_l$ if there exists an $i$ such that $\ell_P \in \delta^{\mathbb{N}\setminus\{0\}} \ell_{Q_i}$ or $\ell = \ell_P = \ell_{Q_i}$ and $\deg_\ell P \square \deg_\ell Q_i$. The process of *Ritt reduction* provides us with a relation of the form

$$I_{Q_1}^{\alpha_1} \cdots I_{Q_l}^{\alpha_l} S_{Q_1}^{\beta_1} \cdots S_{Q_l}^{\beta_l} P \;=\; \Theta_1 Q_1 + \cdots + \Theta_k Q_k + R,$$

where $\alpha_1, ..., \alpha_l, \beta_1, ..., \beta_l \in \mathbb{N}$, $\Theta_1, ..., \Theta_k \in A\{F\}[\delta]$, $R \in A\{F\}$ and where $R$ is reduced with respect to $Q_1, ..., Q_l$. We will denote $R = P \operatorname{rem} Q = P \operatorname{rem} (Q_1, ..., Q_l)$.

Given $Q_1, ..., Q_l \in A\{F\}$, we recall that $[Q] = [Q_1, ..., Q_l] = A[\delta]\, Q_1 + \cdots + A[\delta]\, Q_l$ stands for the differential ideal generated by $Q_1, ..., Q_l$. If $Q_1, ..., Q_l \in A\{F\} \setminus A$, then we also denote $H_Q = H_{Q_1} \cdots H_{Q_l}$ and recall that

$$[Q] : H_Q^\infty \;=\; \{P \in A\{F\} : \exists n \in \mathbb{N}, H_Q^n P \in [Q]\}$$

forms a differential ideal. We say that $Q_1, ..., Q_l$ forms an *autoreduced sequence* if $Q_i$ Ritt reduces to itself with respect to $Q_1, ..., Q_{i-1}, Q_i, ..., Q_l$ for each $i$. In that case the set of differential polynomials which reduce to zero with respect to $Q_1, ..., Q_l$ coincides with the differential ideal $[Q]: H_Q^\infty$.

In section 5, we will also consider differential rings and differential polynomials with respect to a finite number of pairwise commuting derivations $\delta_1, ..., \delta_n$. In that case, $\mathcal{V}$ has to be replaced with the set of all expressions $\delta_1^{j_1} \cdots \delta_n^{j_n} F_i$ with $i \in \{1, ..., k\}$ and $j_1, ..., j_n \in \mathbb{N}$. The notion of admissible rankings and Ritt reduction can be extended to this setting and we refer to classical textbooks on differential algebra [17, 14] for more details.

## 2.2 Decompositions of differential polynomials

In order to explicitly write down a differential polynomial $P \in A\{F\}$, it is convenient to use vector notation. We will index differential monomials by vectors $\boldsymbol{i} = (i_1, ..., i_k)$ where each $i_j$ is itself a finite sequence $i_j = (i_{j,0}, ..., i_{j,r_j})$ which may be padded with zeros whenever necessary. We denote

$$\delta^{\boldsymbol{i}} F \;=\; \prod_{p,q} (\delta^q F_p)^{i_{p,q}},$$

after which we may write

$$P \;=\; \sum_{\boldsymbol{i}} P_{\boldsymbol{i}}\, \delta^{\boldsymbol{i}} F,$$

with $P_{\boldsymbol{i}} \in A$. For a fixed degree $d \in \mathbb{N}$, it will be convenient to denote by $P_d$ the homogeneous component of $P$ of degree $d$:

$$\begin{aligned} P_d \;&=\; \sum_{|\boldsymbol{i}|=d} P_{\boldsymbol{i}}\, \delta^{\boldsymbol{i}} F \\ |\boldsymbol{i}| \;&=\; \sum_{p,q} i_{p,q}. \end{aligned}$$

The largest $d$ with $P_d \neq 0$ will be called the *degree* of $P$ and we will denote it by $\deg P$. The smallest $d$ with $P_d \neq 0$ will be called the *differential valuation* of $P$ and we denote it by $\operatorname{val} P$. It will also be convenient to denote $P_{<d} = P_0 + \cdots + P_{d-1}$ and $P_{>d} = P_{d+1} + \cdots + P_{\deg P}$.

## 2.3 Additive conjugation

Given a differential polynomial $P \in A\{F\}$ and a "point" $f = (f_1, ..., f_k) \in A^k$, it is often convenient to consider the *additive conjugate* of $P$ by $f$, which is defined to be the unique differential polynomial $P_{+f} \in A\{F\}$ with

$$P_{+f}(\varepsilon) = P(f + \varepsilon)$$

for all $\varepsilon \in A^k$. The coefficients $P_{+f,\boldsymbol{i}} = (P_{+f})_{\boldsymbol{i}}$ of $P_{+f}$ can be expressed directly by using a Taylor series expansion:

$$\begin{aligned} P_{+f,\boldsymbol{i}} \;&=\; \tfrac{1}{\boldsymbol{i}!}\, P^{(\boldsymbol{i})}(f) \\ P^{(\boldsymbol{i})} \;&=\; \frac{\partial^{|\boldsymbol{i}|} P}{\prod_{p,q} (\partial(\delta^q F_p))^{i_{p,q}}} \\ \boldsymbol{i}! \;&=\; \prod_{p,q} i_{p,q}!. \end{aligned}$$

In particular, we get $P_{\boldsymbol{i}} = \boldsymbol{i}!^{-1}\, P^{(\boldsymbol{i})}(0)$.

### 2.4 Differential polynomials with power series coefficients

Assume now that $A \subseteq K[[z]]$ and $\delta = z\,\partial/\partial z$. Given $f \in A$, we will denote by $v(f) \in \mathbb{N} \cup \{\infty\}$ its valuation in $z$. This valuation naturally extends to differential polynomials in $A\{F\}$ *via* the inclusion $K[[z]]\{F\} \subseteq K\{F\}[[z]]$.

Assume now that $k = 1$ and let $P \in A[F, ..., \delta^r F] \setminus \{0\}$ be a homogeneous differential polynomial in a single variable of degree $d$. Then we will denote by $J_P \in K[N]$ the polynomial with

$$\begin{aligned} J_P(n) &= \sum_{\boldsymbol{i}} (P_{\boldsymbol{i}})_{v(P)}\, n^{\|\boldsymbol{i}\|} \\ \|\boldsymbol{i}\| &= i_1 + 2\,i_2 + \cdots + r\,i_r. \end{aligned}$$

For any series $f \in K[[z]]$, we then have

$$P(f)_{v(P)+dv(f)} = J_P(v(f))\, f_{v(f)}^d.$$

We will also denote by $Z_P$ the largest root of $P$ in $\mathbb{N}$, while taking $Z_P = -1$ if no such root exists.

### 2.5 Logarithmic power series

For some purposes, we will occasionally consider logarithmic power series $f \in K[\log z][[z]]$. Such series can still be considered as power series $f = f_0 + f_1\,z + \cdots$ in $z$ and we will still denote by $v(f)$ the valuation of $f$ in $z$. The coefficients $f_i$ are polynomials in $K[\log z]$, and we will write $f_i = f_{i,\deg f_i}\,(\log z)^{\deg f_i} + \cdots + f_{i,0}$. Notice that $\delta$ maps $K[\log z]\,z^i$ into itself for each $i$.

**Proposition 1.** *Consider a non-zero linear differential operator $L \in K[\delta]$ and write $L = L_r\,\delta^r + \cdots + L_s\,\delta^s$ with $L_r \neq 0$ and $L_s \neq 0$. Then there exists a unique operator $L^{-1}\colon K[\log z] \to K[\log z]\,(\log z)^s$ with $L\,L^{-1}\,g = g$ for every $g \in K[\log z]$.*

**Proof.** Let us first prove the existence of $L^{-1}$. If $s = 0$, then we may write $L = L_0(1 - R)$ with $R \in K[\delta]\,\delta$, and the equation $L\,f = g$ admits the solution

$$f = (1 + R + R^2 + \cdots)\,\frac{g}{L_0},$$

since $\deg R(h) < \deg h$ for every $h \in K[\log z]$. For general $L$, we may write $L = \tilde{L}\,\delta^s$ with $\tilde{L}_0 \neq 0$ and take $L^{-1}\,g = \delta^{-s}\,\tilde{L}^{-1}\,g$ with

$$\delta^{-s}\left(\sum_i h_i\,(\log z)^i\right) = \sum_i \frac{h_{i+s}}{(i+s)\cdots(i+1)}\,(\log z)^{i+s}.$$

This proves the existence of $L^{-1}$. For any $f \in K[\log z]$ of degree $d \,\square\, s$ in $\log z$, we also notice that $(L\,f)_{d-s} = d\cdots(d-(s-1))\,L_s\,f_d \neq 0$. This implies the uniqueness of $L^{-1}$. $\square$

## 3 D-algebraic power series

### 3.1 Univariate D-algebraic power series

Let $K$ be a field. Let $A \subseteq K[[z]]$ be a differential $K$-subalgebra of $K[[z]]$ for $\delta$ with the property that for all $f \in A$ and $g \in A \setminus \{0\}$ such that $f/g \in K[[z]]$, we have $f/g \in A$. We will also call $A$ a *power series domain.*

A series $f \in K[[z]]$ is said to be *D-algebraic* over $A$ if it satisfies a non trivial differential equation $P(f)=0$ with $P \in A\{F\} \setminus A$. In positive characteristic $p>0$, any series $f \in K[[z]]$ satisfies the linear differential equation

$$[\delta\,(\delta-1)\cdots(\delta-(p-1))](f) \;=\; 0,$$

whence any series is D-algebraic (indeed, $\delta - i$ annihilates all series in $z^i\,K[[z^p]]$). From now on, we will therefore assume that $K$ has characteristic zero.

**Proposition 2.** *The series $f \in K[[z]]$ is D-algebraic if and only if $A\{f\}$ admits finite transcendence degree over $A$.*

**Proof.** Assuming that $f \in K[[z]]$ is D-algebraic over $A$, pick $P \in A\{F\} \setminus A$ of minimal Ritt rank $(\delta^r F, d)$ with $P(f)=0$. Then $S_P(f) \neq 0$ and $B = A[f, ..., \delta^{r-1} f, S_P(f)^{-1}]$ is stable under the derivation $\delta$, whence $A\{f\} \cong B$ and $\mathrm{trdeg}_A\, A\{f\} \leqslant r+1$. Conversely, assume that $\mathrm{trdeg}_A\, A\{f\} = r$. Then $f, ..., \delta^{(r)} f$ satisfy a non trivial algebraic relation, whence $f$ is D-algebraic. □

**Proposition 3.** *The set $A^{\mathrm{dalg}}$ of D-algebraic series over $A$ forms a power series domain.*

**Proof.** Let $f, g \in A^{\mathrm{dalg}}$. Then $A\{f+g\} \subseteq A\{f\} + A\{g\}$, whence $\mathrm{trdeg}_A\, A\{f+g\} \leqslant \mathrm{trdeg}_A\, A\{f\} + \mathrm{trdeg}_A\, A\{g\} < \infty$ and $f+g \in A^{\mathrm{dalg}}$. Similarly, $A\{f\,g\} \subseteq A\{f\}\,A\{g\}$, whence $\mathrm{trdeg}_A\, A\{f\,g\} \leqslant \mathrm{trdeg}_A\, A\{f\} + \mathrm{trdeg}_A\, A\{g\} < \infty$ and $f\,g \in A^{\mathrm{dalg}}$. Clearly, $A\{\delta f\} \subseteq A\{f\}$, so $\mathrm{trdeg}_A\, A\{\delta f\} \leqslant \mathrm{trdeg}_A\, A\{f\}$ and $\delta f \in A^{\mathrm{dalg}}$. Assume finally that $f/g \in K[[z]]$. Then $A\{f/g\} \subseteq (A\{f\}\,A\{g\})[g^{-1}]$, whence $\mathrm{trdeg}_A\, A\{f/g\} \leqslant \mathrm{trdeg}_A\, A\{f\} + \mathrm{trdeg}_A\, A\{g\} + 1 < \infty$, so that $f/g \in A^{\mathrm{dalg}}$. □

Assume now that $A$ is an effective power series domain. The most obvious way to effectively represent a D-algebraic power series in $A^{\mathrm{dalg}}$ is to represent it by a pair $(f, P)$ where $f$ is a computable series and $P \in A\{F\} \setminus A$ a non trivial annihilator with $P(f)=0$. We define the *multiplicity* of $P$ as an annihilator of $f$ to be $\mathrm{val}\, P_{+f}$. We also say that the annihilator $P$ is *non degenerate* if $S_P(f) \neq 0$, and notice that the multiplicity of a non degenerate annihilator is one. In order to make Proposition 3 effective, we will need a way to compute a non degenerate annihilator as a function of an arbitrary annihilator. This is not completely immediate, and we will postpone the presentation of an algorithm for doing so to the end of this section.

## 3.2 Root separation bounds

Let $f \in K[[z]]$ be D-algebraic over $A$ with annihilator $P \in A\{F\} \setminus A$. Assume that there exists a number $\sigma \in \mathbb{N}$ such that for any $\tilde{f} \in K[[z]] \setminus \{f\}$ with $P(\tilde{f})=0$ and $v(\tilde{f}-f) \leqslant \sigma$, we have $\tilde{f} \neq f$. Then the smallest such number $\sigma$ will be denoted by $\sigma_{P,f}$ and we call it the *root separation* of $P$ at $f$. It corresponds to the number of initial conditions which should be known in order to determine $f$ in a unique way as a root of $P$. In fact $\sigma_{P,f}$ always exists and, as we will see in the next section, we can give an algorithm to compute it under suitable assumptions.

**Proposition 4.** *Assume that $f$ is D-algebraic over $A$ with annihilator $P \in A\{F\} \setminus A$. Then the following root separation bound holds:*

$$\sigma_{P,f} \leqslant \max\Big(v(P_{+f,\mathrm{val}\,P_{+f}}), Z_{P_{+f,\mathrm{val}\,P_{+f}}}\Big) + 1. \tag{1}$$

**Proof.** Let $d = \operatorname{val} P_{+f}$ and $\mu_d = v(P_{+f,d})$. Given $\tilde{f} = f + \varepsilon \in K[[z]]$ with $n = v(\varepsilon) < \infty$, we have

$$[P_{+f,d}(\varepsilon)]_{\mu_d + dn} \;=\; J_{P_{+f,d}}(n)\, \varepsilon_n^d. \tag{2}$$

Now assume that $n \,\square\, \max(\mu_d, Z_{P_{+f,d}}) + 1$. Then

$$v(P_{+f,>d}(\varepsilon)) \;\square\; (d+1)\, n \;>\; \mu_d + d\, n,$$

whence

$$[P(\tilde{f})]_{\mu_d + dn} \;=\; J_{P_{+f,d}}(n)\, \varepsilon_n^d\,.$$

Since $n > Z_{P_{+f,d}}$, we get $J_{P_{+f,d}}(n) \neq 0$, which entails $P(\tilde{f}) \neq 0$. □

The following proposition also provides us with a partial converse.

**Proposition 5.** *Let $P \in A\{F\} \setminus A$ and $f \in K[[z]]$. Assume that $S_P(f) \neq 0$ and that $v(P(f)) > 2\,\sigma$, with $\sigma \,\square\, \max(v(P_{+f,1}), Z_{P_{+f,1}}) + 1$. Then there exists a unique root $\tilde{f} \in K[[z]]$ of $P$ with $v(\tilde{f} - f) > \sigma$.*

**Proof.** Notice that $S_P(f) \neq 0$ implies that $P_{+f,1} \neq 0$, so that $\max(v(P_{+f,1}), Z_{P_{+f,1}})$ is finite. Let $\mu_1 = v(P_{+f,1}) < \sigma$. We have to show the existence of a unique series $\varepsilon \in K[[z]]$ with $v(\varepsilon) > \sigma$ and $P_{+f}(\varepsilon) = 0$. We may decompose

$$\begin{aligned} P_{+f} &= \mathrm{H} - \Delta, \\ \mathrm{H} &= (P_{+f,1})_{\mu_1}\, z^{\mu_1}. \end{aligned}$$

Extracting the coefficient of $z^{\mu_1+n}$ in the relation $\mathrm{H}(\varepsilon) = \Delta(\varepsilon)$ now yields

$$J_{\mathrm{H}}(n)\, \varepsilon_n \;=\; \Delta(\varepsilon)_{\mu_1+n}. \tag{3}$$

For all $n > \sigma$, we have $J_{\mathrm{H}}(n) \neq 0$ and $\Delta(\varepsilon)_{\mu_1+n}$ only depends on $\varepsilon_0, \ldots, \varepsilon_{n-1}$. In other words, the relation (3) actually provides us with a recurrence relation for the computation of $\varepsilon$. □

## 3.3 A first effective zero test

We say that $K$ is *effective* if its elements can be represented effectively and if all field operations can be carried out by algorithms. We will call $K$ an *effective diophantine field* if all positive integer roots of polynomials over $K$ can be determined by algorithm. In particular, this means that $K$ admits an effective zero test, i.e. there exists an algorithm which takes an element $x$ of $K$ on input and which returns **true** if $x = 0$ and **false** otherwise.

A power series $f \in K[[z]]$ is said to be *computable*, if there exists an algorithm for computing $f_n$ as a function of $n \in \mathbb{N}$. The power series domain $A$ will said to be *effective*, if its elements are all effective power series and if the differential $K$-algebra operations can be carried out by algorithms. We notice that the differential $K$-algebra $K[[z]]^{\mathrm{com}}$ of all computable series is effective, although it does not admit an effective zero test.

Assume now that we are given an effective power series domain $A$ with an effective zero test over an effective diophantine field $K$. Assume also that we are given an effective D-algebraic power series $f \in K[[z]]$ and an annihilator $P \in A\{F\} \setminus A$ for $f$. Assume finally that the annihilator $P$ has multiplicity one, so that we may compute $v(P_{+f,1})$ and $Z_{P_{+f,1}}$ by expanding the power series coefficients of $P_{+f,1}$. In other words, the bound (1) from Proposition 4 provides us with an effective upper bound for $\sigma_{P,f}$.

Given a polynomial $Q \in A\{F\}$, we will now give an algorithm **ZeroTest** (or $\mathbf{ZeroTest}_{P,f}$ when we want to make the dependency on $P$ and $f$ explicit) for testing whether $Q(f) = 0$. In particular, this shows that the $A$-algebra $A\langle f \rangle \cap K[[z]]$ is again an effective power series domain.

**Algorithm ZeroTest($Q$)**
INPUT: $Q \in A\{F\}$
OUTPUT: the result of the test $Q(f) = 0$

1 If $Q \in A$ then return the result of the test $Q = 0$
2 If **ZeroTest**$(I_Q)$ then return **ZeroTest**$(Q - I_Q\, \ell_Q^*)$
3 If **ZeroTest**$(S_Q)$ then return **ZeroTest**$(Q \operatorname{rem} S_Q)$
4 If $P \operatorname{rem} Q \neq 0$ then return **ZeroTest**$(P \operatorname{rem} Q)$
5 Let $\sigma := \max(v(P_{+f,1}), Z_{P_{+f,1}}, v(I_Q(f)), v(S_Q(f)), v(Q_{+f,1}), Z_{Q_{+f,1}}) + 1$
6 Return the result of the test $v(Q(f)) > 2\,\sigma$

**Proof.** We first notice that recursive calls only occur for differential polynomials of a strictly smaller Ritt rank. This guarantees termination of the algorithm.

As to its correctness, we clearly have $Q(f) = 0 \Leftrightarrow (Q - I_Q\, \ell_Q^*)(f) = 0$ at line 2 whenever $I_Q(f) = 0$.

Assume now that we reach line 3 with $S_Q(f) = 0$. Then the degree of $Q$ in its leader cannot be one, since this would imply $I_Q = S_Q$, and we know that $I_Q(f) \neq 0$. Consequently, $I_{S_Q}$ is a constant multiple of $I_Q$, whence $I_Q^i\, Q = T\, S_Q + Q \operatorname{rem} S_Q$ for some $i \in \mathbb{N}$ and $T \in A\{F\}$, and $Q(f) = 0 \Leftrightarrow (Q \operatorname{rem} S_Q) = 0$.

Assume now that we reach line 4. We have $I_Q^j\, S_Q^k\, P = U_0\, Q + \cdots + U_r\, \delta^r\, Q + P \operatorname{rem} Q$ for some $j, k \in \mathbb{N}$ and $U_0, \ldots, U_r \in A\{F\}$. Since $I_Q(f) \neq 0$ and $S_Q(f) \neq 0$, it follows that $Q(f) = 0 \Leftrightarrow (P \operatorname{rem} Q)(f) = 0$.

Assume finally that we reach step 5. If $v(Q(f)) \not> 2\,\sigma$, then we clearly have $Q(f) \neq 0$, so assume that $v(Q(f)) > 2\,\sigma$. Applying Proposition 5, we obtain a unique power series $\tilde{f} \in K[[z]]$ with $Q(\tilde{f}) = 0$ and $v(\tilde{f} - f) > \sigma$. It follows that $v(P_{+\tilde{f},1}) = v(P_{+f,1}) < \sigma$, $Z_{P_{+\tilde{f},1}} = Z_{P_{+f,1}} < \sigma$, $v(I_Q(\tilde{f})) = v(I_Q(f)) < \sigma$ and $v(S_Q(\tilde{f})) = v(S_Q(f)) < \sigma$. The relation $I_Q^j\, S_Q^k\, P = U_0\, Q + \cdots + U_r\, \delta^r\, Q$ therefore implies $P(\tilde{f}) = 0$. Applying Proposition 4 to $\tilde{f}$, we obtain the bound $\sigma_{P,\tilde{f}} \not> \sigma$. Since $v(\tilde{f} - f) > \sigma$, we conclude that $\tilde{f} = f$. □

**Remark 6.** As a variant to the algorithm, we can also check whether $Q_1(f) = \cdots = Q_n(f) = 0$ for more than one $Q_1, \ldots, Q_n \in A\{F\}$ at the same time. In that case, we keep reducing until we find a $Q \in A\{F\}$ with $(I_Q\, S_Q)(f) \neq 0$ and such that $Y \operatorname{rem} Q = 0$ for all $Y \in \{Q_1, \ldots, Q_n, P\}$.

**Remark 7.** One drawback of the above zero test is that it does not apply to power series which depend on a finite number of parameters $\lambda_1, \ldots, \lambda_l$ in $K$. Indeed, this would require a root separation bound which is uniform in these parameters. Unfortunately, the largest integer root of a simple polynomial such as $N - \lambda_1$ can become arbitrarily large, so the best uniform root separation bounds are usually $+\infty$.

## 3.4 An improved zero test

In practical applications, the series $f$ is often the solution of a classical initial value problem, in which case $Z_{P_{+f,1}} = -1$. One disadvantage of the zero test from section 3.3 is that $Z_{Q_{+f,1}}$ still depends on $Q$ in quite an unpredictable way. In particular, even for simple $Q$, this quantity might *a priori* become arbitrarily large. In this section, we will give an improved version of our algorithm which does not have this drawback. The idea is to not only consider ordinary power solutions to our differential equations, but also logarithmic power series solutions in $K[\log z][[z]]$, as introduced in section 2.5.

Let $f \in K[[z]]$ be D-algebraic over $A$ with annihilator $P \in A\{F\} \setminus A$. Assume that there exists a number $\sigma \in \mathbb{N}$ such that for any $\tilde{f} \in K[\log z][[z]] \setminus \{f\}$ with $v(\tilde{f} - f) \sqsupset \sigma$, we have $\tilde{f} \neq f$. Then the smallest such number $\sigma$ will be denoted by $\sigma^*_{P,f}$ and we call it the *strong root separation* of $P$ at $f$. Proposition 4 naturally strengthens to this setting:

**Proposition 8.** *Assume that $f$ is D-algebraic over $A$ with annihilator $P \in A\{F\} \setminus A$. Then the following strong root separation bound holds:*

$$\sigma^*_{P,f} \sqsupset \max\Big(v(P_{+f,\operatorname{val} P_{+f}}), Z_{P_{+f,\operatorname{val} P_{+f}}}\Big) + 1. \tag{4}$$

**Proof.** The proof is similar to the proof of Proposition 4 with the following change. Writing $\varepsilon_n = \varepsilon_{n,k} (\log z)^k + \cdots + \varepsilon_{n,0}$ with $\varepsilon_{n,k} \neq 0$, we now have

$$[P_{+f,d}(\varepsilon)]_{\mu_d + dn} \;=\; J_{P_{+f,d}}(n)\, \varepsilon_{n,k}^d\, (\log z)^{dk} + \mathcal{O}((\log z)^{dk-1}) \tag{5}$$

instead of (2), and where $\mathcal{O}((\log z)^{dk-1})$ stands for a polynomial of degree at most $d\,k - 1$ in $K[\log z]$. □

The consideration of logarithmic solutions leads to a better bound for the existence part of Proposition 5.

**Proposition 9.** *Let $P \in A\{F\} \setminus A$ and $f \in K[[z]]$. Assume that $S_P(f) \neq 0$ and that $v(P(f)) > 2\,\sigma$, with $\sigma \sqsupset v(P_{+f,1}) + 1$. Then there exists a root $\tilde{f} \in K[\log z][[z]]$ of $P$ with $v(\tilde{f} - f) > \sigma$.*

**Proof.** The proof is analogous to the proof of Proposition 5, with the exception that (3) should be replaced by

$$J_{\mathrm{H}}(\delta + n)\, \varepsilon_n \;=\; \Delta(\varepsilon)_{\mu_1 + n}. \tag{6}$$

For all $n > \sigma$, the right hand side $\Delta(\varepsilon)_{\mu_1+n}$ again only depends on $\varepsilon_0$, ..., $\varepsilon_{n-1}$, but the constant term $L_0$ of the differential operator $L = L_k\, \delta^k + \cdots + L_0 := J_{\mathrm{H}}(\delta + n) \in K[\delta]$ may vanish if $J_H(n) = 0$. Yet, Proposition 1 still implies that the equation $L\,\varepsilon_n = g$ admits a solution in $K[\log z]$ for any $g \in K[\log z]$, which is sufficient for the existence of a solution $\varepsilon$ to the equation $P(f + \varepsilon) = 0$. □

In the proof of the algorithm **ZeroTest**, we only needed the existence of the solution $\tilde{f} \in K[[z]]$ with $Q(\tilde{f}) = 0$ and $v\big(\tilde{f} - f\big) > \sigma$. In view of what precedes, we may thus improve the algorithm as follows:

**Algorithm ZeroTest*($Q$)**
INPUT: $Q \in A\{F\}$
OUTPUT: the result of the test $Q(f) = 0$

1 If $Q \in A$ then return the result of the test $Q = 0$
2 If **ZeroTest***$(I_Q)$ then return **ZeroTest***$(Q - I_Q\, \ell^*_Q)$
3 If **ZeroTest***$(S_Q)$ then return **ZeroTest***$(Q \operatorname{rem} S_Q)$
4 If $P \operatorname{rem} Q \neq 0$ then return **ZeroTest***$(P \operatorname{rem} Q)$
5 Let $\sigma := \max\left(v(P_{+f,1}), Z_{P_{+f,1}}, v(I_Q(f)), v(S_Q(f)), v(Q_{+f,1})\right) + 1$
6 Return the result of the test $v(Q(f)) > 2\,\sigma$

**Remark 10.** Recall from Remark 7 that the zero test from the previous section does not work if $P$ or $Q$ depends on a finite number of parameters $\lambda_1, ..., \lambda_p$ in $K$. One interesting aspect of the improved zero test is that we no longer require any root separation bounds which depend on $Q$, so the zero test still works if $Q$ depends on parameters (when using the technique of dynamic evaluation [3] for examining the finite number of branches which can occur depending on algebraic conditions on the parameters). In fact, the original equation $P$ may also depend on parameters, as long as we have a uniform bound for $Z_{P_{+f,1}}$.

## 3.5 Effective root separation bounds

Assume that we are given an effective power series domain $A$ with an effective zero test over an effective diophantine field $K$. Assume also that we are given an effective D-algebraic power series $f \in \mathbb{K}[[z]]$ and an annihilator $P \in A\{F\} \setminus A$ for $f$. Let us show how the zero test algorithm from the previous section can be used in order to compute $\operatorname{val} P_{+f}$, thereby providing an effective bound for $\sigma_{P,f}$ *via* Proposition 4.

**Algorithm RootSeparationBound($P$, $f$)**
INPUT: a computable D-algebraic series $f$ and $P \in A\{F\} \setminus A$ with $P(f) = 0$
OUTPUT: an upper bound $\sigma$ for $\sigma_{P,f}$.

1 Let $\boldsymbol{i}$ is an index with $(P^{(\boldsymbol{i})}(f))_{v(P_{+f})} \neq 0$
2 Repeat the following
3 Let $d := |\boldsymbol{i}|$ and $\sigma := \max(v(P_{+f,d}), Z_{P_{+f,d}}) + 1$
4 If $d = 1$ then return $\sigma$
5 Let $\boldsymbol{j}$ and $\boldsymbol{k}$ be indices with $\boldsymbol{i} = \boldsymbol{j} + \boldsymbol{k}$, $|\boldsymbol{j}| = d - 1$, $|\boldsymbol{k}| = 1$, and set $Q := P^{(\boldsymbol{j})}$
6 Let $\tau := \max(v(Q_{+f,1}), Z_{Q_{+f,1}}) + 1$
7 If $v(Q(f)) > 2\max(\sigma, \tau)$ then
8 Let $\tilde{f} \in K[[z]]$ be such that $Q(\tilde{f}) = 0$ and $v(\tilde{f} - f) > \max(\sigma, \tau)$
9 If $\mathbf{ZeroTest}_{Q,\tilde{f}}(P^{(\boldsymbol{l})})$ for all $\boldsymbol{l}$ with $|\boldsymbol{l}| < d$ and $P^{(\boldsymbol{l})} \neq 0$, then return $\sigma$
10 Let $\boldsymbol{i}$ be an index with $(P^{(\boldsymbol{i})}_{<d}(f))_{v(P_{<d,+f})} \neq 0$

**Proof.** We first notice that $d$ strictly decreases at every iteration of the main loop, which implies the termination of our algorithm. As a loop invariant, we also notice that $P^{(\boldsymbol{i})}(f) \neq 0$ (whence $P_{+f,d} \neq 0$) whenever we are at line 3, which means that we indeed have an algorithm for the computation of $\sigma \in \mathbb{N}$. If $d = 1$, then the correctness of line 4 follows from Proposition 4. Otherwise, we construct $Q$ such that $Q^{(\boldsymbol{k})}(f) = P^{(\boldsymbol{i})}(f) \neq 0$ and $Q_{+f,1} \neq 0$, whence the computability of $\tau$ at line 6. If $v(Q(f)) > 2 \max(\sigma, \tau)$ at line 7, then Proposition 5 implies the existence and uniqueness of $\tilde{f}$ at line 8, and the relation (3) actually provides us with an algorithm to compute the coefficients of $\tilde{f}$. Moreover $Q$ and $\tilde{f}$ satisfy the assumptions for applying the algorithm $\mathbf{ZeroTest}_{Q,\tilde{f}}$ to $P$ and its derivatives at line 9.

Now if $\operatorname{val} P_{+f} = d$, then in particular $Q(f) = 0$ and $\tilde{f} = f$ by the uniqueness of $\tilde{f}$. Consequently, the zerotests $\mathbf{ZeroTest}_{Q,\tilde{f}}(P^{(\boldsymbol{l})})$ will indeed all succeed at line 9 and we will return a correct bound $\sigma$ by Proposition 4. Conversely, if $\mathbf{ZeroTest}_{Q,\tilde{f}}(P^{(\boldsymbol{l})})$ holds for all $\boldsymbol{l}$ with $|\boldsymbol{l}| < d$ and $P^{(\boldsymbol{l})} \neq 0$, then in particular $P(\tilde{f}) = 0$. Since $v(f - \tilde{f}) > \sigma$, we also have $v(P_{+\tilde{f},d}) = v(P_{+f,d})$ and $Z_{P_{+\tilde{f},d}} = Z_{P_{+f,d}}$, whence $f = \tilde{f}$ by Proposition 4 and $\operatorname{val} P_{+f} = \operatorname{val} P_{+\tilde{f}} = d$. If $\operatorname{val} P_{+f} < d$, then this means that we will reach line 10 and find an index $\boldsymbol{i}$ with $|\boldsymbol{i}| < d$ and $P^{(\boldsymbol{i})}(f) \neq 0$. □

**Remark 11.** In practice, it is better to replace line 9 by a simultaneous zero test as outlined in Remark 6.

## 3.6 Non degenerate annihilators

**Proposition 12.** *There exists an algorithm which, given a computable D-algebraic series $f$ and $P \in A\{F\}$ with $P(f) = 0$, computes an annihilator $\tilde{P} \in A\{F\}$ for $f$ of multiplicity one.*

**Proof.** We may use a variant of the algorithm **RootSeparationBound**. Indeed, it suffices to return $P$ instead of $\sigma$ in step 4, and $Q$ instead of $\sigma$ in step 9. □

**Proposition 13.** *There exists an algorithm which, given a computable D-algebraic series $f$ and $P \in A\{F\}$ with $P(f) = 0$, computes a non degenerate annihilator $\tilde{P} \in A\{F\}$ for $f$.*

**Proof.** Using the previous proposition, we may assume without loss of generality that $P$ has multiplicity one. In particular, we have a zero test for elements in $A\{f\}$. Now let $Q := P$ and keep replacing $Q := S_Q$ as long as $S_Q(f) = 0$. Then we will end up with a $Q$ such that $Q(f) = 0$ and $S_Q(f) \neq 0$. □

We are now in a position to make Proposition 3 effective. We first need a general algorithm for computing algebraic dependencies.

**Proposition 14.** *Let $A$ be an effective integral domain with an effective zero test. There exists an algorithm which takes $r+1$ polynomials $P_0, \ldots, P_r \in A[G_1, \ldots, G_r]$ on input, and which produces a relation $\Phi \in A[F_0, \ldots, F_r]$ with $\Phi(P_0, \ldots, P_r) = 0$.*

**Proof.** Let $d = \max_i \deg P_i$. Given $n \in \mathbb{N}$, the set of power products $\mathcal{P}_n = \{P^i : i \in \mathcal{I}_n\}$ with $\mathcal{I}_n = \{i \in \mathbb{N}^{r+1} : i_0 + \cdots + i_r \,\square\, n\}$ and $P^i = P_0^{i_0} \cdots P_r^{i_r}$ contains at most $\binom{n+r+1}{r+1} \asymp n^{r+1}$ elements. The degree of any polynomial in $\mathcal{P}_n$ is bounded by $n\,d$, and the space of polynomials in $A[G_1, \ldots, G_r]$ of degree $\square d\,r$ has rank $\binom{n\,d+r}{r} \asymp n^r$ as a free $A$-module. Taking $n \in \mathbb{N}$ minimal such that $\binom{n+r+1}{r+1} > \binom{n\,d+r}{r}$, it follows that the set $\mathcal{P}_n$ contains a non trivial $A$-linear dependency $\sum_{i \in \mathcal{I}_n} \lambda_i P^i = 0$, which we may compute using linear algebra. □

If $f$ is a D-algebraic power series with non degenerate annihilator $P \in A\{F\}$ of order $r$, then the $A$-algebra $A\{f\}$ is contained in the $A$-algebra $B = A[f, \ldots, \delta^{r-1} f, S_P(f)^{-1}]$,which is stable under $\delta$.

**Proposition 15.** *The set $A^{\mathrm{dalg}}$ of D-algebraic series over $A$ forms an effective power series domain.*

**Proof.** Let $f_1,\ f_2 \in A^{\mathrm{dalg}}$ be represented by pairs $(f_1,\ P_1)$ and $(f_2, P_2)$ with $P_1(f_1) = P_2(f_2) = 0$. Applying Proposition 13, we may assume without loss of generality that the annihilators $P_1$ and $P_2$ are non degenerate, of orders $r_1$ and $r_2$. Then

$$B \;=\; A[f_1, \ldots, \delta^{r_1-1} f_1, S_{P_1}(f_1)^{-1}, f_2, \ldots, \delta^{r_2-1} f_2, S_{P_2}(f_2)^{-1}]$$

is an effective $A$-algebra which is stable under $\delta$. For $g \in \{f_1 + f_2,\ f_1\, f_2, \delta f_1\} \subseteq B$, we may use Proposition 14 in order to compute an $A$-algebraic relation between $g, \delta g, \ldots, \delta^{r_1+r_2+2} g$. Similarly, assuming that $g = f_1 / f_2 \in B$ with $f_2 \neq 0$, the algebra $B[1/f_2]$ is stable under $\delta$, so we may compute an $A$-algebraic relation between $g, \delta g, \ldots, \delta^{r_1+r_2+3} g$. □

Of course, the algorithm from the proof of Proposition 14 uses brute force for for finding algebraic relations, so any algorithm which relies on this method is deemed to be quite inefficient. In the section 4 below, we will discuss algorithms which avoid relying on Proposition 14 for the computation with D-algebraic series.

# 4 D-domains

In the algorithms from the previous sections, we essentially represent D-algebraic power series by elements of $A\langle f\rangle \cap K[[z]]$, where $f \in K[[z]]$ is a computable root of a differential polynomial $P \in A\{F\} \setminus A$. Since $A\langle f\rangle \cap K[[z]]$ is itself an effective power series domain with an effective zero test, we may also form towers $A\langle f_1\rangle \cdots \langle f_l\rangle$ and represent D-algebraic power series by elements of such towers. This generalization is useful for representing expressions involving $z$, the $K$-algebra operations, and other D-algebraic operations such as $\exp$, $\log$, etc. Indeed, differential polynomials which annihilate such expression can quickly become quite large. In this section, we will introduce an even more convenient representation based on differential algebra, which generalizes the construction of towers and provides more flexibility for representing solutions to implicit equations at the end of section 5.5.

## 4.1 Definition of a D-domain

An *abstract D-domain* over $A$ is a differential algebra $B$ over $A$ of finite transcendence degree $r$ over $A$ together with a differential $A$-algebra morphism $\rho: B \to K[[z]]$ which we will call the *evaluation mapping*. A second abstract D-domain $\tilde{B}$ with evaluation mapping $\tilde{\rho}$ is said to be *equivalent* to $B$ if $\tilde{\rho}$ admits the same image as $\rho$. Assuming that $A$ is an effective power series domain with an effective zero test over an effective diophantine field $K$, we say that $\rho$ is *effective* if $\rho$ is computable and $\rho(P)$ is computable for each $P$; in that case, we also say that $B$ is an effective D-domain.

A *D-domain* is an abstract D-domain $B$ of the form

$$\begin{aligned} B &= A\{F_1, ..., F_k\}/I \\ I &= [P_1, ..., P_k]: (H_{P_1} \cdots H_{P_k})^\infty, \end{aligned}$$

where $P_1, ..., P_k \in A\{F_1, ..., F_k\}$ are such that

$$\rho(H_{P_1} \cdots H_{P_k} + I) \neq 0,$$

and where the leaders of $P_1, ..., P_k$ are $\delta^{r_1} F_1, ..., \delta^{r_k} F_k$ for certain $r_1, ..., r_k \in \mathbb{N}$. It will be convenient to lift the evaluation mapping $\rho$ to $A\{F_1, ..., F_k\}$ using $\rho(Q) = \rho(Q + I)$. Then $\rho$ becomes simply the evaluation mapping at $f = (\rho(F_1), ..., \rho(F_k))$. In particular, $\rho$ is effective as soon as $f$ is a tuple of computable power series. We will call the D-domain $B$ *unmixed* if $P_i \in A\{F_i\}$ for each $i$. We will call the D-domain $B$ *Pfaffian* if $P_i$ is of the form $P_i = S_i\, \delta F_i - R_i$ with $S_i, R_i \in A[F_1, ..., F_k]$ for all $i$.

**Proposition 16.**

*a) Given any D-domain $B$ over $A$ and $P \in B$, the series $\rho(P)$ is D-algebraic over $A$. If $B$ is effective, then we may effectively compute an annihilator for $\rho(P)$.*

*b) Any D-algebraic series $f$ over $A$ is represented by an element of an unmixed D-domain $B$ over $A$. If $A$ is effective and $f \in A^{\mathrm{dalg}}$, then we may effectively compute such a $B$.*

**Proof.** Given a D-algebraic domain $B$ over $A$ and $P \in B$, the sequence $P, \delta P, \delta^2 P, ...$ contains non trivial algebraic dependencies which can be computed using Proposition 14. This proves *a*). Inversely, given $f \in A^{\mathrm{dalg}}$, we may compute a non degenerate annihilator $P \in A\{F\}$ for $f$ using Proposition 13. Then $B = A\{F\}/([P]: H_P^\infty)$ with $\rho(F) = f$ defines an unmixed D-domain in which $F$ represents $f$. □

**Proposition 17.** *Any D-domain $B$ is equivalent to an unmixed D-domain. If $B$ is effective, then this reduction is effective.*

**Proof.** Let $f_1, ..., f_k \in B$ be generators of the $A$-algebra $B$ and let $r$ be the transcendence degree of $B$ over $A$. For each $f_i$, we may compute a non degenerate annihilator $P_i$ for $f_i$ using Proposition 13. Then $\tilde{B} = A\{F_1, ..., F_k\}/([P_1, ..., P_k]: (H_{P_1} \cdots H_{P_k})^\infty)$ with $\rho(F_i) = f_i$ defines an unmixed D-domain which is equivalent to $B$. □

**Proposition 18.** *Any D-domain $B$ is equivalent to a Pfaffian D-domain. If $B$ is effective, then this reduction is effective.*

**Proof.** Let us first show that $B$ is equivalent to a D-domain with orders $r_i = 1$. Modulo the replacement of $P_i$ by $\delta_i P_i$, we may assume without loss of generality that $r_i \sqsupset 1$ and $\deg_{\delta^{r_i} F_i} P_i = 1$ for all $i$. Now consider formal variables $F_{i,j}$ with $1 \sqsupset i \sqsupset k$ and $0 \sqsupset j < r_i$. Let $\mathcal{F} = \{\delta^j F_i : i \sqsupset k, j \sqsupset r_i\}$, $\tilde{\mathcal{F}} = \{F_{i,j} : i \sqsupset k, j < r_i\} \cup \{\delta F_{i,r_i-1} : i \sqsupset k\}$ and consider the $A$-algebra morphism $\phi: A[\mathcal{F}] \to A[\tilde{\mathcal{F}}]$, with $\phi(\delta^j F_i) = F_{i,j}$ for $j < r_i$ and $\phi(\delta^{r_i} F_i) = \delta F_{i,r_i-1}$. Consider the set $\mathcal{P}$ of all polynomials $P_{i,j} \in A[\tilde{\mathcal{F}}]$ with $P_{i,j} = \delta F_{i,j} - F_{i,j+1}$ if $j < r_i$ and $P_{i,r_i} = \phi(P_i)$. Let $\sqsupset$ be the ranking on $\mathcal{V} = \{\delta^j F_i : i \sqsupset k, j \in \mathbb{N}\}$. We define a ranking on $\mathcal{W} = \{\delta^k F_{i,j} : i \sqsupset k, j < r_i, k \in \mathbb{N}\}$ by setting $\delta^k F_{i,j} \sqsupset \delta^{k'} F_{i',j}$ whenever $\delta^{j+k} F_i \prec \delta^{j'+k'} F_{i'}$ or $\delta^{j+k} F_i = \delta^{j'+k'} F_{i'}$ and $k < k'$. Then the D-domain $\tilde{B} = A\{\tilde{\mathcal{F}}\}/\tilde{I}$ with $\tilde{I} = [\mathcal{P}]: H_{\mathcal{P}}^\infty$ is equivalent to $B$.

Assuming that $r_i = 1$ and $\deg_{\delta^{r_i} F_i} P_i = 1$ for all $i$, let us now show that $B$ is equivalent to a Pfaffian D-domain. We may assume that we ordered the variables $F_i$ such that $F_1 \prec \cdots \prec F_k$. In particular, this implies that $P_1 = S_1 \delta F_1 - R_1$ with $S_1, R_1 \in A[F_1, ..., F_k]$. Let us prove by induction over $i$ that we may replace $P_i$ by a differential polynomial of the form $P_i = S_i \delta F_i - R_i$ with $S_i, R_i \in A[F_1, ..., F_k]$. So assume that the induction hypothesis is satisfied for all smaller $i$. We have $P_i = D \delta F_i - N$ with $N, D \in A[F_1, ..., F_k, \delta F_1, ..., \delta F_{i-1}]$. Let $d$ be the maximum of the degrees of $D$ and $N$, and $S_{<i} = S_1 \cdots S_{i-1}$. Then substitution of $R_j/S_j$ for each $\delta F_j$ with $j < i$ in $S_{<i}^d D$ and $S_{<i}^d N$ yields two polynomials $S_i$ and $R_i$ in $A[F_1, ..., F_k]$ such that $S_{<i}^d P_i - (S_i \delta F_i - R_i) \in [P_1, ..., P_{i-1}]$. This means that we may replace $P_i$ by $S_i \delta F_i - R_i$. □

## 4.2 Dominant Hermite normal forms

Before we generalize the zero test algorithms from section 3, we will need a way to asymptotically normalize systems of linear differential equations with power series coefficients. The normalization that we will use is an asymptotic variant of the Hermite normal form.

Let us first consider a square $k \times k$ matrix $M \in K[\delta]^{k \times k}$. We say that $M$ is in *Hermite normal form* if $M$ is upper triangular and there exist integers $1 \sqsupset p_1 < \cdots < p_l \sqsupset k$ such that

- $M_{i,j} = 0$ whenever $i > l$ or $j < p_1$.
- $\deg M_{i',p_i} < \deg M_{i,p_i}$ for all $i' < i \sqsupset l$.

If $M$ has maximal rank $k$, then we must have $p_i = i$ for each $i$. It can be shown that there exists a unique unimodular matrix $U \in K[\delta]^{k \times k}$ such that $UM$ is in Hermite normal form. Moreover, $U^{-1} \in K[\delta]^{k \times k}$ and there is an algorithm for the computation of $U$ if $K$ is an effective field.

Let us now consider a matrix $M \in K[\delta][[z]]^{k \times k}$ of rank $k$. Recall that $P \in K[\delta]$ commutes with $z^i$ following the law $P(\delta)\, z^i = z^i\, P(\delta + i)$. For each $i$ we will denote by $M_i \in K[[z]]^k$ the $i$-th row of $M$ and by

$$D(M_i) = ((z^{-v} M_{i,1})_0, ..., (z^{-v} M_{i,k})_0) \in K^k$$

its "skew dominant coefficient", where

$$v := v(M_i) := \min(v(M_{i,1}), ..., v(M_{i,k})).$$

If $M_i = 0$, then we understand that $D(M_i) = 0$. The matrix $D_{\mathrm{row}}(M)$ with rows $D(M_1), \ldots, D(M_k)$ will be called the row dominant matrix of $M$. We say that $M$ is in *dominant Hermite normal form* if $D_{\mathrm{row}}(M)$ is in Hermite normal form. Any matrix $T \in K[\delta][z, z^{-1}]^{k \times k}$ with an inverse in $K[\delta][z, z^{-1}]^{k \times k}$ and such that $TM$ is in dominant Hermite normal form will be called a *normalization matrix*. We claim that such a matrix always exists. What is more, if the entries of $M$ are computable power series, then we may use the following algorithm to compute $T$.

**Algorithm NormalizationMatrix(*M* )**
INPUT: a matrix $M \in K[\delta][[z]]^{k \times k}$ with computable coefficients and rank $k$
OUTPUT: a normalization matrix in $K[\delta][z, z^{-1}]$ for $M$

1 Let $D := D_{\mathrm{row}}(M)$
2 Let $T \in K[\delta]^{k \times k}$ be such that $TD$ is in Hermite normal form
3 Let $U \in K[\delta][z, z^{-1}]^{k \times k}$ be such that $U_{i,j} = z^{v(M_j)} T_{i,j} z^{-v(M_i)}$
4 If $T$ has rank $k$ then return $U$
5 Otherwise return **NormalizationMatrix**$(UM)\, U$

**Proof.** If $\operatorname{rank} U = k$, then $U$ is a normalization matrix of $M$ by construction. If $\operatorname{rank} U < k$, and assuming that $U'$ is a normalization matrix of $UM$, then $U'U$ is a normalization matrix of $UM$, since $U$ is always invertible. This proves the correctness of the algorithm.

As to its termination, let $r = \operatorname{rank} U$ and let $i_1 < \cdots < i_r$ be minimal such that the matrix with rows $D_{i_1}, \ldots, D_{i_j}$ has rank $j$ for each $j \leqslant r$. We claim that $r$ can only increase and that the $r$-tuple $(i_1, \ldots, i_r)$ can only decrease for the lexicographical ordering, once $r$ stabilizes.

Indeed, let $M' = UM$, $D' = D_{\mathrm{row}}(M')$, $r' = \operatorname{rank} M'$ and let $i'_1 < \cdots < i'_{r'}$ be minimal such that the matrix with rows $D'_{i'_1}, \ldots, D'_{i'_j}$ has rank $j$ for each $j \leqslant r'$. Then the rows $D'_{i'_1}, \ldots, D'_{i'_r}$ are precisely the first $r$ rows of the Hermite normal form $TD$, and therefore form a matrix of rank $r$. This shows that $\operatorname{rank} M' \geqslant r$ and $i'_j \geqslant i_j$ for each $j$.

Having proved our claims, we may assume without loss of generality that $r$ and $(i_1, \ldots, i_r)$ have stabilized. Since the degrees of the polynomials entries of $D_{i_1}$, ..., $D_{i_r}$ can only decrease, we may also assume that $D_{i_1}, \ldots, D_{i_r}$ whence $M_{i_1}, \ldots, M_{i_r}$ have stabilized. Furthermore, we may assume that our rows were ordered in such a way that $i_j = j$ for all $j$. Modulo division of $M_1, \ldots, M_r$ by powers of $z$, we may finally assume that $v(M_1) = \cdots = v(M_r) = 0$. Then $U \in K[\delta][z]$ and $v(M'_j) > v(M_j)$ for all $j > r$. This is repeatedly possible only if $M_j$ lies in the $K[\delta][[z]]$ module spanned by $M_1, \ldots, M_r$ for each $j > r$. Since $M$ has rank $k$, this means that we must have $r = k$, which completes the termination proof. □

## 4.3 Root separation bounds for D-domains

Given an abstract D-domain $B$, we claim that there exists a number $\sigma \in \mathbb{N}$ such that for any alternative evaluation mapping $\tilde{\rho}$ on $B$, we have $\tilde{\rho} = \rho$ whenever $v(\tilde{\rho}(P) - \rho(P)) \geqslant \sigma$ for all $P \in B$. The minimal such number will be called the *root separation* for $B$ and we denote it by $\sigma_B$. Our claim clearly holds when $B = A\{F\}/([P]: H_P^\infty)$ is an unmixed D-domain. Indeed, in this case, we have

$$\sigma_B \geqslant \max\left(\sigma_{P_1, \rho(F_1)}, \ldots, \sigma_{P_k, \rho(F_k)}\right),$$

with the notations from above. The general case reduces to this particular case by applying Proposition 17. However, since the computation of univariate differential polynomials which annihilate given elements of $B$ may be quite expensive, we would like to have a more direct bound. We first need a few preliminaries.

Consider $k$ linear differential polynomials $P_1, ..., P_k \in K[[z]]\{F_1, ..., F_k\}_1$. Any such polynomial can formally be viewed as an element of $K[\delta][[z]]\, F_1 \oplus \cdots \oplus K[\delta][[z]]\, F_k$. Let $M \in K[\delta][[z]]^{k\times k}$ be the matrix with $P_i = M_{i,1}\, F_1 + \cdots + M_{i,k}\, F_k$. Assuming that this matrix has rank $k$ over $K[\delta][[z]]$, we may use the method from section 4.2 to compute a normalization matrix $T \in K[\delta][z, z^{-1}]^{k\times k}$ for $M$. We will call such a $T$ a normalization matrix for $P_1, ..., P_k$. Applying $T$ to the column vector with entries $P_1, ..., P_k$ we obtain a new column vector with "dominant reduced" entries $\tilde{P}_1, ..., \tilde{P}_k$. By construction, the dominant coefficient $\tilde{P}_{i,v(\tilde{P}_i)}$ of $\tilde{P}_i$ is a polynomial of the form

$$\tilde{P}_{i,v(\tilde{P}_i)} = \Theta_{i,i}\, F_i + \cdots + \Theta_{i,k}\, F_k$$

with $\Theta_{i,i}, ..., \Theta_{i,k} \in K[\delta]$. We will denote by $J_{\tilde{P}_i} \in K[N]$ the polynomial with $J_{\tilde{P}_i}(\delta)\, F_i = \Theta_{i,i}$. We also denote by $Z_{\tilde{P}_i}$ the largest root of $J_{\tilde{P}_i}$ in $\mathbb{N}$, or $-1$ if no such root exists.

Now consider a D-domain $B = A\{F\}/([P]: H_P^\infty)$ with evaluation mapping $\rho$. Let $f = (f_1, ..., f_k) = \rho(F) = (\rho(F_1), ..., \rho(F_k))$. Since $H_P(f) \neq 0$, each $P_{i,+f,1}$ is non zero and has the same leader $\delta^{r_i} F_i$ as $P_i$. In particular, the polynomials $P_{i,+f,1}$ are linearly independent over $K(\delta)[[z]]$. Consequently, there exists a normalization matrix $T$ for $P_{+f,1}$, whence $J_{P_{+f,i,1}}$ and $Z_{P_{+f,i,1}}$ are well defined for all $i$.

**Proposition 19.** *Let $B = A\{F\}/([P]: H_P^\infty)$ be a D-domain with evaluation mapping $\rho$ and $f = \rho(F)$. Let $T$ be a normalization matrix for $P_{+f,1}$ and $\tilde{P} = TP$. Then*

$$\sigma_B \;\square\; \max(v(\tilde{P}_{1,1}), ..., v(\tilde{P}_{k,1}), Z_{\tilde{P}_{1,1}}, ..., Z_{\tilde{P}_{k,1}}) + 1.$$

**Proof.** Let $\mu_i := v(\tilde{P}_{i,1})$ for each $i$. Given $\tilde{f} = f + \varepsilon \in K[[z]]^k$ with $n = v(\varepsilon) < \infty$, there exists a largest index $i$ with $v(\varepsilon_i) = n$. We have

$$[\tilde{P}_{i,1}(\varepsilon)]_{\mu_i+n} \;=\; J_{\tilde{P}_{i,1}}(n)\, (\varepsilon_i)_n.$$

Assuming that $n \,\square\, \max(\mu_1, ..., \mu_k, Z_{\tilde{P}_{1,1}}, ..., Z_{\tilde{P}_{k,1}}) + 1$, we also have

$$v(\tilde{P}_{i,>1}(\varepsilon_i)) \;\square\; 2\, n \;>\; \mu_i + n,$$

whence

$$[\tilde{P}_i(\varepsilon_i)]_{\mu_i+n} \;=\; J_{\tilde{P}_{i,1}}(n)\, (\varepsilon_i)_n.$$

Since $n > Z_{\tilde{P}_{i,1}}$, we get $J_{\tilde{P}_{i,1}}(n) \neq 0$, which entails $\tilde{P}_i(\varepsilon_i) \neq 0$, $\tilde{P}(\varepsilon) \neq 0$ and $P_{+f}(\varepsilon) \neq 0$. $\square$

## 4.4 An effective zero test for D-domains

In order to generalize the zero test from section 3.3 to the setting of D-domains, we first need a suitable counterpart of Proposition 5 in addition to Proposition 19.

Assume that we are given a differential ring $B = A\{F\}/([P]: H_P^\infty)$ where $P_1, ..., P_k \in A\{F\} \setminus A$ are such that $\ell_{P_i} = \delta^{r_i} F_i$ for certain $r_1, ..., r_k \in \mathbb{N}$. Given $f \in \mathbb{K}[[z]]^k$ and $n \in \mathbb{N}$, we would like to solve the system of equations $P(f + \varepsilon) = 0$ for $\varepsilon \in K[[z]]^k$ with $v(\varepsilon) > n$. Assuming that $H_{P_i}(f_i) \neq 0$ for each $i$, we may define $T$ and $\tilde{P}$ as in the previous section. Since $T$ is a normalization matrix, there also exists a matrix $U \in K[\delta][z, z^{-1}]^{k\times k}$ with $U\, T = \mathrm{Id}_k$. Then we have $P(f + \varepsilon) = 0 \Rightarrow \tilde{P}(\varepsilon) = T\, P_{+f}(\varepsilon) = 0$ and $\tilde{P}(\varepsilon) = 0 \Rightarrow P(f + \varepsilon) = U\, \tilde{P}(\varepsilon) = 0$. Now consider

$$\sigma_{P_1,...,P_k;\, f_1,...,f_k} := \max(v(\tilde{P}_{1,1}), ..., v(\tilde{P}_{k,1}), Z_{\tilde{P}_{1,1}}, ..., Z_{\tilde{P}_{k,1}}) + 1.$$

We have the following analogue of Proposition 5 for solving the equation $\tilde{P}(\varepsilon) = 0$ for sufficiently small $\varepsilon$.

**Proposition 20.** *With the above notations, if* $\sigma \sqsupset \sigma_{P_1,\ldots,P_k;f_1,\ldots,f_k}$ *and* $v(P(f)) > 2\sigma$*, then there exists a unique* $\tilde{f} \in K[[z]]^k$ *with* $P(\tilde{f}) = 0$ *and* $v(\tilde{f} - f) > \sigma$*.*

**Proof.** By what precedes, it suffices to show that the equation $\tilde{P}(\varepsilon) = 0$ admits a unique solution with $v(\varepsilon) > \sigma$. Let $\mu_i := v(\tilde{P}_{i,1}) < \sigma$ for each $i$. Recall that we may write

$$(\tilde{P}_{i,1})_{\mu_i} = \Theta_{i,i} F_i + \cdots + \Theta_{i,k} F_k$$

for each $i$, with $\Theta_{i,j} \in K[\delta]$. We now decompose each $\tilde{P}_i$ as

$$\begin{aligned} \tilde{P}_i &= \mathrm{H}_i - \Delta_i, \\ \mathrm{H}_i &= \Theta_{i,i} F_i z^{\mu_i}. \end{aligned}$$

Extracting the coefficient of $z^{\mu_i+n}$ in the relation $\mathrm{H}_i(\varepsilon_i) = \Delta(\varepsilon_i)$ now yields

$$J_{\mathrm{H}_i}(n)\,(\varepsilon_i)_n = \Delta_i(\varepsilon)_{\mu_i+n}. \tag{7}$$

For all $n > \sigma$, we have $J_{\mathrm{H}_i}(n) \neq 0$ and $\Delta_i(\varepsilon)_{\mu_i+n}$ only depends on coefficients $(\varepsilon_j)_m$ with $m < n$ and coefficients $(\varepsilon_j)_n$ with $j > i$. Hence (7) provides us with a recurrence relation for the computation of $\varepsilon$. □

**Algorithm ZeroTest($Q$)**
INPUT: $Q \in A\{F\}$
OUTPUT: the result of the test $Q(f) = 0$

1 If $Q \in A$ then return the result of the test $Q = 0$
2 If **ZeroTest**$(I_Q)$ then return **ZeroTest**$(Q - I_Q\, \ell_Q^*)$
3 If **ZeroTest**$(S_Q)$ then return **ZeroTest**$(Q \operatorname{rem} S_Q)$
4 If $P_i \operatorname{rem} Q \neq 0$ for some $i$ then return **ZeroTest**$(P_i \operatorname{rem} Q)$
5 Let $\sigma_1 \in \mathbb{N}$ be an upper bound for $\sigma_B$
6 Let $i$ be such that $\ell_Q = \delta^\alpha F_i$ for some $\alpha \in \mathbb{N}$
7 Let $\sigma_2 := \sigma_{P_1,\ldots,P_{i-1},Q,P_{i+1},\ldots,P_k;f_1,\ldots,f_k}$
8 Return the result of the test $v(Q(f)) > 2\max(\sigma_1, \sigma_2)$

**Proof.** The proof is analogous to the proof of the zero test algorithm from section 3.3. □

## 4.5 An improved zero test for D-domains

The zero test from the previous section may be further improved along similar lines as what we did in section 3.4. Given an abstract D-domain $B$, the *strong root separation* for $B$ is the smallest number $\sigma = \sigma_B^*$ such that for any alternative "evaluation" mapping $\tilde{\rho}: B \to K[\log z][[z]]$, we have $\tilde{\rho} = \rho$ whenever $v(\tilde{\rho}(P) - \rho(P)) \sqsupset \sigma$ for all $P \in B$. The existence of such a number is shown in the same way as before and for D-domains we have the usual explicit bound:

**Proposition 21.** *Let* $B = A\{F\}/([P] : H_P^\infty)$ *be a D-domain with evaluation mapping* $\rho$ *and* $f = \rho(F)$*. Let* $T$ *be a normalization matrix for* $P_{+f,1}$ *and* $\tilde{P} = TP$*. Then*

$$\sigma_B^* \sqsupset \max(v(\tilde{P}_{1,1}), \ldots, v(\tilde{P}_{k,1}), Z_{\tilde{P}_{1,1}}, \ldots, Z_{\tilde{P}_{k,1}}) + 1.$$

**Proof.** The proof is similar to the proof of Proposition 19. This time, $\varepsilon \in K[\log z][[z]]^k$, we again pick $i$ to be the largest index $i$ with $v(\varepsilon_i) = n$, so that we may write $(\varepsilon_i)_n = \varepsilon_{i,n,\ell} \log^\ell z + \cdots + \varepsilon_{i,n,0}$ with $\varepsilon_{i,n,\ell} \neq 0$. In the same way as before, we now get

$$[\tilde{P}_i(\varepsilon_i)]_{\mu_i+n} = J_{\tilde{P}_{i,1}}(n)\, \varepsilon_{i,n,\ell} \log^\ell z + \mathcal{O}(\log^{\ell-1} z).$$

For $n > Z_{\tilde{P}_{i,1}}$, we again get $J_{\tilde{P}_{i,1}}(n) \neq 0$, $\tilde{P}_i(\varepsilon_i) \neq 0$, $\tilde{P}(\varepsilon) \neq 0$ and $P_{+f}(\varepsilon) \neq 0$. □

For the analogue of Proposition 20, we define

$$\sigma^*_{P_1,\ldots,P_k;f_1,\ldots,f_k} := \max(v(\tilde{P}_{1,1}),\ldots,v(\tilde{P}_{k,1})) + 1.$$

**Proposition 22.** *With the above notations, if $\sigma \,\square\, \sigma^*_{P_1,\ldots,P_k;f_1,\ldots,f_k}$ and $v(P(f)) > 2\sigma$, then there exists an $\tilde{f} \in K[\log z][[z]]^k$ with $P(\tilde{f}) = 0$ and $v(\tilde{f} - f) > \sigma$.*

**Proof.** The proof is similar to the proof of Proposition 20, except that (7) should be replaced by

$$(\varepsilon_i)_n = J_{\mathrm{H}_i}(\delta + n)^{-1}\, \Delta_i(\varepsilon)_{\mu_i + n}, \tag{8}$$

where $J_{\mathrm{H}_i}(\delta + n)^{-1}$ is the operator inverse of $J_{\mathrm{H}_i}(\delta + n)$ from Proposition 1. □

In the algorithm **ZeroTest** from the previous section, it is now possible to replace $\sigma_{P_1,\ldots,P_k;f_1,\ldots,f_k}$ by $\sigma^*_{P_1,\ldots,P_k;f_1,\ldots,f_k}$ in the definition of $\sigma_2$.

# 5 Multivariate D-algebraic series

## 5.1 Multivariate power series domains and closure properties

Given a subring $A \subseteq K[[z]] = K[[z_1,\ldots,z_n]]$, we will denote by $A^{\mathrm{fr}}$ the intersection of $K[[z]]$ with the fraction field of $A$. We say that $A \subseteq K[[z]]$ is a *power series domain* if $A$ is a differential ring with respect to the derivations $\delta_i = z_i\,\partial/\partial z_i$ such that $A^{\mathrm{fr}} = A$ and $A$ is stable under the substitutions $\pi_i\colon z_i \mapsto 0$.

A power series domain $A$ is said to be *effective*, if the differential $K$-algebra operations can be carried out by algorithms and for each $i \in \{1,\ldots,n\}$ we have a computable mapping which takes $f \in A$ on input and returns $f$ as a computable power series in $\pi_i(A)[[z_i]]$. In particular, this means that every $f \in A$ can be regarded as an *computable* power series in the sense that there exists an algorithm which takes $i \in \mathbb{N}^n$ on input and returns the coefficient $f_i$ of $z^i = z_1^{i_1} \cdots z_n^{i_n}$ in $f$ on output. We also notice that the quotient field of an effective power series domain is an effective differential field, when representing fractions in the usual way. In particular, $A^{\mathrm{fr}}$ is an effective differential $A$-algebra.

The above definitions can be generalized to countable dimension as follows. We let $K[[z_1, z_2, \ldots]] = K \cup K[[z_1]] \cup K[[z_1, z_2]] \cup \cdots$, where we regard each $K[[z_1,\ldots,z_n]]$ as being naturally included into $K[[z_1,\ldots,z_{n+1}]]$. A subset $A \subseteq K[[z_1, z_2, \ldots]]$ is said to be a *power series domain* if $A_n := A \cap K[[z_1,\ldots,z_n]]$ is a power series domain for each $n$. We say that $A$ is *effective* if each $A_n$ is and if we have an algorithm for computing an upper bound for the dimension $n$ of any given series $f \in A$.

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

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 $A \subseteq K[[z_1, z_2, ...]]$ *satisfies the implicit function theorem* if $\psi_1, ..., \psi_m \in A$ for the above solution of $\varphi \circ \psi = 0$, whenever $\varphi_1, ..., \varphi_m \in A_n$. We say that $A$ *effectively satisfies the implicit function theorem* if we also have an algorithm to compute $\psi_1, ..., \psi_m$ as a function of $\varphi_1, ..., \varphi_m$.

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

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

A power series domain $A \subseteq K[[z_1, ..., z_n]]$ is said to be *stable under monomial transformations* if for any $f \in A$ and invertible matrix $M \in \mathbb{Q}^{n \times n}$ with $M \cdot \operatorname{supp} f \subseteq \mathbb{N}^n$, we have $f \circ z^M \in A$. We say that $A$ is *effectively stable under 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 $M \cdot \operatorname{supp} f \not\subseteq \mathbb{N}^n$).

Given an effective power series domain which effectively satisfies each of the above closure properties (composition, implicit functions, and monomial transformations), it can be shown that an effective version of the Weierstrass preparation theorem holds. We refer to [11] for details.

## 5.2 Multivariate D-algebraic power series

Let $A \subseteq K[[z]] = K[[z_1, ..., z_n]]$ be a multivariate power series domain. Given a power series $f \in K[[z]] = K[[z_1, ..., z_n]]$ and $i \in \{1, ..., n\}$, we may consider $f$ as a power series

$$f \;=\; [z_i^0]\, f + ([z_i^1]\, f)\, z_i + ([z_i^2]\, f)\, z_i^2 + \cdots$$

in $z_i$ with coefficients in $\pi_i(K[[z]])$, and also as a power series in $z_i$ with coefficients in the fraction field of $\pi_i(K[[z]])$. If $f$ is D-algebraic over $A$ for this latter interpretation of $f$, then we say that $f$ is D-algebraic in $z_i$ (or with respect to $\delta_i$). We say that $f$ is D-algebraic over $A$ if $f$ is D-algebraic in each of the variables $z_1, ..., z_n$.

**Proposition 23.** *Given $f \in K[[z]]$ is D-algebraic over $A$ and $i \in \{1, ..., n\}$, each coefficient $[z_i^k]\, f$ of the power series expansion of $f$ in $z_i$ is D-algebraic over $\pi_i(A)$.*

**Proof.** Given $j \neq i$, let $P_j(f) = 0$ be a non trivial differential equation satisfied by $f$ in $\delta_j$. Let $v_i(P_j)$ denote the valuation of $P_j$ in $z_i$. Modulo division of $P_j$ by $z_i^{v_i(P_j)}$, we may assume without loss of generality that $v_i(P_j) = 0$. Now $\pi_i(f)$ satisfies the non trivial equation $\pi_i(P_j)(\pi_i(f)) = 0$. This shows that $[z_i^0]\, f$ is D-algebraic over $\pi_i(A)$.

For $k > 0$, we will prove by induction that $[z_i^k]\, f$ is D-algebraic over $\pi_i(A)$. So assume that $[z_i^0]\, f, \ldots, [z_i^{k-1}]\, f$ are D-algebraic over $\pi_i(A)$, whence over $A$. Given $j \neq i$, the series

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

is D-algebraic in $\delta_j$ over $A$, by Proposition 3. By what precedes, it follows that $[z_i^k]\, f = \pi_i(g)$ is D-algebraic in $\delta_j$. □

**Proposition 24.** *The set $A^{\mathrm{dalg}}$ of D-algebraic power series over $A$ forms a multivariate power series domain.*

**Proof.** The stability of $A^{\mathrm{dalg}}$ under the differential ring operations and division (when defined) directly follows from Proposition 3. The stability under the projections $\pi_i$ follows from Proposition 23. □

From now on, $A\{F\}$ denotes the set of differential polynomials with respect to the pairwise commuting derivations $\delta_1, \ldots, \delta_n$. Proposition 2 also admits a natural generalization:

**Proposition 25.** *The series $f \in K[[z]]$ is D-algebraic if and only if $A\{f\}$ admits finite transcendence degree over $A$.*

**Proof.** Assuming that $f \in K[[z]]$ is D-algebraic over $A$, let $P_i \in A[F, \delta_i F, \delta_i^2 F, \ldots] \setminus A$ be of minimal Ritt rank $(\delta_i^r F, d_i)$ with $P_i(f) = 0$, for each $i$. Let $\mathcal{F} = \left\{\delta_1^{i_1} \cdots \delta_n^{i_n} f : i_1 < r_1, \ldots, i_n < r_n\right\}$. Then $S_{P_i}(f) \neq 0$ for each $i$ and $B = A[\mathcal{F}, S_{P_1}(f)^{-1}, \ldots, S_{P_n}(f)^{-1}]$ is stable under the derivations $\delta_1, \ldots, \delta_n$. Consequently, $A\{f\} \cong B$ and $\mathrm{trdeg}_A\, A\{f\} \leqslant r_1 \cdots r_n + n$. Conversely, assume that $\mathrm{trdeg}_A\, A\{f\} = r$. Then $f, \ldots, \delta_i^r f$ satisfy a non trivial algebraic relation for each $i$, whence $f$ is D-algebraic. □

Assume now that $A$ is an effective multivariate power series domain. We may effectively represent a D-algebraic series $\varphi \in A^{\mathrm{dalg}}$ over $A$ by a tuple $(f, P_1, \ldots, P_n)$ where $f$ is a computable power series in $K[[z]]$ and $P_i$ an annihilator for $f$ with respect to $\delta_i$, for each $i$.

**Proposition 26.** *Assume that $A \subseteq K[[z]] = K[[z_1, \ldots, z_n]]$ is an effective multivariate power series domain over an effective diophantine field $K$ with an effective zero test. Then $A^{\mathrm{dalg}}$ is an effective multivariate power series domain with an effective zero test. Moreover, for any $i \in \{1, \ldots, n\}$, there exists an algorithm for computing the coefficients $[z_i^k]\, f$ of the power series expansion of a given $f \in A^{\mathrm{dalg}}$ with respect to $z_i$.*

**Proof.** We prove the proposition by induction over $n$. For $n = 0$, the result is trivial, so assume that $n > 0$ and that we proved the result for all smaller $n$.

Given $i \in \{1, \ldots, n\}$, let us first show how to compute the coefficients $[z_i^k]\, f$ of the power series expansion of a given $f \in A$ with respect to $z_i$. The induction hypothesis provides us with a zero test in $\pi_i(A^{\mathrm{dalg}}) = \pi_i(A)^{\mathrm{dalg}}$. In the proof of Proposition 23, we thus have an algorithm for the computation of the valuation $v_i(P_j)$, and the remainder of this proof is constructive.

Let $L$ denote the quotient field of $\pi_n(A^{\mathrm{dalg}}) = \pi_n(A)^{\mathrm{dalg}}$. We claim that $L$ is an effective diophantine field. Indeed, given a polynomial $H \in L[\Lambda]$, an integer $\lambda \in \mathbb{N}$ is a root of $H$ if and only if $\lambda$ is a root of $H$ multiplied by the denominators of its coefficients. Without loss of generality, we may therefore assume that $H \in \pi_n(A^{\mathrm{dalg}})[\Lambda]$. After this reduction, $\lambda \in \mathbb{N}$ is a root of $H$ if and only if $\lambda$ is a root of the coefficient $[z_1^{i_1} \cdots z_{n-1}^{i_{n-1}}]\, P \in K[\Lambda]$ of $z_1^{i_1} \cdots z_{n-1}^{i_{n-1}}$ in $P$ for all $i_1, \ldots, i_{n-1} \in \mathbb{N}$. Let $i_1, \ldots, i_{n-1} \in \mathbb{N}$ be such that this coefficient $Q$ is non zero and let $\sigma$ be its largest root in $\mathbb{N}$ (or $-1$ if no such root exists). We may now check whether $H(k) = 0$ for $k = 0, \ldots, \sigma$ and compute the largest root of $H$ in $\mathbb{N}$.

Any series $f$ in $A^{\mathrm{dalg}}$ may be regarded as a univariate series in $z_n$ with coefficients in $L$. By what precedes, $L$ is an effective diophantine field and we have an algorithm for the computation of the coefficients of $f$. The zero tests from section 3 can therefore be used as zero tests for $f$. □

## 5.3 Multivariate D-domains

Let $A \subseteq K[[z]] = K[[z_1, \ldots, z_n]]$ be a multivariate power series domain. An abstract multivariate D-domain over $A$ is a differential $A$-algebra $B$ for $\delta_1, \ldots, \delta_n$ together with a differential $A$-algebra morphism $\rho\colon B \to K[[z]]$. A *multivariate D-domain* over $A$ is an abstract multivariate D-domain $B$ over $A$ of the form

$$\begin{aligned} B &= A\{F_1, \ldots, F_k\}/I \\ I &= [P_{1,1}, \ldots, P_{1,k}, \ldots, P_{n,1}, \ldots, P_{n,k}]\colon (H_{P_{1,1}} \cdots H_{P_{1,k}} \cdots H_{P_{n,1}} \cdots H_{P_{n,k}})^\infty, \end{aligned}$$

where $P_{1,1}, \ldots, P_{1,k}, \ldots, P_{n,1}, \ldots, P_{n,k} \in A\{F_1, \ldots, F_k\}$ are such that

$$\rho(H_{P_{1,1}} \cdots H_{P_{1,k}} \cdots H_{P_{n,1}} \cdots H_{P_{n,k}} + I) \neq 0,$$

and where each $P_{i,j}$ only involves derivations of the form $\delta_i$ and admits a leader of the form $\delta_i^{r_{i,j}} F_j$ for certain $r_{i,j} \in \mathbb{N}$. We will denote by $B^{\mathrm{fr}}$ those elements $P/Q$ of the fraction field of $B$ such that $\rho(P/Q) := \rho(P)/\rho(Q) \in K[[z]]$. We will also write $\rho(P) = \rho(P + I)$ for $P \in A\{F_1, \ldots, F_k\}$. We say that $B$ is *effective* if $A$ is an effective power series domain and $\rho(P)$ is computable for each $P \in B$. We say that $B$ is *unmixed* if $P_{i,j} \in A[F_j, \delta_i F_j, \delta_i^2 F_j, \ldots]$ for all $i$ and $j$. We say that $B$ is *Pfaffian* if $P_{i,j}$ is of the form $P_{i,j} = S_{i,j}\, \delta_i F_j - R_{i,j}$ with $S_{i,j}, R_{i,j} \in A[F_1, \ldots, F_k]$ for all $i, j$.

The proof of the following proposition is analogous to the proof of Proposition 16:

**Proposition 27.**

*a) Given any multivariate D-domain $B$ over $A$ and any $P \in B$, the series $\rho(P)$ is D-algebraic over $A$. If $B$ is effective, then we may effectively compute $\rho(P) \in A^{\mathrm{dalg}}$.*

*b) Any multivariate D-algebraic series $f$ over $A$ is the element of a multivariate D-domain $B$ over $A$. If $A$ is effective and $f \in A^{\mathrm{dalg}}$, then we may effectively compute $B$.* □

**Corollary 28.** *Let $B$ be an effective multivariate D-domain over $A \subseteq K[[z_1, \ldots, z_n]]$. Then there exists an algorithm for testing whether $\rho(P) = 0$, for given $P \in B$.*

**Proof.** This follows from Proposition 27 and the existence of a zero test in $A^{\mathrm{dalg}}$ (Proposition 26). □

The proofs of the following propositions are analogous to the proofs of Propositions 17 and 18:

**Proposition 29.** *Any multivariate D-domain $B$ is equivalent to an unmixed D-domain. If $B$ is effective, then this reduction is effective.* □

**Proposition 30.** *Any multivariate D-domain $B$ is equivalent to a Pfaffian D-domain. If $B$ is effective, then this reduction is effective.* □

Consider $P, Q \in A\{F_1, ..., F_k\}$ with $\ell_P = \delta^p F_j$ and $\ell_Q = \delta^q F_j$. Let $m \in \mathbb{N}^n$ be such that $m_i = \max(p_i, q_i)$ for all $i \in \{1, ..., n\}$ and assume that $m \notin \{p, q\}$. Then we recall from differential algebra [17, 14] that the $\Delta$-polynomial $\Delta_{P,Q}$ of $P$ and $Q$ is defined by

$$\Delta_{P,Q} \;=\; S_Q\, \delta^{m-p} P - S_P \delta^{m-q} Q.$$

Given a D-domain $B$ as above, we say that $B$ is *coherent* if $\Delta_{P_{i,j}, P_{i',j}} \in I$ for all $i, i', j$. Given an arbitrary effective D-domain $B$, we may compute an equivalent effective coherent D-domain using the algorithm below, where we make use of the effective zero test from Corollary 28:

**Algorithm MakeCoherent($B$)**
INPUT: An effective multivariate D-domain $B$
OUTPUT: A coherent effective multivariate D-domain which is equivalent to $B$

1 Let $\mathcal{P} := \{P_{i,j} : 1 \leqslant i \leqslant n, j \leqslant 1 \leqslant k\}$
2 Repeat the following
3  Let $\mathcal{P}^* := \{P \in \mathcal{P} : \rho(P) \neq 0, \rho(H_P) \neq 0\}$
4  If there exists $P \in \mathcal{P}$ with $P \operatorname{rem} \mathcal{P}^* \setminus \{P\} = 0$, then set $\mathcal{P} := \mathcal{P} \setminus \{P\}$
5  Else if $\exists\ P \in \mathcal{P}$ with $R := P \operatorname{rem} \mathcal{P}^* \setminus \{P\} \neq P$ and $R \notin \mathcal{P}$, then set $P := \mathcal{P} \cup \{R\}$
6  Else if $\exists\ P, Q \in \mathcal{P}$ with $R := \Delta_{P,Q} \operatorname{rem} \mathcal{P}^* \neq 0$ and $R \notin \mathcal{P}$, then set $\mathcal{P} := \mathcal{P} \cup \{R\}$
7  Else if $\exists\ P \in \mathcal{P}$ with $\rho(I_P) = 0$ and $I_P \notin \mathcal{P}$, then set $\mathcal{P} := \mathcal{P} \cup \{I_P\}$
8  Else if $\exists\ P \in \mathcal{P}$ with $\rho(S_P) = 0$ and $S_P \notin \mathcal{P}$, then set $\mathcal{P} := \mathcal{P} \cup \{S_P\}$
9  Else return $A\{F_1, ..., F_k\}/([\mathcal{P}] : H_{\mathcal{P}}^{\infty})$ with the evaluation induced by $\rho$

**Proof.** The main loop invariant states that $\mathcal{P}$ only contains annihilators for the point $\rho(F) = (\rho(F_1), ..., \rho(F_k))$, and each of the original differential polynomials $P_{i,j}$ Ritt reduces to zero with respect to $\mathcal{P}^*$. The termination follows from the fact that we only add new elements of smaller and smaller Ritt ranks to $\mathcal{P}$. At the end, the set $\mathcal{P}$ is necessarily coherent and autoreduced, and such that $\rho(H_{\mathcal{P}}) \neq 0$. Since each original polynomial $P_{i,j}$ reduces to zero modulo $\mathcal{P}^* = \mathcal{P}$, there must exist a corresponding polynomial $Q_{i,j} \in \mathcal{P}$ with leader $\delta_i^{s_i} F_j$ and $s_i \leqslant r_i$. This shows that $A\{F_1, ..., F_k\}/([\mathcal{P}] : H_{\mathcal{P}}^{\infty})$ is indeed a D-domain. □

## 5.4 Extraction of coefficients and application to zero testing

By Proposition 26, there exists an algorithm for extracting the coefficients of multivariate D-algebraic power series with respect to a single variable $z_i$. In the case of power series which are represented by elements of a D-domain $B$, it would be nice to have a more efficient and systematic algorithm. In particular, given $i \in \{1, ..., n\}$ and $l \in \mathbb{N}$, we would like to effectively construct a D-domain $B_{\leqslant l}$ such that for any $P \in B$ and any $m \leqslant l$, we can produce a $Q = [z_i^m]\, P \in B_{\leqslant l}^{\mathrm{fr}}$ with $[z_i^m]\, \rho(P) = \rho(Q)$. For this, it suffices that $B_{\leqslant l}^{\mathrm{fr}}$ contains all coefficients of the form $[z_i^m]\, F_j$ with $j \in \{1, ..., k\}$ and $m \leqslant l$.

Theoretically speaking, we may construct $B_{\leqslant l}$ using Proposition 26. As a first optimization, we claim that there exists a computable finite set $\mathcal{L} \subseteq \mathbb{N}$ such that we can take $B_{\leqslant l} = B_{<l} := B_{\leqslant l-1}$ whenever $l \notin \mathcal{L}$. Indeed, for any $f \in \rho(B)$, we may regard $f$ as a power series in $z_i$ with coefficients in the quotient field of $\pi_i(K[[z]])$. For sufficiently large $l$, the coefficients of this power series are determined by a recurrence relation of type (3).

As a second optimization, assume that $B$ is Pfaffian and *regular in* $z_i$, meaning that the valuations $v_i(\rho(S_{P_{i,j}}))$ of the $\rho(S_{P_{i,j}})$ in $z_i$ all vanish. We will take

$$B_{\leqslant l} = B_{<l}\big\{[z_i^l]\, F_1, \ldots, [z_i^l]\, F_k\big\}/I_l,$$

with $\rho\big([z_i^l]\, F_j\big) = [z_i^l]\, \rho(F_j)$ for all $j$, and where the differential ideal $I_l$ is constructed as follows. Given $i' \neq i$ and $j \in \{1, \ldots, k\}$, let

$$\mathcal{F}_{i',j,l} = \{[z_i^m]\, F_{j'} \colon m \sqsubset l, 1 \sqsubset j' \sqsubset k\} \cup \{\delta_{i'}([z_i^m]\, F_j) \colon m < l\}.$$

Since $v_i(\rho(S_{i',j})) = 0$, extracting the coefficient of $z_i^l$ in the equation

$$\rho(S_{i',j})\, \rho(\delta_{i'} F_j) \;=\; \rho(R_{i',j})$$

yields a relation

$$([z_i^0]\, \rho(S_{i',j}))\, ([z_i^l]\, \rho(\delta_{i'} F_j)) \;=\; R_{i',j,l},$$

for some $R_{i',j,l} \in A[\mathcal{F}_{i',j,l}]$. Now let $\mathcal{P}_l$ be the set of all differential polynomials of the form $P_{i',j,l} = ([z_i^0]\, S_{i',j})\, \delta_{i'}([z_i^l]\, F_j) - R_{i',j,l}$. Then we may take $I_l = A\{\mathcal{P}_l\}/([\mathcal{P}_l] \colon H_{P_l}^\infty)$. Notice that $B_{\leqslant l}$ is again Pfaffian if $B_{<l}$ is Pfaffian. However, regularity in the other variables $z_{i'}$ is not necessarily preserved. Nevertheless, if $\rho(S_{P_{i,j}}(0)) \neq 0$ for all $i, j$, then the recursive extraction of coefficients only yields regular Pfaffian D-domains.

**Remark 31.** Given a regular D-domain in $z_i$, it can be shown that the reduction to an equivalent Pfaffian D-domain used in the proof of Proposition 30 actually yields a regular Pfaffian D-domain in $z_i$.

From what precedes, it follows in particular that there exists a constant $L \in \mathbb{N}$ such that we may take $B_{\leqslant l}^{\mathrm{fr}} = B_{\leqslant L}^{\mathrm{fr}}$ for all $l \sqsubset L$. Hence for any $P \in B$ and any $m \in \mathbb{N}$, we have $[z_i^m]\, P \in B_{\leqslant L}^{\mathrm{fr}}$. We may then reinterpret the D-domain $B$ as a univariate D-domain by only retaining the relations $P_{i,1}, \ldots, P_{i,k}$ and using coefficients of the form $\rho(Q) \in \pi_i(\rho(B))^{\mathrm{fr}}$ with $Q \in B_{\leqslant L}^{\mathrm{fr}}$. This allows us to replace the theoretical zero test from Corollary 28 by one of the more efficient zero tests from section 4.

## 5.5 An effective implicit function theorem

Let $\varphi_1, \ldots, \varphi_m \in K[[z]] = K[[z_1, \ldots, z_n]]$ with $m < n$ and denote

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

Let $\Phi_1$ be the submatrix spanned by the first $m$ columns of $\Phi$ and $\Phi_2$ the submatrix spanned by the last $p = n - m$ columns. Assume that $\Phi(0) \in K^{m \times m}$ is invertible. Then the implicit function theorem implies that there exist unique power series $\psi_1, \ldots, \psi_m \in K[[u_1, \ldots, u_p]]$, such that the completed vector $\psi = (\psi_1, \ldots, \psi_n)$ with $\psi_{m+1} = u_1, \ldots, \psi_n = u_p$ satisfies

$$\varphi \circ \psi = 0. \tag{9}$$

Forming the Jacobian matrix $\Psi = \partial\psi/\partial u$ of $\psi$, we let $\Psi_1$ and $\Psi_2$ denote the submatrices spanned by the first $m$ resp. last $p$ rows. Differentiating the relation (9), we obtain

$$(\Phi_1 \circ \psi)\, \Psi_1 + (\Phi_2 \circ \psi)\, \Psi_2 \;=\; 0.$$

Since $\Psi_2 = \mathrm{Id}_p$, this yields

$$\Psi_1 \;=\; (-\Phi_1^{-1}\,\Phi_2)\circ\psi.$$

Given any $f \in K[[z]]$, consider the row matrices $F_1 = (\partial f/\partial z_1, ..., \partial f/\partial z_m)$ and $F_2 = (\partial f/\partial z_{m+1}, ..., \partial f/\partial z_n)$. Then

$$\begin{aligned}\frac{\partial f\circ\psi}{\partial u} &= (F_1\circ\psi)\,\Psi_1 + (F_2\circ\psi)\\ &= \big(F_2 - F_1\,\Phi_1^{-1}\,\Phi_2\big)\circ\psi.\end{aligned}$$

Let $\Delta_1 = (\delta_1, ..., \delta_m)$, $\Delta_2 = (\delta_{m+1}, ..., \delta_n)$ and $\Upsilon = (u_1\,\partial/\partial u_1, ..., u_p\,\partial/\partial u_p)$. Let $Z_1$ and $Z_2$ diagonal matrices with entries $z_1, ..., z_m$ resp. $z_{m+1}, ..., z_n$. Denoting by $\tilde\Delta = (\tilde\delta_1, ..., \tilde\delta_p)$ the row vector of derivations with

$$\tilde\Delta\, f \;=\; \Delta_2\, f - \Delta_1\, f\, Z_1^{-1}\,\Phi_1^{-1}\,\Phi_2\, Z_2,$$

the above relation implies

$$\Upsilon(f\circ\psi) \;=\; (\tilde\Delta\, f)\circ\psi.$$

Notice that $z_1\cdots z_m \det\Phi_1\,\tilde\Delta$ maps power series to row vectors of power series.

Assume now that $\varphi_1, ..., \varphi_m \in B$ for some effective multivariate D-domain $B$ of dimension $n$ over $A = K$ with

$$\begin{aligned}B &= K\{F_1, ..., F_k\}/I\\ I &= [P_{i,j}: i, j]: (\textstyle\prod_{i,j} H_{P_{i,j}})^\infty.\end{aligned}$$

Assume also that the coordinate functions $z_1$, ..., $z_m$ are among the $F_i$. We will make the additional assumption that $z_i\circ\psi \neq 0$ for all $i \in \{1, ..., m\}$. In particular, setting $U = z_1\cdots z_m \det\Phi$, we have $U\circ\psi \neq 0$. We introduce a new evaluation mapping $\tilde\rho$ on $B$ by taking

$$\tilde\rho(F_i) \;=\; \rho(F_i)\circ\psi. \tag{10}$$

We may formally extend $\tilde\rho$ into an evaluation from $B[U^{-1}]$ into $K[[u]][(U\circ\psi)^{-1}]$. This evaluation is not compatible with the original derivations $\delta_1, ..., \delta_n$, but we do have

$$u_i\,\frac{\partial\,\tilde\rho(P)}{\partial u_i} \;=\; \tilde\rho(\tilde\delta_i\, P)$$

for all $P \in B[U^{-1}]$, and for each of the derivations $\tilde\delta_i$. Since $B[U^{-1}]$ is finite dimensional as a $K$-algebra, Proposition 14 implies that $F_j, \tilde\delta_i\, F_j, (\tilde\delta_i)^2\, F_j, ...$ satisfy a computable non trivial $K$-algebraic relation $\tilde P_{i,j}$ for each $i$ and $j$. Using Proposition 13, we may assume without loss of generality that these relations are non degenerate. We now define a new multivariate D-domain $\tilde B$ for the derivations $\tilde\delta_1, ..., \tilde\delta_p$, by taking

$$\begin{aligned}\tilde B &= K\{F_1, ..., F_k\}/\tilde I\\ \tilde I &= [\tilde P_{i,j}: i, j]: (\textstyle\prod_{i,j} H_{\tilde P_{i,j}})^\infty,\end{aligned}$$

and taking the evaluation mapping $\tilde\rho$ as in (10). By construction, $\tilde\rho(z_i) = \psi_i$ for each $i \in \{1, ..., m\}$, so $\psi_i$ is D-algebraic.

The additional assumption that $\psi_i = z_i\circ\psi \neq 0$ for all $i \in \{1, ..., m\}$ is quite benign. Indeed, for any index $i$ with $\psi_i = 0$, postcomposition of $f \in K[[z]]$ with $\psi$ means in particular sending $z_i$ to 0. This can also be achieved by extracting the coefficient of $z_i^0$ in $f$. Consequently, modulo a finite number of extraction of coefficients, we may assume without loss of generality that $\psi_i \neq 0$ for all $i \in \{1, ..., m\}$. We have proved:

**Proposition 32.** *The set of D-algebraic power series over an effective diophantine field $K$ is effectively satisfies the implicit function theorem.*

**Proposition 33.** *The set of D-algebraic power series over an effective diophantine field $K$ is effectively stable under composition.*

**Proof.** Given $f \in K[[z_1, ..., z_n]]$ and $g_1, ..., g_n \in K[[u_1, ..., u_p]]$ with $g_1(0) = \cdots = g_n(0) = 0$, consider the power series $\varphi_i = z_i - g_i \in K[[z_1, ..., z_n, u_1, ..., u_p]]$. The above algorithm allows us to compute $\psi_1, ..., \psi_{n+p} \in K[[u_1, ..., u_p]]$ with $\psi_{n+i} = u_i$ and $\varphi \circ \psi = 0$, as well as the result of the composition $f \circ \psi$ (when considering $f$ as an element of $K[[z_1, ..., z_n, u_1, ..., u_p]]$), which coincides with $f \circ g$. □

The construction of $\tilde{B}$ is somewhat unsatisfactory since the computation of individual $K$-algebraic relations $\tilde{P}_{i,j}$ using Proposition 14 is usually quite expensive. In the frequent situation that $H_{P_{i,j}} \circ \psi \neq 0$ for all $i, j$, we may use the following more efficient technique. Using Proposition 30, we may assume without loss of generality that the original relations $P_{i,j}$ are of the form $P_{i,j} = S_{i,j}\, \delta_i\, F_j - R_{i,j}$ with $S_{i,j}, R_{i,j} \in K[F_1, ..., F_k]$. By assumption, we have $\rho(S_{i,j}) \circ \psi \neq 0$ for all $i, j$. With the above notations, let $\Xi$ denote the horizontal concatenation of the matrices $\mathrm{Id}_p$ and $-Z_1^{-1}\, \Phi_1^{-1}\, \Phi_2\, Z_2$, so that $\tilde{\Delta}\, f = (\Delta\, f)\, \Xi$ for all $f$ and $U\, \Xi$ has coefficients in $B$. Modulo the relations $P_{i,j}$, we may then write

$$\tilde{\delta}_i\, F_j = \sum_{i'} (\delta_{i'}\, F)\, \Xi_{i',i} = \sum_{i'} \Xi_{i',i}\, \frac{R_{i,j}}{S_{i,j}}.$$

For each $i$ and $j$, this means that there exists a power product $\tilde{S}_{i,j}$ of the $S_{i',j'}$ and a polynomial $\tilde{R}_{i,j} \in K[F_1, ..., F_k]$ with

$$U\, \tilde{S}_{i,j}\, \tilde{\delta}_{i,j}\, F_j \;=\; \tilde{R}_{i,j}.$$

This allows us to take $\tilde{P}_{i,j} = U\, \tilde{S}_{i,j}\, \tilde{\delta}_{i,j}\, F_j - \tilde{R}_{i,j}$ in the construction of the multivariate D-domain $\tilde{B}$ instead of the relation found using Proposition 14.

## 5.6 Effective monomial transformations

**Proposition 34.** *Let $A \subseteq K[[z_1, ..., z_n]]$ be an effective power series domain over an effective diophantine field $K$. Then $A^{\mathrm{dalg}}$ is effectively stable under monomial transformations.*

**Proof.** Let $B$ be an effective D-domain over $A$, let $P \in B$ and $f = \rho(P)$. Given an invertible matrix $M \in \mathbb{Q}^{n \times n}$ with $M \cdot \mathrm{supp}\, f \subseteq \mathbb{N}^n$, we have to show how to compute $f \circ z^M$. Given a row vector $\lambda \in \mathbb{Q}^n$, we will denote $\lambda \cdot \delta = \lambda_1\, \delta_1 + \cdots + \lambda_n\, \delta_n$. Then for any power series $\varphi \in K[[z]]$ and any $\lambda \in \mathbb{Q}^n$, we notice that

$$(\lambda \cdot \delta)(\varphi \circ z^M) \;=\; ((\lambda\, M) \cdot \delta)(\varphi) \circ z^M.$$

Since $\mathrm{trdeg}_A\, B \,\square\, s := r_1 \cdots r_n + n$, the elements $P, ((\lambda\, M) \cdot \delta)(P), ..., ((\lambda\, M) \cdot \delta)^s(P)$ satisfy an $A$-algebraic dependency which can be computed using Proposition 14. Applying this result for all $\lambda$ of the form $\lambda = e_i = \big(0, \overset{(i-1)\times}{...}, 0, 1, 0, ..., 0\big)$, we obtain D-algebraic relations over $A$ for $\varphi \circ z^M$ in the individual derivations $\delta_i$. □

The above proposition could in principle be used for computing with monomial transforms of elements in an effective D-domain $B$. However, in a similar way as it is more efficient to keep fractions in their symbolic forms when computing with fractions in $B^{\mathrm{fr}}$, it is often more efficient to keep monomial transforms in their symbolic form $f \circ z^M$ when computing with them.

More precisely, we first notice that monomial transformations $f \mapsto f \circ z^M$ with $M \in \mathbb{N}^n$ are somewhat easier, since they can be computed using our algorithms for composition. Now two monomial transformations $f \mapsto f \circ z^{M_1}$ and $f \mapsto f \circ z^{M_2}$ are said to be *compatible* if there exist invertible matrices $N_1, N_2 \in \mathbb{N}^{n \times n}$ with $M_1 N_1^{-1} = M_2 N_2^{-1}$. Given $f_1, f_2 \in \rho(B)$ with $M_1 \cdot \operatorname{supp} f_1 \subseteq \mathbb{N}^n$ and $M_2 \cdot \operatorname{supp} f_2 \subseteq \mathbb{N}^n$, let $g_1 = f_1 \circ z^{N_1}$, $g_2 = f_2 \circ z^{N_2}$ and $P = M_1 N_1^{-1}$. Since $N_1$ and $N_2$ have coefficients in $\mathbb{N}$, we may construct a D-domain $B'$ with $g_1, g_2 \in \rho(B')$. Now $f_1 \circ z^{M_1} = g_1 \circ z^P$ and $f_2 \circ z^{M_2} = g_2 \circ z^P$. In particular, any $\varphi \in K\{f_1, f_2\}$ can be represented by $\varphi = \psi \circ z^P$ for some $\psi \in \rho(B')$.

From the geometrical point of view, the notion of compatibility can be interpreted as follows. Let $\Sigma$ be an open subset of $\{\lambda \in (\mathbb{R}^{\geqslant})^n \setminus \{0\} : |\lambda| = 1\}$ and $\Omega = \mathbb{R}^{\geqslant} \Sigma$. Let $K[[z_1, \ldots, z_n]]_\Omega$ be the subset of $K[[z_1, \ldots, z_n]]$ of series $f$ with $\operatorname{supp} f \subseteq \Omega$. Given a monomial transformation $f \mapsto f \circ z^M$, we call $(\{0\} \cup M^{-1}(\mathbb{R}^{>})^n) \cap (\mathbb{R}^{\geqslant})^n$ its associated cone. Given two monomial transformations $f \mapsto f \circ z^{M_1}$ and $f \mapsto f \circ z^{M_2}$ with associated cones $\Omega_1$ and $\Omega_2$, it is not hard to check that these transformations are compatible if and only if $\Omega_1 \cap \Omega_2 \neq \{0\}$.

## 5.7 Heuristic zero testing

It should be emphasized that zero testing of power series is a quite asymmetric problem in the sense that it is usually easy to prove that a non zero series is indeed non zero (it suffices to find a non zero coefficient), whereas it is often hard to prove vanishing series to be zero. Since exact zero tests are so slow, it is often preferable to use heuristic zero tests instead. In fact, heuristic zero tests can be combined with genuine zero tests: for a complex computation which involves many zero tests, we first perform all zero tests heuristically. At the end of the computation, we collect all series which were heuristically assumed to be zero in order to compute the result, and we apply an exact zero test to these series.

The most obvious heuristic zero test for a univariate D-algebraic series is to compute all coefficients up to a fixed order. Even for large orders, these coefficients can be computed efficiently using Newton's method or relaxed power series evaluation [2, 8, 1, 9, 6, 10]. In the case of multivariate D-algebraic series $f \in K[[z_1, \ldots, z_n]]$, one simple idea is to generate a random scalar vector $\lambda = (\lambda_1, \ldots, \lambda_n) \in K^n$ and to test whether $f \circ (\lambda z) = 0$. The composition $f \circ (\lambda z)$ can be computed efficiently using the algorithm(s) from section 5.5. Here we notice the remarkable fact that the derivation

$$\hat{\delta} \;=\; \delta_1 + \cdots + \delta_n$$

for which

$$\delta (f \circ (\lambda z)) \;=\; (\hat{\delta} f) \circ (\lambda z)$$

does not depend on $\lambda$. This makes it actually possible to design another exact zero test for multivariate D-algebraic series: compute a univariate D-domain capable of representing $f \circ (\lambda z)$ where $\lambda$ is treated as a formal parameter, and test whether $f \circ (\lambda z) = 0$.

# Bibliography

**[1]** A. Bostan, F. Chyzak, F. Ollivier, B. Salvy, É. Schost, and A. Sedoglavic. Fast computation of power series solutions of systems of differential equations. In *Proceedings of the 18th ACM-SIAM Symposium on Discrete Algorithms*, pages 1012–1021, New Orleans, Louisiana, U.S.A., January 2007.

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

**[3]** 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.

**[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]** M. J. Fischer and L. J. Stockmeyer. Fast on-line integer multiplication. *Proc. 5th ACM Symposium on Theory of Computing*, 9:67–72, 1974.

**[7]** J. van der Hoeven. A new zero-test for formal power series. In Teo Mora, editor, *Proc. ISSAC '02*, pages 117–122, Lille, France, July 2002.

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

**[9]** J. van der Hoeven. Newton's method and FFT trading. *JSC*, 45(8):857–878, 2010.

**[10]** J. van der Hoeven. Faster relaxed multiplication. Technical report, HAL, 2012. http://hal.archives-ouvertes.fr/hal-00687479.

**[11]** J. van der Hoeven. Effective power series computations. Technical report, HAL, 2014. http://hal.archives-ouvertes.fr/.

**[12]** J. van der Hoeven and J.R. Shackell. Complexity bounds for zero-test algorithms. *JSC*, 41:1004–1020, 2006.

**[13]** A.G. Khovanskii. *Fewnomials*, volume 88 of *Translations of Mathematical Monographs*. A.M.S., Providence RI, 1991.

**[14]** E.R. Kolchin. *Differential algebra and algebraic groups*. Academic Press, New York, 1973.

**[15]** A. Péladan-Germa. *Tests effectifs de nullité dans des extensions d'anneaux différentiels*. PhD thesis, Gage, École Polytechnique, Palaiseau, France, 1997.

**[16]** R.H. Risch. Algebraic properties of elementary functions in analysis. *Amer. Journ. of Math.*, 4(101):743–759, 1975.

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

**[18]** J. Shackell. A differential-equations approach to functional equivalence. In *Proc. ISSAC '89*, pages 7–10, Portland, Oregon, A.C.M., New York, 1989. ACM Press.

**[19]** J. Shackell. Zero equivalence in function fields defined by differential equations. *Proc. of the A.M.S.*, 336(1):151–172, 1993.