Computing with D-algebraic power series

Joris van der Hoeven
CNRS, École polytechnique

IHP, Groupe de travail "Transcendance et Combinatoire"

April 8, 2022

The zero-test problem

- $\mathbb{K}$: effective field of characteristic zero
- $f_1, \ldots, f_k$: computable power series in $\mathbb{K}[[z]]$

The zero-test problem

- $\mathbb{K}$: effective field of characteristic zero
- $f_1, \ldots, f_k$: computable power series in $\mathbb{K}[[z]]$

Problem: zero-test

Given $P \in \mathbb{K}[F_1, \ldots, F_k]$*, decide whether* $P(f_1, \ldots, f_k) = 0$.

The zero-test problem

- $\mathbb{K}$: effective field of characteristic zero
- $f_1, \ldots, f_k$: computable power series in $\mathbb{K}[[z]]$

Problem: zero-test

Given $P \in \mathbb{K}[F_1, \ldots, F_k]$, *decide whether* $P(f_1, \ldots, f_k) = 0$.

Definition

A power series $f \in \mathbb{K}[[z]]$ *is said to be* ***D-algebraic*** *if there exists a non-zero polynomial* $P \in \mathbb{K}[F_0, \ldots, F_r]$ *with* $P(f, f', \ldots, f^{(r)}) = 0$.

The zero-test problem

- $\mathbb{K}$: effective field of characteristic zero
- $f_1, \ldots, f_k$: computable power series in $\mathbb{K}[[z]]$

Problem: zero-test

Given $P \in \mathbb{K}[F_1, \ldots, F_k]$, decide whether $P(f_1, \ldots, f_k) = 0$.

Definition

*A power series $f \in \mathbb{K}[[z]]$ is said to be **D-algebraic** if there exists a non-zero polynomial $P \in \mathbb{K}[F_0, \ldots, F_r]$ with $P(f, f', \ldots, f^{(r)}) = 0$.*

Main focus of this talk: $f_1, \ldots, f_k$ are D-algebraic

Outline

Part I — Previous algorithms

Heuristic zero-testing

- $g = P(f_1, \ldots, f_k) = 0$ if and only if $g_0 = \cdots = g_{n-1} = 0$ for some large n

Heuristic zero-testing

- $g = P(f_1, \ldots, f_k) = 0$ if and only if $g_0 = \cdots = g_{n-1} = 0$ for some large n
- Fast expansions using relaxed arithmetic or Newton's method

Heuristic zero-testing

- $g = P(f_1, \ldots, f_k) = 0$ if and only if $g_0 = \cdots = g_{n-1} = 0$ for some large n
- Fast expansions using relaxed arithmetic or Newton's method
- If $\mathbb{K} = \mathbb{Q}$, then first reduce modulo medium-size random prime

Heuristic zero-testing

- $g = P(f_1, \ldots, f_k) = 0$ if and only if $g_0 = \cdots = g_{n-1} = 0$ for some large n
- Fast expansions using relaxed arithmetic or Newton's method
- If $\mathbb{K} = \mathbb{Q}$, then first reduce modulo medium-size random prime

Bottom line

- Proving that $g \neq 0$ is easy
- Proving rigorously that $g = 0$ is the harder question

Shackell's algorithm

Assume that $\mathbb{K}[f_1, \ldots, f_k]$ is stable under differentiation

Assume $\partial: \mathbb{K}[F_1, \ldots, F_k] \longrightarrow \mathbb{K}[F_1, \ldots, F_k]$ with $(\partial P)(f_1, \ldots, f_k) = \partial(P(f_1, \ldots, f_k))$

Algorithm
Input: $P \in \mathbb{K}[F_1, \ldots, F_k]$
Output: result of test $P(f_1, \ldots, f_k) = 0$

For $n = 1, 2, 3, \ldots$ do
    If $P^{(n)} \in (P, P', \ldots, P^{(n-1)})$ then
        Return $P(f_1, \ldots, f_k)_0 = \cdots = P(f_1, \ldots, f_k)_{n-1} = 0$

Other algorithms

Péladan-Germa (1995)

- $f_1, \ldots, f_k$ given by differential equations and initial conditions
- Compute Zariski closed set Z of initial conditions for which $P(f_1, \ldots, f_k) = 0$

  (first compute open subset of Z using differential algebra)
- Test whether the actual initial conditions for $f_1, \ldots, f_k$ belong to Z

Denef–Lipshitz (1984)

General decision procedure for testing whether a system of ordinary differential equations/inequations over $\mathbb{K}$ and equations/inequations on the initial conditions has a solution over $\mathbb{K}[[z]]$.

Part II — Differential algebra

Basic definitions

$\mathbb{A}$: differential $\mathbb{K}$-algebra with respect to a single derivation

Basic definitions

$\mathbb{A}$: differential $\mathbb{K}$-algebra with respect to a single derivation

$\mathbb{A}\{F\} = \mathbb{A}[F, \delta F, \delta^2 F, \ldots]$: ring of (univariate) differential polynomials over $\mathbb{A}$

$\mathbb{A}\langle F\rangle$: fraction field of $\mathbb{A}\{F\}$

Basic definitions

$\mathbb{A}$: differential $\mathbb{K}$-algebra with respect to a single derivation

$\mathbb{A}\{F\} = \mathbb{A}[F, \delta F, \delta^2 F, \ldots]$: ring of (univariate) differential polynomials over $\mathbb{A}$

$\mathbb{A}\langle F\rangle$: fraction field of $\mathbb{A}\{F\}$

For $P \in \mathbb{A}\{F\} \setminus \mathbb{A}$:

ℓ_P	**leader** of P	highest $\delta^i F$ occuring in P
$\operatorname{rank} P$	**Ritt rank** of P	$\operatorname{rank} P := (\ell_P, d)$, $d := \deg_{\ell_P} P$

Basic definitions

$\mathbb{A}$: differential $\mathbb{K}$-algebra with respect to a single derivation

$\mathbb{A}\{F\} = \mathbb{A}[F, \delta F, \delta^2 F, \ldots]$: ring of (univariate) differential polynomials over $\mathbb{A}$

$\mathbb{A}\langle F\rangle$: fraction field of $\mathbb{A}\{F\}$

For $P \in \mathbb{A}\{F\} \setminus \mathbb{A}$:

ℓ_P	**leader** of P	highest $\delta^i F$ occuring in P
$\operatorname{rank} P$	**Ritt rank** of P	$\operatorname{rank} P := (\ell_P, d)$, $d := \deg_{\ell_P} P$

Writing $P = c_d \ell_P^d + \cdots + c_0$

I_P	**initial** of P	$I_P := c_d$
S_P	**separant** of P	$S_P := \partial P / \partial \ell_P$
H_P		$H_P := I_P S_P$

Basic definitions

$\mathbb{A}$: differential $\mathbb{K}$-algebra with respect to a single derivation

$\mathbb{A}\{F\} = \mathbb{A}[F, \delta F, \delta^2 F, \ldots]$: ring of (univariate) differential polynomials over $\mathbb{A}$

$\mathbb{A}\langle F\rangle$: fraction field of $\mathbb{A}\{F\}$

For $P \in \mathbb{A}\{F\} \setminus \mathbb{A}$:

ℓ_P	**leader** of P	highest $\delta^i F$ occuring in P
rank P	**Ritt rank** of P	rank $P := (\ell_P, d)$, $d := \deg_{\ell_P} P$

Writing $P = c_d \ell_P^d + \cdots + c_0$

I_P	**initial** of P	$I_P := c_d$
S_P	**separant** of P	$S_P := \partial P / \partial \ell_P$
H_P		$H_P := I_P S_P$

$$S_P = I_{\delta P} = S_{\delta P} = I_{\delta^2 P} = S_{\delta^2 P} = \cdots$$

Ritt reduction

Reducibility

$P, Q_1, \ldots, Q_l \in \mathbb{A}\{F\} \setminus \mathbb{A}$

$$P \text{ is } \textit{reducible} \text{ w.r.t. } Q_1, \ldots, Q_l \iff \exists i,\ \operatorname{rank} P \geqslant \operatorname{rank} Q_i$$

Ritt reduction

Reducibility

$P, Q_1, \ldots, Q_l \in \mathbb{A}\{F\} \setminus \mathbb{A}$

$$P \text{ is } \textit{reducible} \text{ w.r.t. } Q_1, \ldots, Q_l \iff \exists i,\ \operatorname{rank} P \geqslant \operatorname{rank} Q_i$$

Ritt reduction

$\mathbb{N}$ $\qquad$ $\mathbb{A}\{F\}[\delta]$ $\qquad$ reduced w.r.t. $Q_1, \ldots, Q_l$

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

Ritt reduction

Reducibility

$P, Q_1, \ldots, Q_l \in \mathbb{A}\{F\} \setminus \mathbb{A}$

$$P \text{ is } \textit{reducible} \text{ w.r.t. } Q_1, \ldots, Q_l \iff \exists i,\ \operatorname{rank} P \geqslant \operatorname{rank} Q_i$$

Ritt reduction

$$\underbrace{I_{Q_1}^{\alpha_1} \cdots I_{Q_l}^{\alpha_l} S_{Q_1}^{\beta_1} \cdots S_{Q_l}^{\beta_l}}_{\text{exponents} \in \mathbb{N}} P = \underbrace{\Theta_1}_{\in \mathbb{A}\{F\}[\delta]} Q_1 + \cdots + \underbrace{\Theta_k}_{\in \mathbb{A}\{F\}[\delta]} Q_k + \underbrace{R}_{\text{reduced w.r.t. } Q_1, \ldots, Q_l}$$

$$P \operatorname{rem} Q := P \operatorname{rem} (Q_1, \ldots, Q_l) := R$$

Differential ideal generated by $Q_1, \ldots, Q_l \in \mathbb{A}\{F\}$

$$[Q] \;:=\; [Q_1, \ldots, Q_l] \;:=\; \mathbb{A}[\delta]\, Q_1 + \cdots + \mathbb{A}[\delta]\, Q_l.$$

Differential ideals

Differential ideal generated by $Q_1, \ldots, Q_l \in \mathbb{A}\{F\}$

$$[Q] \ := \ [Q_1, \ldots, Q_l] \ := \ \mathbb{A}[\delta]\, Q_1 + \cdots + \mathbb{A}[\delta]\, Q_l.$$

Saturation w.r.t. $H_Q := H_{Q_1} \cdots H_{Q_l}$

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

Differential ideals

Differential ideal generated by $Q_1, \ldots, Q_l \in \mathbb{A}\{F\}$

$$[Q] \;:=\; [Q_1, \ldots, Q_l] \;:=\; \mathbb{A}[\delta]\, Q_1 + \cdots + \mathbb{A}[\delta]\, Q_l.$$

Saturation w.r.t. $H_Q := H_{Q_1} \cdots H_{Q_l}$

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

Autoreduced sequences

$Q_1, \ldots, Q_l$ **autoreduced** $\Longleftrightarrow$ every Q_i is reduced w.r.t. $Q_1, \ldots, Q_{i-1}, Q_{i+1}, \ldots, Q_l$

Then

$$[Q] : H_Q^\infty \;=\; \{P \in \mathbb{A}\{F\} : P \text{ reduces to } 0 \text{ w.r.t. } Q_1, \ldots, Q_l\}$$

Decompositions of differential polynomials

Natural decomposition

$$P = 3\,F\,\delta F\,\delta^4 F - 7\,(\delta F)^3 + 2\,F^2 + \delta^2 F - 18\,\delta F$$

Natural decomposition

$$P = \underbrace{3\,F\,\delta F\,\delta^4 F - 7\,(\delta F)^3}_{P_3} + \underbrace{2\,F^2}_{P_2} + \underbrace{\delta^2 F - 18\,\delta F}_{P_1}$$

Decomposition by homogeneous parts

$$P = P_3 + P_2 + P_1$$

$$\deg P = 3$$

$$\operatorname{val} P = 1$$

Decompositions of differential polynomials

Natural decomposition

$$P = \sum_{\boldsymbol{i}=(i_0,\ldots,i_r)} P_{\boldsymbol{i}} \delta^{\boldsymbol{i}} F, \qquad \delta^{\boldsymbol{i}} F = \prod_j (\delta^j F)^{i_j}$$

Decomposition by homogeneous parts

$$P = \sum_d P_d, \qquad P_d = \sum_{|\boldsymbol{i}|=d} P_{\boldsymbol{i}} \delta^{\boldsymbol{i}} F, \qquad |\boldsymbol{i}| := \sum_j i_j$$

$$\begin{aligned} \deg P &:= \max\{d : P_d \neq 0\} \\ \operatorname{val} P &:= \min\{d : P_d \neq 0\} \\ P_{<d} &:= P_0 + \cdots + P_{d-1} \end{aligned}$$

Additive conjugation of $P \in \mathbb{A}\{F\}$ by $f \in \mathbb{A}$

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

Additive conjugation of $P \in \mathbb{A}\{F\}$ by $f \in \mathbb{A}$

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

Coefficients $P_{+f,\boldsymbol{i}} = (P_{+f})_{\boldsymbol{i}}$ of P_{+f}

$$P_{+f,\boldsymbol{i}} \ = \ \frac{1}{\boldsymbol{i}!} P^{(\boldsymbol{i})}(f)$$

$$P^{(\boldsymbol{i})} \ = \ \frac{\partial^{i_0 + \cdots + i_r} P}{(\partial F)^{i_0} \cdots (\partial \delta^r F)^{i_r}}$$

$$\boldsymbol{i}! \ = \ i_0! \cdots i_r!$$

Valuation in z

$v(f) \in \mathbb{N} \cup \{\infty\}$: valuation in z of $f \in \mathbb{K}[[z]]$

Valuation extends to $\mathbb{K}[[z]]\{F\} \subseteq \mathbb{K}\{F\}[[z]]$

Differential polynomials over $\mathbb{K}[[z]]$

Valuation in z

$v(f) \in \mathbb{N} \cup \{\infty\}$: valuation in z of $f \in \mathbb{K}[[z]]$

Valuation extends to $\mathbb{K}[[z]]\{F\} \subseteq \mathbb{K}\{F\}[[z]]$

Indicial polynomial $J_P \in \mathbb{K}[N]$ of homogeneous $P \in \mathbb{K}[[z]]\{F\}$ of degree d

$$J_P(n) = \sum_i (P_i)_{v(P)} \, n^{\|i\|}, \qquad \|i\| := i_1 + 2\, i_2 + \cdots + r\, i_r$$

Differential polynomials over $\mathbb{K}[[z]]$

Valuation in z

$v(f) \in \mathbb{N} \cup \{\infty\}$: valuation in z of $f \in \mathbb{K}[[z]]$

Valuation extends to $\mathbb{K}[[z]]\{F\} \subseteq \mathbb{K}\{F\}[[z]]$

Indicial polynomial $J_P \in \mathbb{K}[N]$ of homogeneous $P \in \mathbb{K}[[z]]\{F\}$ of degree d

$$J_P(n) = \sum_i (P_i)_{v(P)} n^{\|i\|}, \qquad \|i\| := i_1 + 2 i_2 + \cdots + r i_r$$

$$\forall f \in \mathbb{K}[[z]], \qquad P(f)_{v(P)+d v(f)} = J_P(v(f)) f_{v(f)}^d.$$

Differential polynomials over $\mathbb{K}[[z]]$

Valuation in z

$v(f) \in \mathbb{N} \cup \{\infty\}$: valuation in z of $f \in \mathbb{K}[[z]]$

Valuation extends to $\mathbb{K}[[z]]\{F\} \subseteq \mathbb{K}\{F\}[[z]]$

Indicial polynomial $J_P \in \mathbb{K}[N]$ of homogeneous $P \in \mathbb{K}[[z]]\{F\}$ of degree d

$$J_P(n) = \sum_i (P_i)_{v(P)} n^{\|i\|}, \qquad \|i\| := i_1 + 2 i_2 + \cdots + r i_r$$

$$\forall f \in \mathbb{K}[[z]], \qquad P(f)_{v(P)+d v(f)} = J_P(v(f)) f_{v(f)}^d.$$

$$Z_P = \begin{cases} \infty & \text{if } J_P = 0 \\ -1 & \text{if } J_P(n) \neq 0 \text{ for all } n \in \mathbb{N} \\ \max \{n \in \mathbb{N} : J_P(n) = 0\} & \text{otherwise} \end{cases}$$

Differential polynomials over $\mathbb{K}[[z]]$

Valuation in z

$v(f) \in \mathbb{N} \cup \{\infty\}$: valuation in z of $f \in \mathbb{K}[[z]]$

Valuation extends to $\mathbb{K}[[z]]\{F\} \subseteq \mathbb{K}\{F\}[[z]]$

Indicial polynomial $J_P \in \mathbb{K}[N]$ of homogeneous $P \in \mathbb{K}[[z]]\{F\}$ of degree d

$$J_P(n) = \sum_i (P_i)_{v(P)} n^{\|i\|}, \qquad \|i\| := i_1 + 2 i_2 + \cdots + r i_r$$

$$\forall f \in \mathbb{K}[[z]], \qquad P(f)_{v(P)+d v(f)} = J_P(v(f)) f_{v(f)}^d.$$

$$Z_P = \begin{cases} \infty & \text{if } J_P = 0 \\ -1 & \text{if } J_P(n) \neq 0 \text{ for all } n \in \mathbb{N} \\ \max\{n \in \mathbb{N} : J_P(n) = 0\} & \text{otherwise} \end{cases}$$

Note: $J_P \neq 0$ whenever $d = 1$, but $J_P = 0$ for $P = F\delta^2 F - (\delta F)^2$

Part III — D-algebraic power series

D-algebraic series over $\mathbb{A}$

Power series domain

- Differential subalgebra $\mathbb{A} \subseteq \mathbb{K}[[z]]$ for $\delta := z\partial/\partial z$
- For all $f \in \mathbb{A}$ and $g \in \mathbb{A} \setminus \{0\}$ with $f/g \in \mathbb{K}[[z]]$, we have $f/g \in \mathbb{A}$.

Power series domain

- Differential subalgebra $\mathbb{A} \subseteq \mathbb{K}[[z]]$ for $\delta := z\partial/\partial z$
- For all $f \in \mathbb{A}$ and $g \in \mathbb{A} \setminus \{0\}$ with $f/g \in \mathbb{K}[[z]]$, we have $f/g \in \mathbb{A}$.

D-algebraic series over $\mathbb{A}$

$f \in \mathbb{A}[[z]]$ with $P(f) = 0$ for some $P \in \mathbb{A}\{F\} \setminus \mathbb{A}$

D-algebraic series over $\mathbb{A}$

Power series domain

- Differential subalgebra $\mathbb{A} \subseteq \mathbb{K}[[z]]$ for $\delta := z\partial/\partial z$
- For all $f \in \mathbb{A}$ and $g \in \mathbb{A} \setminus \{0\}$ with $f/g \in \mathbb{K}[[z]]$, we have $f/g \in \mathbb{A}$.

D-algebraic series over $\mathbb{A}$

$f \in \mathbb{A}[[z]]$ with $P(f) = 0$ for some $P \in \mathbb{A}\{F\} \setminus \mathbb{A}$

Proposition

$f \in \mathbb{A}[[z]]$ is D-algebraic over $\mathbb{A}$ $\Longleftrightarrow$ $\mathbb{A}\{f\}$ has finite transcendence degree over A.

D-algebraic series over $\mathbb{A}$

Power series domain

- Differential subalgebra $\mathbb{A} \subseteq \mathbb{K}[[z]]$ for $\delta := z\partial/\partial z$
- For all $f \in \mathbb{A}$ and $g \in \mathbb{A} \setminus \{0\}$ with $f/g \in \mathbb{K}[[z]]$, we have $f/g \in \mathbb{A}$.

D-algebraic series over $\mathbb{A}$

$f \in \mathbb{A}[[z]]$ with $P(f) = 0$ for some $P \in \mathbb{A}\{F\} \setminus \mathbb{A}$

Proposition

$f \in \mathbb{A}[[z]]$ is D-algebraic over $\mathbb{A}$ $\Longleftrightarrow$ $\mathbb{A}\{f\}$ has finite transcendence degree over A.

Corollary

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

D-algebraic power series

Representation of elements in $\mathbb{A}^{\mathrm{dalg}}$

By pairs $(P, f) \in \mathbb{A}\{F\} \times \mathbb{K}[[z]]^{\mathrm{com}}$ with $P(f) = 0$

- P: **annihilator** of f
- f: **root** of P
- $\operatorname{val} P_{+f}$: **multiplicity** of f as a root of P
- good to ask: P **non-degenerate annihilator**, i.e. $\operatorname{val} P_{+f} = 1$

D-algebraic power series

Representation of elements in $\mathbb{A}^{\text{dalg}}$

By pairs $(P, f) \in \mathbb{A}\{F\} \times \mathbb{K}[[z]]^{\text{com}}$ with $P(f) = 0$

- P: **annihilator** of f
- f: **root** of P
- $\operatorname{val} P_{+f}$: **multiplicity** of f as a root of P
- good to ask: P **non-degenerate annihilator**, i.e. $\operatorname{val} P_{+f} = 1$

Root separation for P at f

Smallest number $\sigma_{P,f} \in \mathbb{N} \cup \{\infty\}$ such that

$$\forall \varepsilon \in \mathbb{K}[[z]], \quad P(f + \varepsilon) = 0 \ \wedge \ v(\varepsilon) \geqslant \sigma_{P,f} \implies \varepsilon = 0$$

D-algebraic power series

Representation of elements in $\mathbb{A}^{\text{dalg}}$

By pairs $(P, f) \in \mathbb{A}\{F\} \times \mathbb{K}[[z]]^{\text{com}}$ with $P(f) = 0$

- P: **annihilator** of f
- f: **root** of P
- $\operatorname{val} P_{+f}$: **multiplicity** of f as a root of P
- good to ask: P **non-degenerate annihilator**, i.e. $\operatorname{val} P_{+f} = 1$

Root separation for P at f

Smallest number $\sigma_{P,f} \in \mathbb{N} \cup \{\infty\}$ such that

$$\forall \varepsilon \in \mathbb{K}[[z]], \quad P(f + \varepsilon) = 0 \ \wedge \ v(\varepsilon) \geqslant \sigma_{P,f} \implies \varepsilon = 0$$

Note: $\sigma_{P,f} \in \mathbb{N}$ as soon as $J_{P_{+f},d} \neq 0$ where $d = \operatorname{val} P_{+f}$ (always the case when $d = 1$)

Root separation bounds

Proposition

f : D-algebraic over $\mathbb{A}$ with annihilator $P \in \mathbb{A}\{F\} \setminus \mathbb{A}$ of multiplicity d. Then

$$\sigma_{P,f} \leqslant \max\left(v(P_{+f,d}), Z_{P_{+f,d}}\right) + 1$$

Root separation bounds

Proposition

f: D-algebraic over $\mathbb{A}$ with annihilator $P \in \mathbb{A}\{F\} \setminus \mathbb{A}$ of multiplicity d. Then

$$\sigma_{P,f} \leqslant \max(v(P_{+f,d}), Z_{P_{+f,d}}) + 1$$

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

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

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

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

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

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

A partial converse

Proposition

Let $P \in \mathbb{A}\{F\} \setminus \mathbb{A}$ *and* $f \in \mathbb{K}[[z]]$. *Assume that* $S_P(f) \neq 0$ *and* $v(P(f)) > 2\sigma$, *with*

$$\sigma \geqslant \max(v(P_{+f,1}), Z_{P_{+f,1}}) + 1.$$

Then there exists a unique $\varepsilon \in \mathbb{K}[[z]]$ *with* $v(\varepsilon) > \sigma$ *and* $P_f(\varepsilon) = P(f + \varepsilon) = 0$.

A partial converse

Proposition

Let $P \in \mathbb{A}\{F\} \setminus \mathbb{A}$ *and* $f \in \mathbb{K}[[z]]$. *Assume that* $S_P(f) \neq 0$ *and* $v(P(f)) > 2\sigma$, *with*

$$\sigma \geqslant \max(v(P_{+f,1}), Z_{P_{+f,1}}) + 1.$$

Then there exists a unique $\varepsilon \in \mathbb{K}[[z]]$ *with* $v(\varepsilon) > \sigma$ *and* $P_f(\varepsilon) = P(f + \varepsilon) = 0$.

Proof. Let $\mu_1 = v(P_{+f,1}) < \sigma$.

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

Extracting the coefficient of z^{μ_1+n} in the relation $\mathrm{H}(\varepsilon) = \Delta(\varepsilon)$ yields

$$J_{\mathrm{H}}(n)\, \varepsilon_n = \Delta(\varepsilon)_{\mu_1+n}. \tag{2}$$

$n \leqslant \sigma \Longrightarrow \Delta(\varepsilon)_{\mu_1+n} = 0.$ $\qquad$ $n > \sigma \Longrightarrow J_{\mathrm{H}}(n) \neq 0$ and $\Delta(\varepsilon)_{\mu_1+n}$ only depends on $\varepsilon_0, \ldots, \varepsilon_{n-1}$.
So (2) is a recurrence relation for the computation of ε. □

Part IV — First algorithm

First algorithm

$\mathbb{A}$: effective power series domain (includes zero-test)

Let $f \in \mathbb{K}[[z]]^{\mathrm{com}}$ be a single root of $P \in \mathbb{A}\{F\} \setminus \mathbb{A}$

Algorithm ZeroTest($Q_1, \ldots, Q_n$)

INPUT: $Q_1, \ldots, Q_n \in \mathbb{A}\{F\} \setminus \{0\}$, ordered by non-decreasing Ritt rank

OUTPUT: **true** if $Q_1(f) = \cdots = Q_n(f) = 0$ and **false** otherwise

1. If $Q := Q_1 \in \mathbb{A}$ then return **false**
2. If **ZeroTest**(I_Q) then return **ZeroTest**($I_Q, Q_1, \ldots, Q_n$)
3. If **ZeroTest**(S_Q) then return **ZeroTest**($S_Q, Q_1, \ldots, Q_n$)
4. If $\exists J \in \{Q_2, \ldots, Q_n, P\}$, $J \operatorname{rem} Q \neq 0$ then return **ZeroTest**($J \operatorname{rem} Q, Q_1, \ldots, Q_n$)
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 $v(Q(f)) > 2\sigma$

Correctness

Algorithm ZeroTest($Q_1, \ldots, Q_n$)

INPUT: $Q_1, \ldots, Q_n \in \mathbb{A}\{F\} \setminus \{0\}$, ordered by non-decreasing Ritt rank

OUTPUT: **true** if $Q_1(f) = \cdots = Q_n(f) = 0$ and **false** otherwise

1. If $Q := Q_1 \in \mathbb{A}$ then return **false**
2. If **ZeroTest**(I_Q) then return **ZeroTest**($I_Q, Q_1, \ldots, Q_n$)
3. If **ZeroTest**(S_Q) then return **ZeroTest**($S_Q, Q_1, \ldots, Q_n$)
4. If $\exists J \in \{Q_2, \ldots, Q_n, P\}, J \operatorname{rem} Q \neq 0$ then return **ZeroTest**($J \operatorname{rem} Q, Q_1, \ldots, Q_n$)
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 $v(Q(f)) > 2\sigma$

$$I_Q^j S_Q^k P = U_0 Q + \cdots + U_r \delta^r Q$$

Correctness

Algorithm ZeroTest($Q_1, \ldots, Q_n$)

INPUT: $Q_1, \ldots, Q_n \in \mathbb{A}\{F\} \setminus \{0\}$, ordered by non-decreasing Ritt rank

OUTPUT: **true** if $Q_1(f) = \cdots = Q_n(f) = 0$ and **false** otherwise

1. If $Q := Q_1 \in \mathbb{A}$ then return **false**
2. If **ZeroTest**(I_Q) then return **ZeroTest**($I_Q, Q_1, \ldots, Q_n$)
3. If **ZeroTest**(S_Q) then return **ZeroTest**($S_Q, Q_1, \ldots, Q_n$)
4. If $\exists J \in \{Q_2, \ldots, Q_n, P\}$, $J \operatorname{rem} Q \neq 0$ then return **ZeroTest**($J \operatorname{rem} Q, Q_1, \ldots, Q_n$)
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 $v(Q(f)) > 2\sigma$

$$I_Q^j S_Q^k P = U_0 Q + \cdots + U_r \delta^r Q \qquad \longrightarrow \qquad \exists!\, \varepsilon \in \mathbb{K}[[z]],\ v(\varepsilon) > \sigma \ \wedge\ Q(f + \varepsilon) = 0$$

Correctness

Algorithm ZeroTest$(Q_1, \ldots, Q_n)$

INPUT: $Q_1, \ldots, Q_n \in \mathbb{A}\{F\} \setminus \{0\}$, ordered by non-decreasing Ritt rank

OUTPUT: **true** if $Q_1(f) = \cdots = Q_n(f) = 0$ and **false** otherwise

1. If $Q := Q_1 \in \mathbb{A}$ then return **false**
2. If **ZeroTest**(I_Q) then return **ZeroTest**$(I_Q, Q_1, \ldots, Q_n)$
3. If **ZeroTest**(S_Q) then return **ZeroTest**$(S_Q, Q_1, \ldots, Q_n)$
4. If $\exists J \in \{Q_2, \ldots, Q_n, P\}, J \operatorname{rem} Q \neq 0$ then return **ZeroTest**$(J \operatorname{rem} Q, Q_1, \ldots, Q_n)$
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 $v(Q(f)) > 2\sigma$

$$I_Q^j S_Q^k P \;=\; U_0 Q + \cdots + U_r \delta^r Q$$

$$\exists!\, \varepsilon \in \mathbb{K}[[z]],\ v(\varepsilon) > \sigma \ \wedge\ Q(f + \varepsilon) = 0$$

$$v(P_{+f+\varepsilon,1}) = v(P_{+f,1}) < \sigma$$

$$Z_{P_{+f+\varepsilon,1}} = Z_{P_{+f,1}} < \sigma$$

$$v(I_Q(f + \varepsilon)) = v(I_Q(f)) < \sigma$$

$$v(S_Q(f + \varepsilon)) = v(S_Q(f)) < \sigma$$

Correctness

Algorithm ZeroTest($Q_1, \ldots, Q_n$)
INPUT: $Q_1, \ldots, Q_n \in \mathbb{A}\{F\} \backslash \{0\}$, ordered by non-decreasing Ritt rank
OUTPUT: **true** if $Q_1(f) = \cdots = Q_n(f) = 0$ and **false** otherwise

1. If $Q := Q_1 \in \mathbb{A}$ then return **false**
2. If **ZeroTest**(I_Q) then return **ZeroTest**($I_Q, Q_1, \ldots, Q_n$)
3. If **ZeroTest**(S_Q) then return **ZeroTest**($S_Q, Q_1, \ldots, Q_n$)
4. If $\exists J \in \{Q_2, \ldots, Q_n, P\}$, $J \operatorname{rem} Q \neq 0$ then return **ZeroTest**($J \operatorname{rem} Q, Q_1, \ldots, Q_n$)
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 $v(Q(f)) > 2\sigma$

$$I_Q^j S_Q^k P = U_0 Q + \cdots + U_r \delta^r Q$$

$$P(f + \varepsilon) = 0$$

$$\exists!\, \varepsilon \in \mathbb{K}[[z]],\ v(\varepsilon) > \sigma \ \wedge\ Q(f + \varepsilon) = 0$$

$$v(P_{+f+\varepsilon,1}) = v(P_{+f,1}) < \sigma$$

$$Z_{P_{+f+\varepsilon,1}} = Z_{P_{+f,1}} < \sigma$$

$$v(I_Q(f + \varepsilon)) = v(I_Q(f)) < \sigma$$

$$v(S_Q(f + \varepsilon)) = v(S_Q(f)) < \sigma$$

Correctness

Algorithm ZeroTest($Q_1, \ldots, Q_n$)
INPUT: $Q_1, \ldots, Q_n \in \mathbb{A}\{F\} \setminus \{0\}$, ordered by non-decreasing Ritt rank
OUTPUT: **true** if $Q_1(f) = \cdots = Q_n(f) = 0$ and **false** otherwise

1. If $Q := Q_1 \in \mathbb{A}$ then return **false**
2. If **ZeroTest**(I_Q) then return **ZeroTest**($I_Q, Q_1, \ldots, Q_n$)
3. If **ZeroTest**(S_Q) then return **ZeroTest**($S_Q, Q_1, \ldots, Q_n$)
4. If $\exists J \in \{Q_2, \ldots, Q_n, P\}$, $J \operatorname{rem} Q \neq 0$ then return **ZeroTest**($J \operatorname{rem} Q, Q_1, \ldots, Q_n$)
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 $v(Q(f)) > 2\sigma$

$$I_Q^j S_Q^k P = U_0 Q + \cdots + U_r \delta^r Q$$

$$P(f + \varepsilon) = 0$$

$$\varepsilon = 0$$

$$\exists!\, \varepsilon \in \mathbb{K}[[z]],\ v(\varepsilon) > \sigma \ \wedge\ Q(f + \varepsilon) = 0$$

$$v(P_{+f+\varepsilon,1}) = v(P_{+f,1}) < \sigma$$

$$Z_{P_{+f+\varepsilon,1}} = Z_{P_{+f,1}} < \sigma$$

$$v(I_Q(f + \varepsilon)) = v(I_Q(f)) < \sigma$$

$$v(S_Q(f + \varepsilon)) = v(S_Q(f)) < \sigma$$

Correctness

Algorithm ZeroTest($Q_1, \ldots, Q_n$)
INPUT: $Q_1, \ldots, Q_n \in \mathbb{A}\{F\} \setminus \{0\}$, ordered by non-decreasing Ritt rank
OUTPUT: **true** if $Q_1(f) = \cdots = Q_n(f) = 0$ and **false** otherwise

1. If $Q := Q_1 \in \mathbb{A}$ then return **false**
2. If **ZeroTest**(I_Q) then return **ZeroTest**($I_Q, Q_1, \ldots, Q_n$)
3. If **ZeroTest**(S_Q) then return **ZeroTest**($S_Q, Q_1, \ldots, Q_n$)
4. If $\exists J \in \{Q_2, \ldots, Q_n, P\}$, $J \operatorname{rem} Q \neq 0$ then return **ZeroTest**($J \operatorname{rem} Q, Q_1, \ldots, Q_n$)
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 $v(Q(f)) > 2\sigma$

$$I_Q^j S_Q^k P = U_0 Q + \cdots + U_r \delta^r Q$$

$$P(f + \varepsilon) = 0$$

$$\varepsilon = 0$$

$$Q(f) = 0$$

$$\exists!\, \varepsilon \in \mathbb{K}[[z]],\ v(\varepsilon) > \sigma \ \wedge\ Q(f + \varepsilon) = 0$$

$$v(P_{+f+\varepsilon,1}) = v(P_{+f,1}) < \sigma$$

$$Z_{P_{+f+\varepsilon,1}} = Z_{P_{+f,1}} < \sigma$$

$$v(I_Q(f + \varepsilon)) = v(I_Q(f)) < \sigma$$

$$v(S_Q(f + \varepsilon)) = v(S_Q(f)) < \sigma$$

Correctness

Algorithm ZeroTest($Q_1, \ldots, Q_n$)
INPUT: $Q_1, \ldots, Q_n \in \mathbb{A}\{F\} \setminus \{0\}$, ordered by non-decreasing Ritt rank
OUTPUT: **true** if $Q_1(f) = \cdots = Q_n(f) = 0$ and **false** otherwise

1. If $Q := Q_1 \in \mathbb{A}$ then return **false**
2. If **ZeroTest**(I_Q) then return **ZeroTest**($I_Q, Q_1, \ldots, Q_n$)
3. If **ZeroTest**(S_Q) then return **ZeroTest**($S_Q, Q_1, \ldots, Q_n$)
4. If $\exists J \in \{Q_2, \ldots, Q_n, P\}, J \operatorname{rem} Q \neq 0$ then return **ZeroTest**($J \operatorname{rem} Q, Q_1, \ldots, Q_n$)
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 $v(Q(f)) > 2\sigma$

$$I_Q^j S_Q^k P = U_0 Q + \cdots + U_r \delta^r Q$$

$$P(f + \varepsilon) = 0$$

$$\varepsilon = 0$$

$$Q(f) = Q_2(f) = \cdots = Q_n(f) = 0$$

$$\exists!\, \varepsilon \in \mathbb{K}[[z]],\ v(\varepsilon) > \sigma \ \wedge\ Q(f + \varepsilon) = 0$$

$$v(P_{+f+\varepsilon,1}) = v(P_{+f,1}) < \sigma$$

$$Z_{P_{+f+\varepsilon,1}} = Z_{P_{+f,1}} < \sigma$$

$$v(I_Q(f + \varepsilon)) = v(I_Q(f)) < \sigma$$

$$v(S_Q(f + \varepsilon)) = v(S_Q(f)) < \sigma$$

Pessimistic bound

$$\sigma \;:=\; \max\left(v(P_{+f,1}), Z_{P_{+f,1}}, v(I_Q(f)), v(S_Q(f)), v(Q_{+f,1}), Z_{Q_{+f,1}}\right) + 1$$

Shortcomings

Pessimistic bound

$$\sigma \;:=\; \max\left(v(P_{+f,1}), Z_{P_{+f,1}}, v(I_Q(f)), v(S_Q(f)), v(Q_{+f,1}), Z_{Q_{+f,1}}\right) + 1$$

Consequence

Algorithm cannot be applied when elements in $\mathbb{K}$ depend on parameters

(Dynamic or directed evaluation)

Part V — Second algorithm

Idea: allow perturbed solutions $f + \varepsilon$ in a larger space $\mathbb{K}[\log z][[z]]$

Logarithmic power series

Idea: allow perturbed solutions $f + \varepsilon$ in a larger space $\mathbb{K}[\log z][[z]]$

- Valuation in z defined as before
- δ maps $\mathbb{K}[\log z]\, z^i$ into itself for all i

Logarithmic power series

Idea: allow perturbed solutions $f+\varepsilon$ in a larger space $\mathbb{K}[\log z][[z]]$

- Valuation in z defined as before
- δ maps $\mathbb{K}[\log z]\,z^i$ into itself for all i

Strong root separation for P at f

Smallest number $\sigma^*_{P,f} \in \mathbb{N} \cup \{\infty\}$ such that

$$\forall \varepsilon \in \mathbb{K}[\log z][[z]], \quad P(f+\varepsilon) = 0 \;\wedge\; v(\varepsilon) \geqslant \sigma^*_{P,f} \implies \varepsilon = 0$$

Logarithmic power series

Idea: allow perturbed solutions $f+\varepsilon$ in a larger space $\mathbb{K}[\log z][[z]]$

- Valuation in z defined as before
- δ maps $\mathbb{K}[\log z]\, z^i$ into itself for all i

Strong root separation for P at f

Smallest number $\sigma^*_{P,f} \in \mathbb{N} \cup \{\infty\}$ such that

$$\forall \varepsilon \in \mathbb{K}[\log z][[z]], \quad P(f+\varepsilon) = 0 \;\wedge\; v(\varepsilon) \geqslant \sigma^*_{P,f} \;\Longrightarrow\; \varepsilon = 0$$

Proposition

f : D-algebraic over $\mathbb{A}$ with annihilator $P \in \mathbb{A}\{F\} \setminus \mathbb{A}$ of multiplicity d. Then

$$\sigma^*_{P,f} \leqslant \max(v(P_{+f,d}), Z_{P_{+f,d}}) + 1$$

Existence

Proposition

Let $P \in \mathbb{A}\{F\} \setminus \mathbb{A}$ *and* $f \in \mathbb{K}[[z]]$*. Assume that* $S_P(f) \neq 0$ *and* $v(P(f)) > 2\sigma$*, with*

$$\sigma \geqslant \max(v(P_{+f,1}), Z_{P_{+f,1}}) + 1.$$

Then there exists a root $\varepsilon \in \mathbb{K}[\log z][[z]]$ *with* $v(\varepsilon) > \sigma$ *and* $P_f(\varepsilon) = P(f + \varepsilon) = 0$.

Lemma

Let $L = L_r \delta^r + \cdots + L_s \delta^s \in \mathbb{K}[\delta]$ *with* $L_r \neq 0$ *and* $L_s \neq 0$*. Then there exists a unique operator*

$$L^{-1}: \mathbb{K}[\log z] \longrightarrow \mathbb{K}[\log z]\,(\log z)^s$$

with $L L^{-1} g = g$ *for every* $g \in \mathbb{K}[\log z]$.

Second algorithm

$\mathbb{A}$: effective power series domain (includes zero-test)

Let $f \in \mathbb{K}[[z]]^{\text{com}}$ be a single root of $P \in \mathbb{A}\{F\} \setminus \mathbb{A}$

Algorithm ZeroTest*($Q_1, \ldots, Q_n$)

INPUT: $Q_1, \ldots, Q_n \in A\{F\} \backslash \{0\}$, ordered by non-decreasing Ritt rank

OUTPUT: **true** if $Q_1(f) = \cdots = Q_n(f) = 0$ and **false** otherwise

1. If $Q := Q_1 \in A$ then return **false**
2. If **ZeroTest***(I_Q) then return **ZeroTest***($I_Q, Q_1, \ldots, Q_n$)
3. If **ZeroTest***(S_Q) then return **ZeroTest***($S_Q, Q_1, \ldots, Q_n$)
4. If $\exists J \in \{Q_2, \ldots, Q_n, P\}, J \operatorname{rem} Q \neq 0$ then return **ZeroTest***($J \operatorname{rem} Q, Q_1, \ldots, Q_n$)
5. Let $\sigma := \max(v(P_{+f,1}), Z_{P_{+f,1}}, v(I_Q(f)), v(S_Q(f)), v(Q_{+f,1})) + 1$
6. Return the result of the test $v(Q(f)) > 2\sigma$

Single extension

We have shown that $\mathbb{A}\{f\}$ has an effective zero-test

Consequently, $\mathbb{A}\langle f\rangle$ has an effective zero-test

Hence $\mathbb{A}\langle f\rangle \cap \mathbb{K}[[z]]$ is again an effective power series domain

Towers

Single extension

We have shown that $\mathbb{A}\{f\}$ has an effective zero-test

Consequently, $\mathbb{A}\langle f\rangle$ has an effective zero-test

Hence $\mathbb{A}\langle f\rangle \cap \mathbb{K}[[z]]$ is again an effective power series domain

Multiple extensions

$$\mathbb{A} \subseteq \mathbb{A}\langle f_1\rangle \cap \mathbb{K}[[z]] \subseteq \mathbb{A}\langle f_1, f_2\rangle \cap \mathbb{K}[[z]] \subseteq \cdots \subseteq \mathbb{A}\langle f_1, \ldots, f_k\rangle \cap \mathbb{K}[[z]]$$

Towers

Single extension

We have shown that $\mathbb{A}\{f\}$ has an effective zero-test

Consequently, $\mathbb{A}\langle f\rangle$ has an effective zero-test

Hence $\mathbb{A}\langle f\rangle \cap \mathbb{K}[[z]]$ is again an effective power series domain

Multiple extensions

$$\mathbb{A} \subseteq \mathbb{A}\langle f_1\rangle \cap \mathbb{K}[[z]] \subseteq \mathbb{A}\langle f_1, f_2\rangle \cap \mathbb{K}[[z]] \subseteq \cdots \subseteq \mathbb{A}\langle f_1, \ldots, f_k\rangle \cap \mathbb{K}[[z]]$$

Variant

Direct extension $\mathbb{A} \subseteq \mathbb{A}\langle f_1, \ldots, f_k\rangle \cap \mathbb{K}[[z]]$ using multivariate differential polynomials

Towers

Single extension

We have shown that $\mathbb{A}\{f\}$ has an effective zero-test

Consequently, $\mathbb{A}\langle f\rangle$ has an effective zero-test

Hence $\mathbb{A}\langle f\rangle \cap \mathbb{K}[[z]]$ is again an effective power series domain

Multiple extensions

$$\mathbb{A} \subseteq \mathbb{A}\langle f_1\rangle \cap \mathbb{K}[[z]] \subseteq \mathbb{A}\langle f_1, f_2\rangle \cap \mathbb{K}[[z]] \subseteq \cdots \subseteq \mathbb{A}\langle f_1, \ldots, f_k\rangle \cap \mathbb{K}[[z]]$$

Variant

Direct extension $\mathbb{A} \subseteq \mathbb{A}\langle f_1, \ldots, f_k\rangle \cap \mathbb{K}[[z]]$ using multivariate differential polynomials

Note

Elements of “base” $\mathbb{A}$ need not be D-algebraic

Multivariate power series domain

- Differential subalgebra $\mathbb{A} \subseteq \mathbb{K}[[z_1, \ldots, z_n]]$ for $\delta_1 := z_1 \partial / \partial z_1, \ldots, \delta_n := z_n \partial / \partial z_n$
- For all $f \in \mathbb{A}$ and $g \in \mathbb{A} \setminus \{0\}$ with $f / g \in \mathbb{K}[[z_1, \ldots, z_n]]$, we have $f / g \in \mathbb{A}$
- $\mathbb{A}$ closed under the substitutions of $z_i := 0$ for $i = 1, \ldots, n$

D-algebraic series

- D-algebraic series w.r.t. δ_i for $i = 1, \ldots, n$

Effective tribes

Theorem

The collection $\mathscr{D} = (\mathscr{D}_n)$ of D-algebraic series over $\mathbb{K}$ for all n forms an effective tribe:

- *Each $\mathscr{D}_n$ forms an effective multivariate power series domain*
- *$\mathscr{D}$ is effectively closed under the implicit function theorem and composition*
- *$\mathscr{D}$ is effectively closed under monomial transformations*

Theorem

- *The tribe $\mathscr{D}$ is effectively closed under Weierstrass division*
- *Possible to develop an effective elimination theorem for $\mathscr{D}$*

Thank you !

http://www.texmacs.org