# Computing with D-algebraic power series

**Joris van der Hoeven**
CNRS, École polytechnique

*DART XII, Kassel, Germany*

**April 11, 2024**

# The zero-test problem



- $\mathbb{K}$: effective field of characteristic zero

**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

**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 $P(f, f', \ldots, f^{(r)}) = 0$.*

- Assume $f_1, \ldots, f_k \in \mathbb{K}[[z]]$ D-algebraic
- Each $f_i$ the unique solution of $P_i(f_i) = 0$ with a finite number of initial conditions.

**Problem: zero-test**

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

# Brief history



**Folklore** Various algorithms that do not take into account initial conditions.

**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 $\mathbb{K}[[z]]$.

**Shackell (1989–1993)** Various more dedicated zero-tests.

**Péladan-Germa (1995)** Perturbation approach for zero-testing.

**van der Hoeven (2002, 2019)** Today.

# Outline

# **Part I** — Differential algebra

# Basic notation



$\mathbb{K}$: differential field for $\delta := z\frac{\partial}{\partial z}$

$\mathbb{A}$: differential $\mathbb{K}$-algebra

$\mathbb{A}\{F\} := \mathbb{A}[F, \delta F, \delta^2 F, \ldots]$

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

$I_P$ : initial of $P \in \mathbb{A}\{F\}$

$S_p$ : separant of $P$

$H_P := I_P S_P$

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

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

$P$ rem $(Q_1, \ldots, Q_l)$ : remainder after Ritt reduction

# Decomposition by homogeneous parts



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

# Decomposition by homogeneous parts



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

$$\deg P = 3$$
$$\operatorname{val} P = 1$$

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

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

# Additive conjugation



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

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

**Example**

$$\begin{aligned} P &= z + z^2 - zF - (1+z)\,\delta F + F\,\delta F - z\,(\delta^2 F)^3 \\ \varphi &= 1 + z \\ P_{+\varphi} &= F\,\delta F - z\,(\delta^2 F)^3 \end{aligned}$$

# Additive conjugation 

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

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

**Example**

$$\begin{aligned} P &= z + z^2 - zF - (1+z)\,\delta F + F\,\delta F - z\,(\delta^2 F)^3 \\ \varphi &= 1 + z \\ P_{+\varphi} &= F\,\delta F - z\,(\delta^2 F)^3 \end{aligned}$$

**Note**

$\operatorname{val} P_{+\varphi} \;=\; 2 \qquad \longrightarrow \qquad \varphi$ is a root of $P$ of multiplicity 2

**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 $d$**

$$P = (z^4 - 3z^5 + \cdots) F^2 - z^3 F \delta F + (4z^3 - 5z^4 + \cdots)(\delta^2 F)^2$$

# 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 $d$**

$$P \;=\; (z^4 - 3z^5 + \cdots) F^2 - z^3 F \delta F + (4z^3 - 5z^4 + \cdots)(\delta^2 F)^2$$

**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 $d$**

$$P \;=\; (z^4 - 3z^5 + \cdots)\,F^2 - z^3 F\,\delta F + (4z^3 - 5z^4 + \cdots)\,(\delta^2 F)^2$$

$$D_P \;=\; -F\,\delta F + 4\,(\delta^2 F)^2$$

# 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 $d$**

$$P \;=\; (z^4 - 3z^5 + \cdots)\, F^2 - z^3 F\, \delta F + (4z^3 - 5z^4 + \cdots)\, (\delta^2 F)^2$$

$$D_P \;=\; -F\, \delta F + 4\, (\delta^2 F)^2$$

$$\downarrow \qquad \delta^i F \rightarrow N^i$$

$$J_P \;=\; -N + 4N^4$$

# 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 $d$**

$$P = (z^4 - 3z^5 + \cdots) F^2 - z^3 F \delta F + (4z^3 - 5z^4 + \cdots)(\delta^2 F)^2$$

$$D_P = -F \delta F + 4(\delta^2 F)^2$$

$$\downarrow \qquad \delta^i F \to N^i$$

$$J_P = -N + 4N^4$$

$$P(7z^{10} + \cdots) = 7^2 \cdot 39990 \cdot z^{23} + \cdots = 7^2 J_P(10) z^{3+2\cdot 10} + \cdots$$

# Indicial polynomial — continued



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

# Indicial polynomial — continued



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

**Largest zero**

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

# Indicial polynomial — continued

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

**Largest zero**

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

**Case $d = 1$ →** $J_P \neq 0$ and $Z_P$ is finite

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

**Largest zero**

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

**Case $d = 1$ →** $J_P \neq 0$ and $Z_P$ is finite

**Case $d \geqslant 2$ →** we may have $J_P = 0$:

$$P = F\delta^2 F - (\delta F)^2$$

$P(z^\lambda) = 0$ for any $\lambda$

# **Part II** — D-algebraic power series

## 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 $\mathbb{A}^{\text{dalg}}$ of D-algebraic series over $\mathbb{A}$ forms a power series domain.*

**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. $\operatorname{val} P_{+f} = 1$

## 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

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

### 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. $\operatorname{val} P_{+f} = 1$

### Root separation for $P$ at $f$

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

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

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

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

$n \leqslant \sigma \Rightarrow \Delta(\varepsilon)_{\mu_1+n} = 0$. $n > \sigma \Rightarrow J_{\mathrm{H}}(n) \neq 0$ 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 $\varepsilon$. □

# **Part III** — First algorithm

# First 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: $Q_1, \ldots, Q_n \in \mathbb{A}\{F\} \setminus \{0\}$, 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 $\sigma := \max\left(v(P_{+f,1}), Z_{P_{+f,1}}, v(I_Q(f)), v(S_Q(f)), v(Q_{+f,1}), Z_{Q_{+f,1}}\right) + 1$
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 $v(Q(f)) > 2\sigma$

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

**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 $v(Q(f)) > 2\sigma$

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

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

# 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: $Q_1, \ldots, Q_n \in \mathbb{A}\{F\} \setminus \{0\}$, 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 $v(Q(f)) > 2\sigma$

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

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

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

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

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

$$\left\{ \begin{array}{l} v(I_Q(f+\varepsilon)) = v(I_Q(f)) < \sigma \\ v(S_Q(f+\varepsilon)) = v(S_Q(f)) < \sigma \end{array} \right.$$

# 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 IV** — Second algorithm

# Logarithmic power series



**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
- $\delta$ maps $\mathbb{K}[\log z]\, z^i$ into itself for all $i$

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

- Valuation in $z$ defined as before
- $\delta$ 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

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

# Logarithmic power series

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

- Valuation in $z$ defined as before
- $\delta$ 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

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

### Proposition

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

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

# 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* $P_f(\varepsilon) = P(f + \varepsilon) = 0$.

No similar uniqueness result needed.

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

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

1. If $Q := Q_1 \in A$ 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 $v(Q(f)) > 2\sigma$

# **Part V** — Generalizations and related results

# 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

# 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 differential polynomials in several indeterminates $F_1,\ldots,F_k$

# 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 differential polynomials in several indeterminates $F_1, \ldots, F_k$

## Note

Elements of the "base" algebra $\mathbb{A}$ need not be D-algebraic

# Non-degenerate annihilators



**Theorem**

*There exists an alorithm which, given*

- *a computable power series* $f \in \mathbb{K}[[z]]^{\mathrm{com}}$
- *a differential polynomial* $P \in \mathbb{A}\{F\}$ *with* $P(f) = 0$,

*computes a non-degenerate annihilator* $\tilde{P} \in \mathbb{A}\{F\}$ *of* $f$.

# Generalization



**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. $\delta_i$ for $i = 1, \ldots, n$

# Effective tribes



**Theorem**

*Let $\mathcal{D}_n \subseteq \mathbb{K}[[z_1, \ldots, z_n]]$ be the set of D-algebraic series over $\mathbb{K}$ in $n$ variables.*

*The collection $\mathcal{D} = (\mathcal{D}_n)$ for all $n \in \mathbb{N}$ forms an effective tribe:*

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

**Theorem**

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

# Thank you !

http://www.texmacs.org

**New:** erc European Research Council Established by the European Commission ODELIX