# A new zero-test for formal power series 

$\infty \infty \infty$

by Joris van der Hoeven<br>C.N.R.S., Université Paris-Sud<br>ISSAC' 02, Lille, 10/7/2002

$\infty 000$

Written using GNU $T_{E} X_{\text {MACS }}$ (www.texmacs.org)

## The problem

## Testing functional identities

- $\sin ^{2} x+\cos ^{2} x=1$
- $\log \left(x^{x^{x}}+e^{x \log x}\right)-x^{x} \log x=\log \left(1+x^{x\left(1-x^{x-1}\right)}\right)$
functional identities $=$ constant identities + power series identities


## Testing constant identities

- $\sqrt[3]{\sqrt[5]{32 / 5}-\sqrt[5]{27 / 5}}=(1+\sqrt[5]{3}-\sqrt[5]{9}) / \sqrt[5]{25}$
- $\int_{-\infty}^{\infty} e^{-x^{2}} \mathrm{~d} x=\sqrt{\pi}$

Testing power series identities

- $Q \in \mathcal{R}\left[F, F^{\prime} \ldots, F^{(r)}\right] \subseteq \mathcal{R}\{F\}, \mathcal{R}=\mathcal{K}[z], Q \notin \mathcal{R}$
- $f \in \mathcal{K}[[z]]$ such that $Q\left(f, f^{\prime}, \ldots, f^{(r)}\right)=0$
- Given $P \in \mathcal{R}\{F\}$, do we have $P(f)=0$ ?
- Towers: replace $\mathcal{R}$ by $\mathcal{R}\left[f, \ldots, f^{(r)}, S_{Q}(f)^{-1}\right]$ and continue.

Structural approches.
Ax, Risch, Richardson

Bounding the valuation.
Khovanskii, Shackell/vdH, witness conjectures

Model theoretical approach.
Dedef/Lipschitz

Groebner bases and saturation.
Shackell, Péladan-Germa/vdH

Varying the initial conditions.
Péladan-Germa

Generalized solution approach.
Shackell, Shackell/vdH, vdH

1. Ensure that $\frac{\partial Q}{\partial F^{(i)}}(f) \neq 0$ for some $i \in\{0, \ldots, r\}$ (modulo replacing $Q$ by $\frac{\partial Q}{\partial F^{(i)}}$ )
2. Work with derivation $\delta=\frac{z \partial}{\partial z}$ and reduce to the case when

$$
Q=L F+z M
$$

with $L \in \mathcal{K}[\delta]$ and $M \in \mathcal{R}\{F\}$
(modulo a transformation $f \rightarrow f_{0}+\cdots+f_{k} z^{k}+\tilde{f} z^{k+1}$ )
3. We now have a recurrence relation for the coefficients of $f$ :

$$
f_{k}=-\frac{1}{\Lambda(k)}(M(f))_{k-1}
$$

where $\Lambda \in \mathcal{K}[k]$ is obtained by substituting $\delta \rightarrow k$ in $L$
4. Let $s$ be the largest root of $\Lambda$ in $\mathbb{N}$
$f$ unique solution to $Q(f)=0$ with fixed $f_{0}, \ldots, f_{s}$

## The algorithm

Algorithm $P \equiv 0$
Input: a differential polynomial $P \in \mathcal{R}\{F\}$
Output: true if and only if $P \equiv 0$
Step 1 [Initialize]
$H:=1, R:=P$, reducing $:=$ true

## Step 2 [Reduction]

while reducing [invariant: $H \not \equiv 0$ and $P \equiv 0 \Leftrightarrow R \equiv 0$ ]

$$
\begin{array}{ll}
\text { if } \quad R \in \mathcal{R} & \text { then return } R=0 \\
\text { else if } I_{R} \equiv 0 & \text { then } R:=R-I_{R} V_{R} \\
\text { else if } S_{R} \equiv 0 & \text { then } H:=I_{R} H, R:=R \text { rem } S_{R} \\
\text { else if } Q \text { rem } R \neq 0 & \text { then } H:=I_{R} S_{R} H, R:=Q \text { rem } R \\
\text { else } & H:=I_{R} S_{R} H, \text { reducing }:=\text { false }
\end{array}
$$

[Final test]
let $k$ be minimal with $\operatorname{deg}_{\prec z^{k}} H_{+f_{0}+\cdots+f_{k} z^{k}}=0$
$k:=\max \{k, s\}$
return $\operatorname{deg}_{\prec z^{k}} R_{+f_{0}+\cdots+f_{k} z^{k}} \neq 0$

## Asymptotic algebraic equations

The Puiseux theorem
Let $A \in \mathcal{K}[[z]][F]^{*}$. Then

$$
A(f)=0
$$

admits $\operatorname{deg} A$ solutions in $\mathcal{K}^{\text {alg }}\left[\left[z^{\mathbb{Q}}\right]\right]$.

The Puiseux theorem for asymptotic algebraic equations [vdH 1997]
Let $A \in \mathcal{K}[[z]][F]^{*}$ and $\nu \in \mathbb{R} \cup\{-\infty\}$. Then

$$
A(f)=0 \quad\left(f \prec z^{\nu}\right)
$$

admits $\operatorname{deg}_{\prec z^{\nu}} A$ solutions in $\mathcal{K}^{\text {alg }}\left[\left[z^{\mathbb{Q}}\right]\right]$,
where $\operatorname{deg}_{\prec z^{\nu}} A$ is the Newton degree.

Definition of the Newton degree



$$
\begin{aligned}
& \frac{z^{3}}{1-z}+\frac{z}{1-z^{2}}\left(f+f^{\prime}\right)+\left(f+f^{\prime \prime}\right)^{2}+\left(f+f^{\prime}\right)^{4}+ \\
& z^{4}\left(f^{\prime}+f^{\prime \prime \prime}\right)^{5}+z^{3}\left(f^{6}+f f^{\prime} f^{\prime \prime} f^{\prime \prime \prime} f^{\prime \prime \prime \prime} f^{\prime \prime \prime \prime \prime}\right)=0
\end{aligned}
$$

1 Logarithmic transseries
Generalized series in $z, \log z, \log \log z, \ldots, \log _{l} z$ for some $l$
Example: $z+(\log z) z+2!(\log z)^{2} z^{2}+3!(\log z)^{3} z^{3}+\cdots$
Notation: $\mathbb{L}$ field of grid-based logarithmic transseries
2 Theorem for the resolution of aade's in $\mathbb{L}$ [vdH 2001]
Let $A \in \mathbb{L}\{F\}$ and $\nu \in \mathbb{R} \cup\{-\infty\}$. Then

$$
A(f)=0 \quad\left(f \prec z^{\nu}\right)
$$

admits at least $\operatorname{deg}_{\prec z^{\nu}} A$ solutions in $\mathbb{L}$.
3 Also

- There exist no solutions if $\operatorname{deg}_{\prec z^{\nu}} A=0$.
- $\quad f$ remains the unique solution to $Q(f)=0$ in $\mathbb{L}$ modulo $\prec z^{s}$.

4 Negative case
If $\operatorname{deg}_{\prec z^{k}} R_{+f_{0}+\cdots+f_{k} z^{k}}=0$, then $R \not \equiv 0$ and $P \not \equiv 0$.

## 5 Positive case

- Assume that $\operatorname{deg}_{\prec z^{k}} R_{+f_{0}+\cdots+f_{k} z^{k}} \neq 0$.
- There exists an $\tilde{f} \in \mathbb{L}$ with $R(\tilde{f})=0$ and $\tilde{f}-f \prec z^{k}$.
- Since $Q$ rem $R=0$ and $I_{R} S_{R} \mid H$, we have a relation of the form

$$
H^{\beta} Q=X_{0} R+\cdots+X_{t} R^{(t)}
$$

- Since $R(\tilde{f})=0$ and $H(\tilde{f}) \neq 0$, we have $Q(\tilde{f})=0$.
- But $f$ was the unique solution to $Q(f)=0$ modulo $\prec z^{s}$.
- Hence $f=\tilde{f}$ and $R \equiv P \equiv 0$.


## Advantages of the new algorithm

- Differential equations of arbitrary order.
- Accomodates divergent power series solutions and "diveregence does not get worse during the algorithm".
- Better understanding of previous work by Shackell using the differential algebra setting.
- More efficient?

Witness conjectures...

- Generalizations to partial differential equations?

In order to test whether $P(f)=0$, it suffices to test whether

$$
P(f)_{0}=\cdots=P(f)_{\varpi(\sigma)}=0
$$

where

- $\sigma$ is the "total input size" (in order to describe the problem).
- The witness function $\varpi(\sigma)$ is linear (probably $\varpi(\sigma)=2 \sigma$ is OK).

