A zero test for σ-algebraic power series[*]

JORIS VAN DER HOEVEN[a], GLEB POGUDIN[b]

CNRS, École polytechnique, Institut Polytechnique de Paris
Laboratoire d'informatique de l'École polytechnique (LIX, UMR 7161)
1, rue Honoré d'Estienne d'Orves
Bâtiment Alan Turing, CS35003
91120 Palaiseau, France

[a]. *Email:* vdhoeven@lix.polytechnique.fr
[b]. *Email:* gleb.pogudin@polytechnique.edu

May 11, 2021

One fundamental problem in symbolic computation is zero testing of expressions that involve special functions. Several such zero tests have been designed for the case when such special functions satisfy algebraic differential equations or linear difference equations. In this paper, we present an algorithm for the case of power series solutions to certain non-linear difference equations.

KEYWORDS: σ-algebraic power series, algorithm, zero test

A.M.S. SUBJECT CLASSIFICATION: 68W30, 34A09, 34A12

1. INTRODUCTION

How far can we push exact computations with symbolic mathematical expressions? Starting from polynomial arithmetic, efficient algorithms have been developed for computing with expressions that involve increasingly elaborate algebraic and transcendental functions. The central problem for such computations is to decide whether two expressions represent the same mathematical function or constant. This problem in turn reduces to testing whether a given expression represents zero.

One popular traditional approach for zero testing is based on "structure theorems". For instance, given a function f that is built up using algebraic functions, exponentiation, and logarithm, we may test whether $f=0$ using the Risch structure theorem [10]. Zeilberger's holonomic systems approach [12] is another popular tool for proving equalities, in the restricted setting of solutions to linear differential and difference equations. A powerful theoretical approach for computations with power series solutions to non-linear differential equations was proposed by Denef and Lipshitz in [2, 3]. Several more practical alternative algorithms have also been developed for that purpose [11, 9, 4, 6].

In this paper, we study the zero testing problem for solutions of non-linear difference equations. For such equations there are two prominent solution spaces: power series and sequences. In the latter case, there exists a zero-test for a large class of non-linear algebraic difference equations [8]. We will consider the power series case.

[*]. This article has been written using GNU $\mathrm{T_EX_{MACS}}$ [7].

In order to state our main result, we need to introduce a few notions. A *power series domain* is a K-algebra $A \subseteq K[[z]]$ with $A \ni z$ and such that A is closed under division whenever defined. We say that A is a *σ-difference power series domain* if it is also closed under the difference operator $\sigma: f \longmapsto f \circ g$ for some fixed $g = z + O(z^2) \in A$. Note that the standard shift operator $x \rightarrow x + 1$ is of this form if one considers the power series expansion at infinity, that is, $z = \frac{1}{x}$ (see Example 1). Finally, A is said to be *effective* if all these operations can be carried out through algorithms. Now assume that we are given a power series solution $f \in K[[z]]$ to the equation

$$P(f, \sigma f, \ldots, \sigma^r f) \;=\; 0. \tag{1}$$

for some non-trivial polynomial $P \in A[F, \ldots, \sigma^r F]$. Such a power series f is said to be σ-algebraic over A. A typical example is the power series part of Stirling's asymptotic expansion for the Γ-function: see section 6.1. Our main result (see section 5) is a zero-test for elements in $A[f, \sigma f, \ldots]$ under assumption $\frac{\partial P}{\partial \sigma^r F}(f) \neq 0$ (note that this assumption can be forced by differentiating P a finite number of times). In particular, this implies that $A(f, \sigma f, \ldots) \cap K[[z]]$ is again an effective σ-difference power series domain.

A similar type of zero-test was designed in [4, 6] for the case when the difference operator σ is replaced by differentiation with respect to z. We show that this approach can indeed be transposed, but there are a few subtleties. The algorithm in the differential case exploits the fact that a prime univariate differential ideal is defined by a single differential equation. In the present setting, the main difficulty is that this is not longer the case in difference algebra, so we have to work with a system of compatible difference equations (called a coherent autoreduced chain). One of the key ingredients of our algorithm, Proposition 6, is an existence result for a power series solution to such a system of difference equations.

Another feature of our algorithm is that it integrates an optimization of [6] over [4]: in order to test whether $Q(f, \ldots, \sigma^s f) = 0$ for some $Q \in A[F, \ldots, \sigma^s F]$, the number of coefficients of f that we need to evaluate only depends on s and $\deg Q$, but not on the individual coefficients of Q.

A proof-of-concept implementation of the algorithm in Julia based on the OSCAR computer algebra system is available at `https://github.com/pogudingleb/DifferenceZeroTest`.

2. REMINDERS FROM DIFFERENCE ALGEBRA

2.1. Ritt reduction

Let us start with some notions from difference algebra. Let K be a field of characteristic zero. A *K-difference algebra* is a K-algebra A together with an injective morphism $\sigma: A \rightarrow A$ of K-algebras. In what follows, we will always assume that A is also an integral domain.

Given an indeterminate F, we denote by $A\{F\} := A[F, \sigma F, \sigma^2 F, \ldots]$ the difference ring of *difference polynomials* in F and by $A\langle F \rangle := A(F, \sigma F, \sigma^2 F, \ldots)$ its fraction field. The algebraic variables $F, \sigma F, \sigma^2 F, \ldots$ are naturally ordered by $\sigma^i F \preccurlyeq \sigma^j F \Longleftrightarrow i \leqslant j$.

For a difference polynomial $P \in A\{F\} \setminus A$, the *leader* ℓ_P of P is the largest variable $\sigma^r F$ that occurs in P, and we set $\operatorname{ord} P := r$. We write $P = P_d \, \ell_P^d + \cdots + P_0$ with $P_0, \ldots, P_d \in A[F, \ldots, \sigma^{r-1} F]$ and $P_d \neq 0$ and define:

- $I_P := P_d$, the *initial* of P;

- $S_P := \partial P / \partial \ell_P$, the *separant* of P;
- $\ell_P^* := \ell_P^d$, the *extended leader* of P;
- $\operatorname{rank} P := (\ell_P, d)$, the *Ritt rank* of P.

It is convenient to further extend the definition of Ritt rank by setting $\operatorname{rank} P := (-\infty, -\infty)$ for polynomials $P \in A$. We finally define a total ordering $\leqslant$ and a partial ordering $\preccurlyeq$ on Ritt ranks by

$$\begin{aligned}(\ell_P, d_P) &\leqslant (\ell_Q, d_Q) \iff (\ell_P \prec \ell_Q \vee (\ell_P = \ell_Q \wedge d_P \leqslant d_Q))\\ (\ell_P, d_P) &\preccurlyeq (\ell_Q, d_Q) \iff (\ell_P \preccurlyeq \ell_Q \wedge d_P \leqslant d_Q).\end{aligned}$$

A list of difference polynomials $Q_1,\ldots,Q_l$ such that $\operatorname{rank} Q_1 \leqslant \cdots \leqslant \operatorname{rank} Q_l$ is called a *chain*.

Given $P \in A\{F\} \setminus A$, we say that P is *ℓ-reducible* with respect to a chain $Q_1,\ldots,Q_l$ if there exists an i with $\operatorname{rank} Q_i \preccurlyeq \operatorname{rank} P$. For $P, Q \in A\{F\}$ such that $Q \notin A$, we define the *ℓ-remainder* of P with respect to Q denoted by $P \operatorname{rem} Q$ as follows:

1. If P is not ℓ-reducible with respect to Q, we set $P \operatorname{rem} Q := P$;
2. Let P' be the remainder of the Euclidean pseudo-division of P by $\sigma^{\operatorname{ord} P - \operatorname{ord} Q} Q$ as univariate polynomials in ℓ_P. We set $P \operatorname{rem} Q := P' \operatorname{rem} Q$.

For a chain $Q_1,\ldots,Q_l \in A\{F\} \setminus A$, we define

$$P \operatorname{rem} (Q_1,\ldots,Q_l) := (((P \operatorname{rem} Q_l) \operatorname{rem} Q_{l-1}) \cdots) \operatorname{rem} Q_1.$$

If $P \operatorname{rem} (Q_1,\ldots,Q_l) = 0$, we say that P is *ℓ-reduced to zero* with respect to $Q_1,\ldots,Q_l$.

Let us now consider $P, Q \in A\{F\} \setminus A$ such that $\operatorname{rank} P$ and $\operatorname{rank} Q$ are incomparable for $\preccurlyeq$. So either $\ell_P \prec \ell_Q$ and $d_P > d_Q$, or $\ell_P \succ \ell_Q$ and $d_P < d_Q$. If $\ell_P = \sigma^i F \prec \ell_Q = \sigma^j F$, then we define the *$\Delta$-polynomial* of P and Q by

$$\Delta_{P,Q} := (\sigma^{j-i} I_P)\, \ell_Q^{d_P - d_Q} Q - I_Q \sigma^{j-i} P.$$

If $\ell_P \succ \ell_Q$, then we define $\Delta_{P,Q} := -\Delta_{Q,P}$.

We say that the chain $Q_1,\ldots,Q_l$ is *ℓ-autoreduced* if Q_i is ℓ-reduced with respect to $Q_1,\ldots, Q_{i-1}, Q_{i+1},\ldots,Q_l$ for each i. We say that $Q_1,\ldots,Q_l$ is *coherent* if $\Delta_{Q_i,Q_j} \operatorname{rem} (Q_1,\ldots,Q_l) = 0$ for all $i \neq j$ such that $\operatorname{rank} Q_i$ and $\operatorname{rank} Q_j$ are incomparable for $\preccurlyeq$.

2.2. Differential polynomials with power series coefficients

Consider a power series $g = z + g_\kappa z^\kappa + g_{\kappa+1} z^{\kappa+1} + \cdots$ with $g_\kappa \neq 0$ and $\kappa \geqslant 2$. Then we may define an injective homomorphism $\sigma: K[[z]] \longrightarrow K[[z]]$ of K-algebras by

$$\sigma(f(z)) = f(g(z)),$$

so $K[[z]]$ is a difference K-algebra with respect to the mapping σ. From now on, we will assume that A is a difference subalgebra of $K[[z]]$ for σ (in particular, A is closed under σ). In addition, we assume that $f z^{-1} \in A$ whenever $f \in zA$. This allows us to define a second operator

$$\delta := \frac{\sigma - 1}{z^{\kappa-1}}$$

on A and we note that any operator in $A[\sigma]$ can be rewritten as an operator in $A[\delta]$ by substituting $1 + z^{\kappa-1}\delta$ for σ.

Example 1. For an infinitely large variable x, the shift operator $\sigma: \varphi(x) \longmapsto \varphi(x+1)$ can be regarded as an injective homomorphism of $\mathbb{K}[[x^{-1}]]$ into itself. Setting $z = x^{-1}$, this operator corresponds to the operator $\sigma: f(z) \longmapsto f\left(\frac{z}{1+z}\right)$ on $\mathbb{K}[[z]]$.

The corresponding operator δ in this case will be $\delta: f(z) \rightarrow \frac{1}{z}\left(f\left(\frac{z}{1+z}\right) - f(z)\right)$. The conversion between $A[\sigma]$ and $A[\delta]$ can be performed by formulas

$$\sigma(f) = z\delta(f) + f, \quad \sigma^2(f) = \frac{z^2}{1+z}\delta^2(f) + \frac{z(2+z)}{1+z}\delta(f) + f.$$

For example, the operator $P := (1+2z)\,\sigma^2(f) - f$ can be written as

$$P = \frac{z^2(1+2z)}{1+z}\delta^2(f) + \frac{z(2+z)(1+2z)}{1+z}\delta(f) + 2zf$$

Given $f = \sum_{i \in \mathbb{N}} f_i z^i \in A$, we will denote by $v(f) \in \mathbb{N} \cup \{\infty\}$ its valuation in z. We extend this valuation to difference polynomials in $A\{F\}$ so that $v(P)$ is the minimum of the valuation of the non-zero coefficients of P if $P \neq 0$ and ∞ otherwise. The advantage of using the operator δ instead of σ is that $v(\delta f) = v(f)$ for all $f \in zA$. More generally, assume that $P = P_{[0]}F + \cdots + P_{[r]}\delta^r F \in AF + \cdots + A\delta^r F$ is a linear difference polynomial of order r. For each $i \in \{0, \ldots, r\}$, we have $P_{[i]} = \sum_{j \in \mathbb{N}} (P_{[i]})_j z^j$. Let $v(P) := \min(v(P_{[0]}), \ldots, v(P_{[r]}))$. Then, for any $f \in K[[z]]$, we have

$$v(P(f)) \geqslant v(P) + v(f).$$

Furthermore, the coefficient in front of $z^{v(P)+v(f)}$ in $P(f)$ can be written as

$$P(f)_{v(P)_{v(f)}} = J_P(v(f))\, f_{v(f)}, \tag{2}$$

where $J_P(n)$ is the *indicial polynomial* of P defined by

$$J_P(n) := \sum_{i=1}^{r} (P_{[i]})_{v(P)}\,(g_\kappa n)^i.$$

In particular, whenever $J_P(v(f)) \neq 0$, we have $v(P(f)) = v(P) + v(f)$, so P does not vanish at f. We will denote by Z_P the largest root of J_P in $\mathbb{N}$, while taking $Z_P = -1$ if no such root exists. This number will be an upper bound for the valuation of a power series solutions of $P = 0$.

Example 2. (Continuation of Example 1) Consider the operator P from Example 1. We have $v(P_{[0]}) = 1, v(P_{[1]}) = 1, v(P_{[2]}) = 2$, so $v(P) = 1$. Then the indicial polynomial will be $J_P(n) = -2 - 2n$, so we have $Z_P = 1$. This implies that the valuation of every power series solution of $P = 0$ must be equal to one. Note that there is a solution $f = z$ with $v(f) = 1$.

Given a general difference polynomial $P \in A\{F\}$ and a "point" $f \in A$, the unique difference polynomial $P_{+f} \in A\{F\}$ such that

$$P_{+f}(g) = P(f+g)$$

for all $g \in A$ is called the *additive conjugate* of P by f. This transformation can be thought as shifting the "origin" to f.

For every difference polynomial $P \in A\{F\}$ and $i \in \mathbb{N}$, we define P_i to be the homogeneous component of degree i in $F, \delta F, \ldots$. If P has total degree d, then $P = P_0 + \cdots + P_d$ is the decomposition of P into homogeneous parts. Given $f \in A$, we will use $P_{+f,1}$ as an abbreviation for $(P_{+f})_1$.

2.3. Logarithmic power series

In order to ensure the existence of solutions to certain difference equations, it is convenient to also 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 $f_i = f_{i,\deg f_i} (\log z)^{\deg f_i} + \cdots + f_{i,0}$. Note that, for every $p \in K[t]$ and $i \in \mathbb{N}$, we have

$$\delta(p(\log z)\, z^i) \;=\; g_k(p'(\log z) + i p(\log z))\, z^i + O(z^{i+1}).$$

This allows us to generalize (2) to the case when $f \in K[\log z][[z]]$ and $P \in K[\log z][[z]]\{F\}$ is a homogeneous linear differential polynomial:

$$P(f)_{v(P)+v(f)} \;=\; J_P(v(f) + \delta)\, f_{v(f)}, \tag{3}$$

where δ acts on $K[\log z]$ as the derivation with respect to $\log z$.

3. σ-ALGEBRAIC POWER SERIES

3.1. Univariate σ-algebraic power series

Let K be a field of characteristic zero. Let $A \subseteq K[[z]]$ be a σ-difference K-subalgebra of $K[[z]]$ with corresponding shift operator δ. Assume furthermore 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 call such an algebra A a *σ-difference power series domain*. A series $f \in K[[z]]$ is said to be *σ-algebraic* over A if it satisfies a non-trivial difference equation $P(f) = 0$ with $P \in A\{F\} \setminus A$.

Assume now that A is an effective power series domain. The most obvious way to effectively represent a σ-algebraic power series over A 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 say that the annihilator P is *non-degenerate* if $S_P(f) \neq 0$.

3.2. Root separation bounds

Let $f \in K[[z]]$ be σ-algebraic over A with annihilator $P \in A\{F\} \setminus A$. Assume that there exists a number $s \in \mathbb{N}$ such that for any $\tilde{f} \in K[[z]] \setminus \{f\}$ with $v(\tilde{f} - f) \geqslant s$, we have $P(\tilde{f}) \neq 0$. Then we define $s_{P,f}$ to be the smallest such number s and call it the *root separation* of P at f. It corresponds to the number of initial conditions that should be known in order to determine f in a unique way as a root of P.

PROPOSITION 3. *Assume that f is σ-algebraic over A with a non-degenerate annihilator $P \in A\{F\} \setminus A$. Then the following root separation bound holds:*

$$s_{P,f} \;\leqslant\; \max(v(P_{+f,1}), Z_{P_{+f,1}}) + 1. \tag{4}$$

Proof. Since S_P does not vanish at f, we have $P_{+f,1} \neq 0$. Let $\mu := v(P_{+f,1}) \geqslant v(P_{+f})$. Given $\tilde{f} = f + \varepsilon \in K[[z]]$ with $n = v(\varepsilon) < \infty$, we have

$$[P_{+f,1}(\varepsilon)]_{\mu+n} \;=\; J_{P_{+f,1}}(n)\, \varepsilon_n. \tag{5}$$

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

$$v(P_{+f,>1}(\varepsilon)) \;\geqslant\; 2n \;>\; \mu + n,$$

whence

$$[P(\tilde{f})]_{\mu+n} \;=\; J_{P_{+f,1}}(n)\, \varepsilon_n.$$

Since $n > Z_{P_{+f,1}}$, we also get $J_{P_{+f,1}}(n) \neq 0$, which entails $P(\tilde{f}) \neq 0$. □

What we will really need is a stronger version of Proposition 3 that also takes care of logarithmic power series solutions. Assume that there exists a number $s \in \mathbb{N}$ such that for any $\tilde{f} \in K[\log z][[z]] \setminus \{f\}$ with $v(\tilde{f} - f) \geqslant s$, we have $P(\tilde{f}) \neq 0$. Then we define $s_{P,f}^{*}$ to be the smallest such number s and call it the *strong root separation* of P at f.

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

$$s_{P,f}^{*} \leqslant \max(v(P_{+f,1}), Z_{P_{+f,1}}) + 1. \tag{6}$$

Proof. The proof is similar to the proof of Proposition 3 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

$$[P_{+f,1}(\varepsilon)]_{\mu+n} = J_{P_{+f,1}}(n)\, \varepsilon_{n,k} (\log z)^k + O((\log z)^{k-1}) \tag{7}$$

instead of (5), and where $O((\log z)^{k-1})$ stands for a polynomial of degree at most $k-1$ in $K[\log z]$. □

Note that in the both propositions above, the non-degeneracy of the annihilator implies that $P_{+f,1} \neq 0$, so the provided bounds are always finite.

3.3. Existence of logarithmic power series solutions

The following proposition also provides us with a partial converse of Proposition 4.

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

Proof. $S_P(f) \neq 0$ implies that $P_{+f,1} \neq 0$. Let $\mu = v(P_{+f,1}) < s$. We have to show the existence of a unique series $\varepsilon \in K[\log z][[z]]$ with $v(\varepsilon) > s$ and $P_{+f}(\varepsilon) = 0$. We may decompose

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

Extracting the coefficient of $z^{\mu+n}$ in the relation $\mathrm{H}(\varepsilon) = \Delta(\varepsilon)$ now yields (similarly to (3))

$$J_{\mathrm{H}}(n + \vartheta)\, \varepsilon_n = \Delta(\varepsilon)_{\mu+n}. \tag{8}$$

For all $n > \sigma$, the right hand side $\Delta(\varepsilon)_{\mu+n}$ only depends on $\varepsilon_0, \ldots, \varepsilon_{n-1}$, and $J_H(n + \vartheta) \in K[\vartheta]$ is a non-zero differential operator with $\vartheta(\log z) = 1$. Then [6, Proposition 1] implies that the equation $J_H(n + \vartheta)\, \varepsilon_n = g$ has a solution in $K[\log z]$ for any $g \in K[\log z]$. Therefore, there exists a solution ε to the equation $P(f + \varepsilon) = 0$. □

4. EXISTENCE OF SOLUTIONS FOR COHERENT AUTOREDUCED SETS

PROPOSITION 6. *Let $Q_1, Q_2, \ldots, Q_n$ be a coherent ℓ-autoreduced chain in $K\{F\}$. For every $1 \leqslant i \leqslant n$, denote $r_i := \operatorname{ord} Q_i$ and $d_i := \deg_{\ell_{Q_i}} Q_i$, and assume $r_1 < r_2 < \cdots < r_n$. Let $f \in K[\log z][[z]]$ be a logarithmic power series and let $s \in \mathbb{N}$ be such that*

- $Q_1(f) = 0$;

- $v(Q_i(f)) > s$, *for* $i = 2, \ldots, n$;
- $s > \max\limits_{2 \leqslant i \leqslant n} ((d_{i-1} - d_i + 1)\, v(I_{Q_i}(f)) + v(S_{Q_{i-1}}(f)))$.

Then $Q_2(f) = \cdots = Q_n(f) = 0$.

Proof. Let us prove by induction that $Q_i(f) = 0$ for $i = 1, \ldots, n$. The base case $i = 1$ is already given. Assume that $i > 1$. Since $Q_1, \ldots, Q_n$ is ℓ-autoreduced, the ℓ-reduction of $\Delta_{Q_i, Q_{i-1}}$ with respect to $Q_1, \ldots, Q_n$ vanishes. Since the leader of $\Delta_{Q_i, Q_{i-1}}$ is at most $X := \sigma^{r_i} F$, the polynomial $\Delta_{Q_i, Q_{i-1}}$ also ℓ-reduces to zero with respect to $Q_1, \ldots, Q_i$. Setting $k := \deg_X \Delta_{Q_i, Q_{i-1}} < d_{i-1}$, the ℓ-reduction of $\Delta_{Q_i, Q_{i-1}}$ with respect to Q_i therefore yields a relation

$$I_{Q_i}^{k - d_i + 1} \Delta_{Q_i, Q_{i-1}} = A\, Q_i + B,$$

where $\deg_X B < d_i$ and the ℓ-reduction of B with respect to $Q_1, \ldots, Q_{i-1}$ is zero. Since $\deg_X B < d_i$ and $d_j > d_i$ for all $j < i$, we actually must have $\deg_X B = 0$. Writing $R := \sigma^{r_i - r_{i-1}} Q_{i-1}$, so that

$$I_{Q_i} R = \Delta_{Q_i, Q_{i-1}} + \sigma^{r_i - r_{i-1}}(I_{Q_{i-1}})\, X^{d_{i-1} - d_i} Q_i.$$

we have

$$\begin{aligned} I_{Q_i}^{d_{i-1} - d_i + 1} R &= I_{Q_i}^{d_{i-1} - d_i} \Delta_{Q_i, Q_{i-1}} + I_{Q_i}^{d_{i-1} - d_i} \sigma^{r_i - r_{i-1}}(I_{Q_{i-1}})\, X^{d_{i-1} - d_i} Q_i \\ &= (I_{Q_i}^{d_{i-1} - (k+1)} A + I_{Q_i}^{d_{i-1} - d_i} \sigma^{r_i - r_{i-1}}(I_{Q_{i-1}})\, X^{d_{i-1} - d_i})\, Q_i + I_{Q_i}^{d_{i-1} - (k+1)} B. \end{aligned}$$

This yields a new relation of the form

$$I_{Q_i}^{d_{i-1} - d_i + 1} R = C\, Q_i + D, \tag{9}$$

where $\deg_X D = 0$. Differentiating this relation with respect to X yields

$$I_{Q_i}^{d_{i-1} - d_i + 1} \sigma^{r_i - r_{i-1}}(S_{Q_{i-1}}) = C'\, Q_i + C\, S_{Q_i}.$$

Now we evaluate this relation at f and compute the valuations of both sides. This yields

$$s > v(I_{Q_i}^{d_{i-1} - d_i + 1}(f)\, S_{Q_{i-1}}(f)) = v(C'(f)\, Q_i(f) + C(f)\, S_{Q_i}(f))$$

Since $v(Q_i(f)) > s$, we deduce $C(f)\, S_{Q_i}(f) \neq 0$, whence $C(f) \neq 0$. Since the ℓ-reduction of B with respect to $Q_1, \ldots, Q_{i-1}$ vanishes and $I_{Q_j}(f) \neq 0$ for all $j < i$, we have $B(f) = 0$ and $D(f) = 0$. Evaluating (9) at f, we conclude that $C(f)\, Q_i(f) = 0$ and therefore $Q_i(f) = 0$. □

5. AN 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 call K an *effective diophantine field* if all positive integer roots of polynomials over K can be determined by an algorithm. In particular, this means that K has 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 is said to be *effective*, if its elements are all effective power series and if the difference K-algebra operations can be carried out by algorithms. We notice that the difference K-algebra $K[[z]]^{\mathrm{com}}$ of all computable series is effective, although it does not have 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 σ-algebraic power series $f \in K[[z]]$ and an annihilator $P \in A\{F\} \setminus A$ for f. Assume finally that the annihilator P is non-degenerate, that is, $S_P(f) \neq 0$. In this case, $P_{+f,1} \neq 0$, so 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 (4) from Proposition 3 provides us with an effective upper bound for $s_{P,f}$. Proposition 4 also yields an upper bound for $s^*_{P,f}$.

Given difference polynomials $Q_1, \ldots, Q_n \in A\{F\}$, we will now give an algorithm **ZeroTest** for testing whether $Q_1, \ldots, Q_n$ simultaneously vanish at f. In particular, this will show that the A-algebra $A\langle f \rangle \cap K[[z]]$ is again an effective power series domain.

Algorithm ZeroTest$_{f,P}$($Q_1, \ldots, Q_n$)

INPUT: $Q_1, \ldots, Q_n \in A\{F\} \setminus \{0\}$

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

PARAMETERS: a computable $f \in K[[z]]$ with non-degenerate annihilator $P \in A\{F\} \setminus A$

```
 1 If $\{Q_1, \ldots, Q_n\} \cap A \neq \emptyset$, then return **false**
 2 Let $R_1, \ldots, R_r$ be an $\ell$-autoreduced chain consisting of elements of minimal Ritt
   rank in $\{Q_1, \ldots, Q_n\}$, and take this chain to be of maximal length
 3 For $i = 1, \ldots, r$ and $S \in \{I_{R_i}, S_{R_i}\}$:
 4     $S := S$ rem $(R_1, \ldots, R_r)$
 5     If $S \neq 0$, then
 6         If **ZeroTest**$_{f,P}(S, Q_1, \ldots, Q_n)$, then return **true**
 7         Expand $S(f), Q_1(f), \ldots, Q_n(f)$ until a non-zero coefficient is found
 8         If this coefficient comes from one of the $Q_i$, then return **false**
 9 For $Q \in \{Q_1, \ldots, Q_n, P\}$:
10     If $T := Q$ rem $(R_1, \ldots, R_r) \neq 0$, then return **ZeroTest**$_{f,P}(T, Q_1, \ldots, Q_n)$
11 For $2 \leqslant i \leqslant r$:
12     If $T := \Delta_{R_{i-1}, R_i}$ rem $(R_1, \ldots, R_i) \neq 0$, then return **ZeroTest**$_{f,P}(T, Q_1, \ldots, Q_n)$
13 Let $s_0 := \max_{2 \leqslant i \leqslant r} ((\deg_{\ell_{i-1}} R_{i-1} - \deg_{\ell_i} R_i + 1)\, v(I_{R_i}(f)) + v(S_{R_{i-1}}(f)))$
14 Let $s := \max(s_0, v(P_{+f,1}), Z_{P_{+f,1}}, v(R_{+f,1})) + 1$, where $R := R_1$
15 Return the result of the test $\min(v(R_1(f)), \ldots, v(R_r(f))) > 2s$
```

Remark 7. Obviously, the last test in step 15 requires the computation of at most $2s + 1$ coefficients of the series $R_1(f), \ldots, R_r(f)$. Such power series expansions can be done efficiently using relaxed power series arithmetic [5].

THEOREM 8. *The algorithm* **ZeroTest** *is correct and terminates.*

Proof. Let us first prove that the algorithm always terminates. To each input $Q_1, ..., Q_n$, we assign the tuple with the Ritt ranks of $R_1, \ldots, R_r$. We order such tuples lexicographically, and this ordering is well-founded. Then the assigned tuple strictly decreases for this ordering during any recursive call. This shows that our algorithm always terminates.

In step 1, note that we assumed that $Q_i \neq 0$ as an element of $A\{F\}$ for all i. So if $Q_i \in A$, then we indeed have $Q_i(f) = Q_i \neq 0$. The correctness of the algorithm is also clear if we return during one of the steps 6, 8, 10, or 12.

Assume now that we reach step 15. By construction, this means that $I_{R_i}(f)\, S_{R_i}(f) \neq 0$ for every $1 \leqslant i \leqslant r$ and Q rem $(R_1, \ldots, R_r) = 0$ for every $Q \in \{Q_1, \ldots, Q_n, P\}$. Furthermore, since we passed step 11, the chain $R_1, \ldots, R_r$ is both coherent and ℓ-autoreduced.

Applying Proposition 5, we obtain a unique logarithmic power series $\tilde{f} \in K[\log z][[z]]$ with $R_1(\tilde{f}) = 0$ and $v(\tilde{f} - f) > s$. Since $s \geqslant s_0$, Proposition 6 implies that $R_2(\tilde{f}) = R_3(\tilde{f}) = \cdots = R_r(\tilde{f}) = 0$. Since each of $Q_1, \ldots, Q_n, P$ is ℓ-reducible to zero with respect to $R_1, \ldots, R_r$ and none of the initials of $R_1, \ldots, R_r$ vanishes at $\tilde{f}$, we deduce that $Q_1(\tilde{f}) = \cdots = Q_n(\tilde{f}) = P(\tilde{f}) = 0$. Proposition 4 applied to P and its roots f and $\tilde{f}$ implies that $f = \tilde{f}$ whenever the test succeeds, so the returned result is correct. □

Remark 9. One interesting aspect of the improved zero test is that it still works if Q depends on parameters $\lambda_1,\ldots,\lambda_l$ in K (when using the technique of dynamic evaluation [1] for examining the finite number of branches that can occur depending on algebraic conditions on the parameters). The original equation P may also depend on parameters, as long as we have a uniform bound for $Z_{P_{+f,1}}$.

6. EXAMPLES

6.1. Stirling's series

Consider Stirling's series

$$\log n! = \log \Gamma(n+1) = n \log n - n + \frac{1}{2} \log (2\pi n) + \sum_{k \geqslant 1} \frac{S_k}{n^k}.$$

Rewritten in terms of $z = \frac{1}{n}$, the rightmost series $S(z) := \sum_{k \in \mathbb{N}} S_k z^k$ satisfies

$$z\sigma(S) - zS - z + \left(1 + \frac{z}{2}\right) \log(1+z) = 0,$$

where $\sigma: f(z) \mapsto f\left(\frac{z}{1+z}\right)$. The coefficients of this difference equation belong to

$$\begin{aligned} A &= \mathbb{Q}\{z, \log(1+z)\} \\ &= \mathbb{Q}\left(z, \log(1+z), \log\left(1 + \frac{z}{1+z}\right), \log\left(1 + \frac{z}{2+z}\right), \ldots\right), \end{aligned}$$

where we note that $\log(1+z)$ is σ-transcendental over $\mathbb{Q}(z)$. In particular, A comes with a natural zero test and our algorithm yields a zero test for $A\{S\}$.

One can perform the same computations for functions of the form $\Gamma(\alpha n + \beta)$. Having a zero test for expressions involving the corresponding Stirling series can be used to prove identities for the gamma function, for example, to formally establish the Legendre duplication formula:

$$\Gamma(n)\Gamma\left(n + \frac{1}{2}\right) = 2^{1-2n} \sqrt{\pi}\, \Gamma(2n). \tag{10}$$

In order to do this, we inductively construct a zero test for the σ-ring

$$\mathbb{Q}\left\{z, \log(1+z), \log\left(1 + \frac{z}{1+z/2}\right), \log\left(1 + \frac{z}{2}\right), S(z), S\left(\frac{z}{1+z/2}\right), S\left(\frac{z}{2}\right)\right\}$$

and then test whether the following expression is zero:

$$z\left(S\left(\frac{z}{2}\right) - S(z) - S\left(\frac{z}{1+z/2}\right)\right) - \log\left(1 + \frac{z}{2}\right) + \frac{z}{2}.$$

Our implementation allows to do this; the details can be found in the notebook `https://github.com/pogudingleb/DifferenceZeroTest/blob/main/examples/LegendreDuplication.ipynb`.

Note that, althought the identity (10) can be proved for integer values of n using the algorithms for P-recursive sequences, we are not aware of an existing symbolic computation algorithm that could be used to verify this identity automatically.

6.2. Mixing differential and difference extensions

The example from the previous subsection required the incorporation of logarithms in our base ring A. Such logarithms are usually construed as solutions to differential equations. In fact, it is possible to alternate the adjunction of solutions to differential equations to our base ring A with the adjunction solutions to difference equations, while preserving our ability to do zero testing. Let us briefly explain how this works.

Assume that $A \ni z$ is an effective power series domain that is closed under both $\sigma: \varphi \mapsto \varphi \circ g$ and differentiation $\partial = \partial / \partial z$. Given a σ-algebraic power series f over A, we have seen that $A_0 = A(f, \sigma f, \ldots) \cap \mathbb{K}[[z]]$ is an effective power series domain that is closed under σ. Moreover, there is a polynomial $P \in A[F, \ldots, \sigma^r F]$ with $P(f, \ldots, \sigma^r f) = 0$. Differentiating this equation, we get

$$\frac{\partial P}{\partial F}(f, \ldots, \sigma^r f)\, f' + \cdots + \frac{\partial P}{\partial\, (\sigma^r F)}(f, \ldots, \sigma^r f)\, (\sigma^r(z))'\, \sigma^r(f') \; = \; 0,$$

so ∂f is σ-algebraic over A_0. Consequently, $A_1 = A_0(f', \sigma f', \ldots) \cap \mathbb{K}[[z]]$ is an effective power series domain that is closed under σ. By induction, we obtain a sequence $(A_n)_{n \in \mathbb{N}}$ of effective power series domains with $A_n = A_{n-1}(f^{(n)}, \sigma f^{(n)}, \ldots) \cap \mathbb{K}[[z]]$ and such that each A_n is closed under σ. We conclude that $A_\infty = A_0 \cup A_1 \cup \cdots \ni f$ is an effective power series domain that is closed under both σ and ∂.

In a similar way, given a d-algebraic power series f over A, and in view of the algorithm from [4], we may construct a sequence $(A_n)_{n \in \mathbb{N}}$ of effective power series domains that are closed under ∂, with $A_0 = A(f, f', \ldots) \cap \mathbb{K}[[z]]$ and $A_n = A_{n-1}(\sigma^n f, \sigma^n f', \ldots) \cap \mathbb{K}[[z]]$. Then $A_\infty = A_0 \cup A_1 \cup \cdots \ni f$ is an effective power series domain that is closed both under σ and ∂.

6.3. Barnes G-function and the log-gamma integral

The Barnes G-function is a solution of the difference equation

$$G(n+1) \; = \; \Gamma(n)\, G(n)$$

and the log-gamma integral is defined by

$$\Lambda(n) \; := \; \int_0^n \log \Gamma(x)\, \mathrm{d}x.$$

These functions are related via

$$\Lambda(n) \; = \; \frac{n\,(1-n)}{2} + \frac{n}{2} \log\,(2\,\pi) + n \log \Gamma(n) - \log G(1+n).$$

In view of subsection 6.2, such relations can be proved automatically using our algorithm in combination with the zero test from [4]. Alternatively, we may derive a difference equation for Λ:

$$\begin{aligned} \Lambda(n+1) \; &= \; \int_0^1 \log \Gamma(x)\, \mathrm{d}x + \int_0^n \log \Gamma(x+1)\, \mathrm{d}x \\ &= \; \int_0^1 \log \Gamma(x)\, \mathrm{d}x + \int_0^n (\log x + \Gamma(x))\, \mathrm{d}x \\ &= \; \Lambda(n) + n \log n - n + \Lambda(1). \end{aligned}$$

After rewriting G and Λ in terms of z, we may then directly use our new algorithm. Our implementation allows to do this; the details can be found in the notebook `https://github.com/pogudingleb/DifferenceZeroTest/blob/main/examples/LoggammaIntegral.ipynb`.

Acknowledgements

The authors would like to thank the referees for helpful comments and suggestions. Gleb Pogudin was partially supported NSF grants DMS-1853482, DMS-1760448, DMS-1853650, CCF-1564132, and CCF-1563942 and by the Paris Ile-de-France region.

BIBLIOGRAPHY

[1] 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.

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

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

[4] 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.

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

[6] J. van der Hoeven. Computing with D-algebraic power series. *AAECC*, 30(1):17–49, 2019.

[7] J. van der Hoeven. *The Jolly Writer. Your Guide to GNU TeXmacs*. Scypress, 2020.

[8] Manuel Kauers. An algorithm for deciding zero-equivalence of nested polynomially recurrent sequences. *ACM Transactions on Algorithms*, 2007.

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

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

[11] 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.

[12] D. Zeilberger. A holonomic systems approach to special functions identities. *Journal of Comp. and Appl. Math.*, 32:321–368, 1990.