Fast Algorithms for Discrete Differential Equations

Alin Bostan
Inria
Palaiseau, France
alin.bostan@inria.fr

Hadrien Notarantonio
Inria
Palaiseau, France
hadrien.notarantonio@inria.fr

Mohab Safey El Din
Sorbonne Université
Paris, France
mohab.safey@lip6.fr

ABSTRACT

Discrete Differential Equations (DDEs) are functional equations that relate algebraically a power series $F(t,u)$ in t with polynomial coefficients in a "catalytic" variable u and the specializations, say at $u = 1$, of $F(t,u)$ and of some of its partial derivatives in u. DDEs occur frequently in combinatorics, especially in map enumeration. If a DDE is of fixed-point type then its solution $F(t,u)$ is unique, and a general result by Popescu (1986) implies that $F(t,u)$ is an algebraic power series. Constructive proofs of algebraicity for solutions of fixed-point type DDEs were proposed in 2006 by Bousquet-Mélou and Jehanne. Last year, Bostan et al. initiated a systematic algorithmic study of such DDEs of order 1. We generalize this study to DDEs of arbitrary order. First, we propose nontrivial extensions of algorithms based on polynomial elimination and on the guess-and-prove paradigm. Second, we design two brand-new algorithms that exploit the special structure of the underlying polynomial systems. Last, but not least, we report on implementations that are able to solve highly challenging DDEs with a combinatorial origin.

CCS CONCEPTS

• **Computing methodologies → Algebraic algorithms**.

KEYWORDS

Functional equations; Discrete differential equations; Algorithms; Complexity; Catalytic variables; Algebraic functions.

1 INTRODUCTION

Context and motivation. Enumerative combinatorics contains a vast landscape of nontrivial counting problems that can hardly be solved without introducing the associated generating functions [1]. Setting up and solving a functional equation for such a generating function generally makes it possible to deduce properties of the discrete objects of interest (e.g. closed formulas [21, p. 104] and asymptotic behaviors [24, p. 147], [35, §5.4.5]). Among these problems, many require refining the initial enumeration in order to more easily write a functional equation [15, 16, 38]. Algebraically, this process amounts to introducing an additional variable, called *catalytic* [40].

The so-obtained functional equation with one catalytic variable usually relates the refined generating function to its specializations with respect to the catalytic variable, one of these specializations being the generating function of the initial enumeration problem. A standard way to deduce combinatorial properties from the functional equation is first to determine the nature of the generating function [37, Chapter 6] (e.g. rational, algebraic, D-finite, ...), then to compute a witness (e.g. an annihilating polynomial or an annihilating linear differential equation, ...).

A typical example. One enumeration problem consists in studying bicolored maps (black, white) such that the degree of each black face is 3 and the degree of each white face is a multiple of 3. Such objects are called 3-*constellations* [11, Fig. 6]; they have been enumerated via a bijective approach in [13]. Let us define a_n as the number of 3-constellations with n black faces. We consider the refined sequence $a_{n,d}$ as the number of 3-constellations having n black faces and outer degree $3d$. Let $F(t,u) = \sum_{n,d\geq 0} a_{n,d} u^d t^n \in \mathbb{Q}[u][[t]]$ be its generating function[1]. The catalytic variable is u and the specialization $F(t,1)$ is the generating function of the sequence $(a_n)_{n\geq 0}$. Using a classical "deletion of the root edge" argument [11, Fig. 7], one gets the following functional equation with 1 catalytic variable:

$$F(t,u) = 1 + tu(2F(t,u) + F(t,1))\frac{F(t,u) - F(t,1)}{u-1} + tuF(t,u)^3 + tu\frac{F(t,u) - F(t,1) - (u-1)\partial_u F(t,1)}{(u-1)^2}. \quad (1)$$

Note that for any $a \in \mathbb{Q}$, the *divided difference operator* $\Delta_a : F \mapsto (F(t,u)-F(t,a))/(u-a)$ maps $\mathbb{Q}[u][[t]]$ to itself. As a consequence, it follows that Equation (1) admits a unique solution in $\mathbb{Q}[u][[t]]$: the first fraction is $\Delta_1 F$ while the second one is $\Delta_1^2 F \equiv \Delta_1(\Delta_1 F)$. Rewritten as $F = 1 + tu(3F - (u-1)\Delta_1 F)\Delta_1 F + tuF^3 + tu\Delta_1^2 F$, Equation (1) is a *discrete differential equation* (DDE) of order 2, since the operator Δ_1 is iterated 2 times.
Equation (1) has the property that its unique solution $F \in \mathbb{Q}[u][[t]]$ has a specialization $F(t,1)$ which is algebraic over $\mathbb{Q}(t)$. More precisely, in (1) the specialization $F(t,1) = 1+t+6t^2+54t^3+594t^4+\cdots$ is a root in z of $81t^2z^3 - 9t\,(9t-2)\,z^2 + \left(27t^2 - 66t + 1\right)z - 3t^2 + 47t - 1$.

A general algebraicity result. The algebraicity of the unique solution in $\mathbb{Q}[u][[t]]$ of (1) is in fact a consequence of the following strong and elegant result proved in 2006 by Bousquet-Mélou and Jehanne. It ensures algebraicity of solutions of the most frequent class of DDEs of arbitrary order k and with one catalytic variable, namely the class of DDEs of the fixed-point type.

Theorem 1.1. ([11, Thm. 3]) *Let $\mathbb{K}$ be a field of characteristic 0 and consider two polynomials $Q \in \mathbb{K}[x, y_1, \ldots, y_k, t, u]$ and $f \in \mathbb{K}[u]$, where $k \in \mathbb{N} \setminus \{0\}$. Let $a \in \mathbb{K}$ and $\Delta_a : \mathbb{K}[u][[t]] \to \mathbb{K}[u][[t]]$ be the divided difference operator $\Delta_a F(t,u) := (F(t,u)-F(t,a))/(u-a)$. Let us denote by Δ_a^i the operator obtained by iterating i times Δ_a. Then, there exists a unique solution $F \in \mathbb{K}[u][[t]]$ of the equation*

$$F(t,u) = f(u) + t\,Q(F(t,u), \Delta_a F(t,u), \ldots, \Delta_a^k F(t,u), t, u), \quad (2)$$

and moreover $F(t,u)$ is algebraic over $\mathbb{K}(t,u)$.

Theorem 1.1 has been further extended in [31] to the case of *systems of DDEs* of the form (2) with 1 catalytic variable. In fact, the algebraicity results proved in [11, 31] are particular cases of a

[1] $F(t,u)$ has polynomial coefficients in u since for a fixed number of black faces, the outer degree is finite.

much deeper and older result in commutative algebra proved by Popescu [32] in the context of Artin approximation theory with nested conditions. The strength of the approaches presented in [11, 31] lies in the effectivity of their algebraicity proofs. Despite a recent improvement in the linear case [18], Popescu's result is still not known to admit an effective proof.

Setting and main goal. In the remainder of this article, we focus only on DDEs of the form (2). Note that one can consider the associated *polynomial functional equation* obtained by multiplying (2) by the smallest power of $(u-a)$ such that the product becomes polynomial in u. This new equation is denoted by

$$P(F(t,u), F(t,a), \dots, \partial_u^{k-1} F(t,a), t, u) = 0, \tag{3}$$

for some nonzero polynomial $P \in \mathbb{K}[x, z_0, \dots, z_{k-1}, t, u]$.

Starting from (3), our main goal is to compute a nonzero $R \in \mathbb{K}[t, z_0]$ such that $R(t, F(t,a)) = 0$. Remark that setting $u = a$ in (3) yields a tautology, and that differentiating (3) with respect to t yields a sum of $k+2$ terms and introduces $k+1$ series from which nothing can be deduced, a priori. In this article, we will focus on designing systematic algorithms for solving equations such as (3).

Previous work. We use the notation $\overline{\mathbb{K}}[[t^{\frac{1}{\star}}]] \equiv \cup_{d\geq 1} \overline{\mathbb{K}}[[t^{\frac{1}{d}}]]$. For *linear* DDEs, the *kernel method* (which already appears in an exercise of Knuth's book [30, Ex. 2.2.1-4] and was systematized in [2]) consists in finding the roots $u = U(t) \in \overline{\mathbb{K}}[[t^{\frac{1}{\star}}]]$ of the coefficient in x of P. By taking the resultant with respect to u of this coefficient and of P, one obtains a polynomial relation relating $F(t,a), \dots, \partial_u^{k-1} F(t,a)$. Since the work [12] of Bousquet-Mélou and Petkovšek, the linear case can be considered as fully understood. An extension of this method to the setting where $\deg_x(P) = 2$ is also classical and is called the *quadratic method*. It first appears in Brown's work [17] for the case $k = 1$. It is based on a different elegant argument which produces a polynomial relation between these specialized series. This method was extended thirty years later on a particular family of examples by Bender and Canfield [5].

Both the kernel method and the quadratic method were generalized by the approach proposed by Bousquet-Mélou and Jehanne in [11]. Their method consists of starting from (3) and of creating more polynomial equations having a nontrivial solution with $F(t,a)$ as its $\{z_0\}$-coordinate. When this method produces as many polynomials as variables and if the induced system generates a 0-dimensional ideal, a polynomial elimination strategy performed on the polynomial system allows one to compute a nonzero element $R \in \mathbb{K}[t, z_0]$ annihilating $F(t,a)$. In the case where the system does not have the above properties, a deformation of (2) via the introduction of a parameter allows one to compute such an R.

This unified method contains however some intrinsic limitations due to the number of variables introduced when creating more polynomial equations, and to the lack of geometric interpretation of the problem. It was already mentioned in [11, §12] that the method was "lacking an efficient elimination theory for polynomial systems which (...) are highly symmetric".

A first step in the algorithmic study of DDEs has been initiated in [8] for DDEs of order 1.

Main results. In constrast with [8], the purpose of the present article is to entirely treat the challenging case of DDEs of order $k \geq 1$. In Section 2, we recall the polynomial system reduction from [11] and provide a geometric interpretation of it. In Section 3, we prove under genericity assumptions on the input DDE (3) that the algebraicity degree of $F(t,a)$ is bounded by $\delta^{3k}/k!$ (Prop. 3). Here and in all that follows, δ denotes an upper bound on the total degree of P in (3). We deduce from this bound that a nonzero annihilating polynomial of $F(t,a)$ can be computed in $\tilde{O}(\delta^{6k}(k^2\delta^{k+3}+\delta^{1.89k}/k!))$ ops. in $\mathbb{K}$ (Prop. 4). Here, and in the whole paper, the soft-O notation $\tilde{O}(\cdot)$ hides polylogarithmic factors in the argument. In Section 4, we use the upper-bound $\delta^{3k}/k!$ to generalize Prop. 2.11 in [8] and deduce a complexity estimate in $\tilde{O}(k \cdot \delta^{10.12 \cdot k}/(k-1)!^2)$ ops. in $\mathbb{K}$ (Prop. 5). In Section 5, we introduce a new algorithm based on algebraic elimination and specialization properties of Gröbner bases. In Section 6, we design one more new algorithm based on a geometric interpretation of the problem. In Section 8, we provide experimental results based on efficient implementations of Sections 3 to 6 for several DDEs coming from combinatorics. The practical gains compared to the state-of-the-art go from a few minutes to several days of computation time, and we solve the DDE related to 5-constellations ($k = 4$) using a combination of Sections 4 and 5.

Notation. We denote by $\mathbb{K}$ an effective field of characteristic 0. We write $\overline{\mathbb{K}}$ for an algebraic closure of $\mathbb{K}$, and $\mathbb{K}[t]$, $\mathbb{K}(t)$ and $\mathbb{K}[[t]]$ for, respectively, the rings of polynomials, rational functions and formal power series in t with coefficients in $\mathbb{K}$. We also use the notation $\mathbb{K}[[t^{1/\star}]] := \bigcup_{d\geq 1} \mathbb{K}[[t^{1/d}]]$ for the ring of "fractional power series", that is series of the form $\sum_{n\geq 0} u_n t^{n/d}$ for some integer $d \geq 1$. We use the convention $\partial_x f$ and alike for the partial derivative of a function f with respect to x. For p a polynomial in n variables over $\mathbb{K}$, we denote by $\mathrm{disc}_x(p)$ its discriminant with respect to a variable x, by $\deg(p)$ its total degree and by $\deg_x(p)$ its degree w.r.t. the variable x. For an ideal $I \subset \mathbb{K}[x_1, \dots, x_n]$, we denote by $V(I) = V_{\overline{\mathbb{K}}}(I)$ the affine variety, or the zero set, defined by I over $\overline{\mathbb{K}}$.

Polynomial elimination basics. We will repeatedly make use of the following fundamental results in polynomial elimination theory. For proofs and further context, we refer to [20, Chap. 3, Thm. 2, p. 122] for Fact 1(1), [20, Chap. 3, §5, Theorem 3, p. 159] for Fact 1(2), [19, Theorem 1.1] for Fact 1(3) and [19, Theorem 1.2] for Fact 1(4).

Fact 1. Let $\mathbb{K}$ be a field and let $I \subset \mathbb{K}[x_1, \dots, x_n]$ be an ideal.

(1) (Elimination theorem) Let G be a Gröbner basis of I with respect to the *lexicographic* order with $x_1 \succ \cdots \succ x_n$. Then, for any $0 \leq \ell \leq n$, the set $G_\ell = G \cap \mathbb{K}[x_{\ell+1}, \dots, x_n]$ is a Gröbner basis of the ℓ-th elimination ideal $I_\ell = I \cap \mathbb{K}[x_{\ell+1}, \dots, x_n]$.
(2) (Extension theorem) Assume that $\mathbb{K}$ is algebraically closed. Let $I = (f_1, \dots, f_s)$, with $f_i = c_i(x_2, \dots, x_n) x_1^{N_i} +$ (lower degree terms in x_1). If $(a_2, \dots, a_n) \in V(I_1) \setminus V(c_1, \dots, c_s)$, then there exists $a_1 \in \mathbb{K}$ such that $(a_1, \dots, a_n) \in V(I)$.
(3) (Eigenvalue Theorem) Assume I is zero-dimensional, let $\mathbb{A} = \mathbb{K}[x_1, \dots, x_n]/I$ and $m_f : \mathbb{A} \to \mathbb{A}$ the multiplication-by-f endomorphism of $\mathbb{A}$. Then, the eigenvalues of m_f are the values of f at the finitely many points of $V(I)$.
(4) (Stickelberger's theorem) If I is radical and under the assumptions of (3), the characteristic polynomial $\det(xI - m_f)$ of m_f is equal to $\prod_{a\in V(I)} (x - f(a))$.

Complexity basics. The algorithmic costs are estimated by counting elementary arithmetic operations $(+, -, \times, \div)$ in the base field $\mathbb{K}$ at unit cost. The notation θ refers to any feasible exponent for matrix multiplication over $\mathbb{K}$. The best current upper-bound is $\theta < 2.37188$ [22]. All classical operations on univariate polynomials of degree d in $\mathbb{K}[x]$ (multiplication, multipoint evaluation and interpolation, extended gcd, resultant, squarefree part, etc) can be performed in softly linear time $\tilde{O}(d)$. We refer to the book by von zur Gathen and Gerhard [25] for these facts and related questions.

2 FROM COMBINATORICS TO POLYNOMIALS

2.1 Solving DDEs via polynomial systems

The method of Bousquet-Mélou and Jehanne [11, Section 2] is based on the idea of creating, starting from the input equation (3), new polynomial equations inducing a polynomial system that admits a solution which has $F(t, a)$ as its z_0-coordinate.

The corresponding procedure is the following. One takes the derivative of (3) with respect to the catalytic variable u and finds

$$\partial_u F(t,u) \cdot \partial_x P(F(t,u), F(t,a), \dots, \partial_u^{k-1} F(t,a), t, u) + \partial_u P(F(t,u), F(t,a), \dots, \partial_u^{k-1} F(t,a), t, u) = 0. \tag{4}$$

Now, for any solution $u = U(t)$ in $\overline{\mathbb{K}}[[t^{\frac{1}{\star}}]] \setminus \{a\}$ of the equation

$$\partial_x P(F(t,u), F(t,a), \dots, \partial_u^{k-1} F(t,a), t, u) = 0, \tag{5}$$

one obtains by plugging $u = U(t)$ in (4) that

$$(x, z_0, \dots, z_{k-1}, u) = (F(t, U(t)), F(t,a), \dots, \partial_u^{k-1} F(t,a), U(t)) \in \overline{\mathbb{K}}[[t^{\frac{1}{\star}}]] \times \mathbb{K}[[t]] \times \cdots \times \mathbb{K}[[t]] \times \overline{\mathbb{K}}[[t^{\frac{1}{\star}}]]$$

is a solution of the following polynomial system

$$\begin{cases} P(x, z_0, \dots, z_{k-1}, t, u) = 0, \\ \partial_x P(x, z_0, \dots, z_{k-1}, t, u) = 0, \quad u \neq a. \\ \partial_u P(x, z_0, \dots, z_{k-1}, t, u) = 0, \end{cases} \tag{6}$$

Showing the existence of solutions $u = U(t)$ in $\overline{\mathbb{K}}[[t^{\frac{1}{\star}}]] \setminus \{a\}$ to (5) is generally done in combinatorics by applying [11, Theorem 2] and by computing the first terms of the solutions to show that they are not constantly equal to a. In order to avoid those checks, we make the following assumption.

Hypothesis 1: $\deg_u(\partial_x P(x, z_0, \dots, z_{k-1}, 0, u)) \geq k,$ **(H1)**

$$\partial_{y_k} Q\left(f(a), f'(a), \dots, \frac{f^{(k)}(a)}{k!}, 0, a\right) \neq 0.$$

Under **(H1)**, we show that there exist k distinct solutions u to the constraints given by (6). Note that **(H1)** holds for a generic choice of f and Q in (2).

Proposition 1. Under assumption **(H1)**, there exist k distinct solutions $U_1(t), \dots, U_k(t)$ in u to (5). Moreover, all of them are distinct from a and lie in $\mathbb{L}[[t^{\frac{1}{k}}]]$, where $\mathbb{L}/\mathbb{K}$ is a field extension of degree upper bounded by k.

Proof. By expressing equation (5) in terms of the derivatives of Q and by using the first part of **(H1)**, searching solutions $u \neq a$ of (5) is seen to be equivalent to looking for solutions $u \neq a$ of

$$(u-a)^k = t \cdot (u-a)^k \cdot \partial_x Q(F(t,u), \Delta_a F(t,u), \dots, \Delta_a^k F(t,u), t, u) + t \cdot \sum_{i=1}^{k} (u-a)^{k-i} \partial_{y_i} Q(F(t,u), \Delta_a F(t,u), \dots, \Delta_a^k F(t,u), t, u).$$

By specializing this equation at $t = 0$, it follows that the constant term of any solution in u of Eq. (5) is equal to a. Then, taking the k-th root of the previous equation yields an identity of the form $u = a + t^{\frac{1}{k}} (\alpha + X)^{\frac{1}{k}}$, where $\alpha := \partial_{y_k} Q(f(a), f'(a), \dots, \frac{1}{k!} f^{(k)}(a), 0, a) \in \mathbb{K} \setminus \{0\}$ and $X \in \mathbb{K}[[t]][[u]]$ satisfies $X(0, a) = 0$. By applying Newton's generalized binomial theorem, one expands $(\alpha + X)^{\frac{1}{k}}$ in $\mathbb{L}[[t]][[u]]$, with $\mathbb{L} = \mathbb{K}(\alpha^{\frac{1}{k}})$. By a fixed-point argument applied to $u = a + t^{\frac{1}{k}} (\alpha + X)^{\frac{1}{k}}$, the k-th roots of α induce the existence of k distinct solutions $U_1(t), \dots, U_k(t) \in \mathbb{L}[[t^{\frac{1}{k}}]] \setminus \{a\}$ in u to (5), all of them lying in $\mathbb{L}[[t^{\frac{1}{k}}]]$. □

The main idea of [11] is that the existence of the distinct solutions $U_1(t), \dots, U_k(t)$ induce distinct pairs $(F(t, U_i(t)), U_i(t)) \in \overline{\mathbb{K}}[[t^{\frac{1}{k}}]]^2$ for every $1 \leq i \leq k$. Hence the point

$$(x_1, u_1, \dots, x_k, u_k, z_0, \dots, z_{k-1}) = (F(t, U_1(t)), U_1(t), \dots, F(t, U_k(t)), U_k(t), F(t,a), \dots, \partial_u^{k-1} F(t,a)) \tag{7}$$

is a solution of the *duplicated* polynomial system

$$\forall\ 1 \leq i \leq k\ , \begin{cases} P(x_i, z_0, \dots, z_{k-1}, t, u_i) = 0, \\ \partial_x P(x_i, z_0, \dots, z_{k-1}, t, u_i) = 0, \\ \partial_u P(x_i, z_0, \dots, z_{k-1}, t, u_i) = 0, \end{cases} \tag{8}$$

defined by $3k$ equations in $3k$ variables over $\mathbb{K}(t)$. Now, to avoid the irrelevant solutions of (8), we restrict our attention to the solutions of (8) that are not solutions of $\prod_{i \neq j}(u_i - u_j) \cdot \prod_i (u_i - a) = 0$; we define diag $\in \mathbb{K}[u_1, \dots, u_k]$ as the left-hand side of this equation.

Notation 1. We write $\underline{x}$ (resp. $\underline{u}$ and $\underline{z}$) for the variables $x_1, \dots, x_k$ (resp. $u_1, \dots, u_k$ and $z_0, \dots, z_{k-1}$) and $\mathcal{I}$ for the ideal of $\mathbb{K}(t)[\underline{x}, \underline{u}, \underline{z}]$ generated by (8).

With the extra condition that diag $\neq 0$, those $3k$ equations and variables generically define a 0-dimensional ideal over $\mathbb{K}(t)$ and hence induce a finite set of solutions. For a later effective use of this finiteness, we introduce the following regularity assumption.

Hypothesis 2: The ideal $\mathcal{I}_\infty := \mathcal{I} : \text{diag}^\infty$ in $\mathbb{K}(t)[\underline{x}, \underline{u}, \underline{z}]$ **(H2)** is radical and has dimension 0 over $\mathbb{K}(t)$.

We now show that eliminating all variables in $\mathcal{I}_\infty$ except t and z_0 yields a nonzero annihilating polynomial of $F(t, a)$.

Proposition 2. Under **(H1)** and **(H2)**, if $R \in \mathcal{I}_\infty \cap \mathbb{K}[t, z_0] \setminus \{0\}$ then $R(t, F(t, a)) = 0$.

Proof. Under **(H1)**, we apply Proposition 1 to justify that the point given by (7) lies in $V(\mathcal{I})$. Now by definition of a saturated ideal, there exists $m \in \mathbb{N}$ such that $\text{diag}^m \cdot R \in \mathcal{I}$ writes as an algebraic expression in the polynomials involved in (8). Specializing this expression to the point given by (7) and using Proposition 1, the point given by (7) does not annihilate diag. Hence it annihilates R. Finally, the dimension property in **(H2)** implies that $\mathcal{I}_\infty \cap \mathbb{K}[t, z_0]$ is not reduced to $\{0\}$. □

2.2 Geometric interpretation

We now introduce a geometric interpretation of the fact that (7) is a solution of (8). Recall that a subset of $\overline{\mathbb{K}(t)}^k$ is said to be *constructible* if it is a finite union of Zariski open subsets of a Zariski closed subset of $\overline{\mathbb{K}(t)}^k$. Typically, a set defined by polynomial equations and inequations is constructible. Hence denoting by $\mathcal{X} \subset \overline{\mathbb{K}(t)}^{k+2}$ the set defined by the constraints (6), we have that $\mathcal{X}$ is a constructible set. We now define new geometric objects and assumptions for any constructible set $\mathscr{W} \subset \overline{\mathbb{K}(t)}^{k+2}$ associated with polynomial constraints in $\mathbb{K}(t)[x, u, \underline{z}]$, and deduce simple properties when $\mathscr{W} = \mathcal{X}$. Define the canonical projection $\pi : (x, u, \underline{z}) \in \overline{\mathbb{K}(t)}^{k+2} \mapsto (\underline{z}) \in \overline{\mathbb{K}(t)}^k$ onto the $\underline{z}$-coordinate space. In the whole paper, we assume that:

$$\text{The restriction of } \pi \text{ to } \mathscr{W} \text{ has finite fibers.} \qquad \textbf{(F)}$$

For $\boldsymbol{\alpha} \in \overline{\mathbb{K}(t)}^k$, we denote by $\mathscr{W}_{\boldsymbol{\alpha}} \subset \overline{\mathbb{K}(t)}^2 \times \overline{\mathbb{K}(t)}^k$ the fiber $\pi^{-1}(\boldsymbol{\alpha}) \cap \mathscr{W}$, by $\sharp_u(\mathscr{W}, \boldsymbol{\alpha})$ the number of u-coordinates of the points in $\mathscr{W}_{\boldsymbol{\alpha}}$. We set $\mathcal{F}_k(u, \mathscr{W}) := \{\boldsymbol{\alpha} \in \overline{\mathbb{K}(t)}^k \mid \sharp_u(\mathscr{W}, \boldsymbol{\alpha}) \geq k\}$.

Lemma 2.1. *If $\mathscr{W} \subset \overline{\mathbb{K}(t)}^{k+2}$ is constructible, then $\mathcal{F}_k(u, \mathscr{W})$ is also constructible. Moreover, under* **(H1)***, $\mathcal{F}_k(u, \mathcal{X})$ is not empty.*

Proof. By fixing the variables $\underline{z}$ and duplicating k times the variables x and u, it is possible to define relevant equations ensuring at least k solutions with distinct u coordinates. Now, eliminating all variables but $\underline{z}$ and using [20, Thm. 7, §7, Ch. 4, p. 226] is enough to deduce that the projection of the solution set of these duplicated constraints onto the $\underline{z}$-coordinate space is a constructible set. Under **(H1)**, Proposition 1 implies that the system (6) admits (at least) k solutions in $\overline{\mathbb{K}}[[t^{\frac{1}{\star}}]]$ with same $\underline{z}$-coordinates, and distinct u-coordinates. This proves that $\mathcal{F}_k(u, \mathcal{X})$ is not empty. ◻

The aim of the new algorithm that we will introduce in Section 5 is to compute a disjunction of conjunctions of polynomial equations and inequations in $\mathbb{K}(t)[\underline{z}]$ whose solution set in $\overline{\mathbb{K}(t)}^k$ is $\mathcal{F}_k(u, \mathcal{X})$.

Denoting $z_0, z_2, \ldots, z_{k-1}$ by $\check{z}_1$, we now consider the projection map $\pi_{\check{z}_1} : (x, u, \underline{z}) \in \overline{\mathbb{K}(t)}^{k+2} \mapsto (\check{z}_1) \in \overline{\mathbb{K}(t)}^{k-1}$. We assume in the rest of this paper that the following assumption holds:

$$\text{The restriction of } \pi_{\check{z}_1} \text{ to } \mathscr{W} \text{ has finite fibers.} \qquad (\check{\mathbf{F}})$$

Also, we introduce a set $\mathcal{S}_k(\check{z_1}, \mathscr{W})$ that will provide a second geometric interpretation of our problem, and will yield a second algorithm, given in Section 6. We thus define

$$\mathcal{S}_k(\check{z_1}, \mathscr{W}) := \{\boldsymbol{\alpha} = (\alpha_0, \ldots, \alpha_{k-1}) \in \overline{\mathbb{K}(t)}^k \mid \ \boldsymbol{\alpha} \in \pi(\mathscr{W}) \ \wedge \ \#\mathscr{W} \cap \pi_{\check{z}_1}^{-1}((\alpha_0, \alpha_2, \ldots, \alpha_{k-1})) \geq k\}.$$

Lemma 2.2. *The set $\mathcal{S}_k(\check{z_1}, \mathscr{W})$ is constructible. Moreover, under assumption* **(H1)** *the set $\mathcal{S}_k(\check{z}_1, \mathcal{X})$ is not empty.*

Proof. Considering polynomial constraints defining the set $\mathscr{W}$, the cardinality condition is modeled by: fixing the variables $\check{z}_1$, duplicating the variables x, u, z_1 and defining a conjunction of polynomial constraints ensuring the solutions of such a system to be distinct w.r.t. the duplicated coordinates. By [20, Thm. 7, §7, Ch. 4, p. 226], we deduce that $\mathcal{S}_k(\check{z_1}, \mathscr{W})$ is constructible. Under **(H1)**, the set $\mathcal{S}_k(\check{z}_1, \mathcal{X})$ contains $(F(t,a), \ldots, \partial_u^{k-1} F(t,a)) \in \overline{\mathbb{K}(t)}^k$. ◻

In Sec. 6, we will introduce a new algorithm that computes a finite set of polynomial constraints in $\mathbb{K}(t)[\underline{z}]$ characterizing $\mathcal{S}_k(\check{z}_1, \mathcal{X})$. Note that $\mathcal{F}_k(u, \mathcal{X})$ and $\mathcal{S}_k(\check{z}_1, \mathcal{X})$ are related as follows:

Lemma 2.3. *The following inclusion holds $\mathcal{F}_k(u, \mathcal{X}) \subset \mathcal{S}_k(\check{z}_1, \mathcal{X})$.*

Proof. Let us choose $\boldsymbol{\alpha} = (\alpha_0, \ldots, \alpha_{k-1}) \in \mathcal{F}_k(u, \mathcal{X})$. By definition of $\mathcal{F}_k(u, \mathcal{X})$ we have that $\boldsymbol{\alpha} \in \pi(\mathcal{X})$, hence $(\alpha_0, \alpha_2, \ldots, \alpha_{k-1}) \in \pi_{\check{z}_1}(\mathcal{X})$. Now, any of the k points in $\mathcal{X} \cap \pi^{-1}(\boldsymbol{\alpha})$ also belongs to $\mathcal{X} \cap \pi_{\check{z}_1}^{-1}((\alpha_0, \alpha_2, \ldots, \alpha_{k-1}))$. Hence $\boldsymbol{\alpha} \in \mathcal{S}_k(\check{z}_1, \mathcal{X})$. ◻

3 DIRECT APPROACH: DEGREE BOUNDS AND COMPLEXITY

In this section, we focus on the complexity of computing a nonzero element R of $\mathcal{I}_\infty \cap \mathbb{K}[t, z_0]$, by using the work of Bousquet-Mélou and Jehanne [11]. The following analysis is a generalization of the one given in [8, Proposition 2.8]. It takes benefit of the group action of the symmetric group $\mathfrak{S}_k$ on the zero set $V(\mathcal{I}_\infty)$, which can be exploited for DDEs of order $k > 1$.

Proposition 3. Let P be as in (3) of total degree δ. Assume that **(H1)** and **(H2)** hold. Then $\deg(\mathcal{I}_\infty)$ and $\#V(\mathcal{I}_\infty)$ are bounded by $\delta^k \cdot (\delta - 1)^{2k}$, and there exists $R \in \mathbb{K}[t, z_0] \setminus \{0\}$ satisfying $R(t, F(t,a)) = 0$, with $\deg_t(R)$ and $\deg_{z_0}(R)$ at most $\mathfrak{b}$, where $\mathfrak{b} := \delta^k(\delta-1)^{2k}/k!$.

Proof. First, we identify a nonzero polynomial in $\mathcal{I}_\infty \cap \mathbb{K}[t, z_0]$. Note that **(H1)** and **(H2)** allow us to apply Proposition 2 which implies that such a polynomial annihilates $F(t,a)$. Now, **(H2)** implies that the quotient ring $\mathbb{K}(t)[\underline{x}, \underline{u}, \underline{z}]/\mathcal{I}_\infty$ is a finite dimensional $\mathbb{K}(t)$-vector space. Hence by Fact 1(3), the endomorphism $m_{z_0} : f \mapsto z_0 \cdot f$ admits a characteristic polynomial $\xi_{z_0} \in \mathbb{K}(t)[z_0]$ whose roots are exactly the z_0-coordinates of all points in $V(\mathcal{I}_\infty)$ (in finite number by assumption **(H2)**). Hence, multiplying ξ_{z_0} by the lcm of the denominators of its coefficients and denoting by R the squarefree part of the resulting polynomial, the radicality of $\mathcal{I}_\infty$, together with Hilbert's Nullstellensatz, implies that $R \in \mathcal{I}_\infty \cap \mathbb{K}[t, z_0] \setminus \{0\}$. Hence R satisfies $R(t, F(t,a)) = 0$.

We now prove that the degrees of R in t and z_0 are both bounded by $\mathfrak{b}$. We apply the exact same proof as the one done for proving [8, Proposition 2.8] but with $\mathcal{I}$ replaced by $\mathcal{I}_\infty$ and with $\deg(\partial_x P)$ and $\deg(\partial_u P)$ both bounded by $\delta - 1$. This implies that $\deg(\mathcal{I}_\infty)$ and $\#V(\mathcal{I}_\infty)$ are bounded by $\delta^k(\delta-1)^{2k}$. As the partial degrees of R are bounded by $\deg(\mathcal{I}_\infty)$, it follows that $\deg_{z_0}(R) \leq \delta^k(\delta-1)^{2k}$.

It remains to justify the nontrivial division by $k!$ (which did not appear in [8, Proposition 2.8]). We exploit the following group action of $\mathfrak{S}_k$ over $V(\mathcal{I}_\infty)$. Denote by $\pi_{\underline{z}} : \overline{\mathbb{K}(t)}^{3k} \to \overline{\mathbb{K}(t)}^k$ the map such that $\pi_{\underline{z}}(V(\mathcal{I}_\infty))$ is the projection of $V(\mathcal{I}_\infty)$ onto the $\underline{z}$-coordinate space. Let $\boldsymbol{\alpha} \in \pi_{\underline{z}}(V(\mathcal{I}_\infty))$, and consider any k-tuple $(\xi_i, v_i, \boldsymbol{\alpha})$ (for $1 \leq i \leq k$) in $\mathcal{X} \cap \pi^{-1}(\boldsymbol{\alpha})$. Then for all $1 \leq i \leq k$, and all $\sigma \in \mathfrak{S}_k$, the concatenation of all $(\xi_{\sigma(i)}, v_{\sigma(i)})$ remains a solution to the system defining $\mathcal{I}_\infty$, where the $\underline{z}$-coordinates are specialized to the coordinates of $\boldsymbol{\alpha}$. Since diag $\neq 0$, then $v_i \neq v_j$ for $i \neq j$. Hence the above orbit has cardinality $k!$. Since all roots in $\overline{\mathbb{K}(t)}$ of R, seen as a polynomial in $\mathbb{K}(t)[z_0]$, correspond to one coordinate of $\boldsymbol{\alpha} \in \pi_{\underline{z}}(V(\mathcal{I}_\infty))$, we deduce that $\deg_{z_0}(R)$ is bounded by the cardinality of $V(\mathcal{I}_\infty)$ divided by $k!$, the combinatorial complexity of $\mathfrak{S}_k$. Bounding $\deg_t(R)$ is done the same way, by inverting the roles of z_0 and t. ◻

Proposition 4. Let P be as in (3) of total degree δ. We suppose that (**H1**) and (**H2**) hold. Then there exists an algorithm which takes as input a straight-line program of length L evaluating P and diag, and returns a nonzero polynomial $R \in \mathbb{K}[t, z_0]$ such that $R(t, F(t, a)) = 0$, using

$$\tilde{O}((kL+1)\delta^{2k}(\delta-1)^{4k} + \delta^{2.63k}(\delta-1)^{5.26k}/k!) \subset \tilde{O}(\delta^{6k}(k^2\delta^{k+3} + \delta^{1.89k}/k!))$$

arithmetic operations in $\mathbb{K}$.

Remark 3.1. Note that the above complexity is polynomial in $\mathfrak{b}$.

Proof. We generalize the proof of [8, Proposition 2.9] to our situation. By Proposition 3, $\deg(\mathcal{I}_\infty)$ and $\#V(\mathcal{I}_\infty)$ are bounded by $\delta^k \cdot (\delta-1)^{2k}$. Using the algorithm underlying [36, Theorem 2], we thus compute a parametric geometric resolution [36] of the zero set $V(\mathcal{I}_\infty)$ in $\tilde{O}((kL+1)\delta^{2k}(\delta-1)^{4k})$ ops. in $\mathbb{K}$. This algorithm computes two polynomials $V(t, \lambda), W(t, \lambda) \in \mathbb{K}(t)[\lambda]$ giving the parametrization $z_0 = V(t, \lambda)/\partial_\lambda W(t, \lambda)$ whenever $W(t, \lambda) = 0$. Now, we define the map $m_{z_0} : f \mapsto f \cdot z_0$ in $\mathbb{K}(t)[\underline{x}, \underline{u}, \underline{z}]/\mathcal{I}_\infty$ and observe that its characteristic polynomial is the resultant w.r.t. λ of $z_0 \cdot \partial_\lambda W(t, \lambda) - V(t, \lambda)$ and $W(t, \lambda)$. We thus compute the squarefree part R of this resultant: *(i)* by performing evaluation–interpolation on t with, by Proposition 3, $O(\mathfrak{b})$ points; *(ii)* for each evaluation in $t = \theta \in \mathbb{K}$, the polynomials $z_0 \cdot \partial_\lambda W(\theta, \lambda) - V(\theta, \lambda)$ and $W(\theta, \lambda)$ are bivariate polynomials, which allows us to use [28, §5] for the bivariate resultant computation. This step is in $\tilde{O}(\delta^{2.63k}(\delta-1)^{5.26k}/k!)$ ops. in $\mathbb{K}$. Finally, the inclusion comes from the cost for evaluating P and the saturating polynomial diag, which by the Baur-Strassen theorem [4, Theorem 1] satisfies $L \in O(k\delta^{k+3})$. □

Despite the process of duplicating variables as done for obtaining the system (8) is, up to deforming the initial DDE, very fruitful for creating zero dimensional ideals and showing theoretical algebraicity results [11, 31], it usually suffers from efficiency issues. Applying [27, Prop. 2] for $n, m \in \mathbb{N}$ and an algebraic set $V \subset \overline{\mathbb{K}}^n$, we have that $\deg(V^m) = \deg(V)^m$. The degenerate behavior of the state-of-the-art when k grows up comes from this exponential growth of the ideal's degree in the number of duplications (which is k in our case). Moreover, duplicating variables also introduces $3k+2$ variables, while the initial system in (6) only deals with $k+3$ variables. A natural hope is hence to avoid these duplications by a careful analysis of the geometry given by the initial constraints (6).

Remark 3.2. This number of duplications and the group action of $\mathfrak{S}_k$ over $V(\mathcal{I}_\infty)$ is usually exploited by the state-of-the-art of the polynomial system solving theory by working in the invariant ring associated to this group action (see [23]). However, in our case, this approach would imply to introduce a number of variables which would be at least equal to k. In the algorithm we propose in Sections 5 and 6, we focus on introducing no more extra variables.

4 HYBRID GUESS-AND-PROVE ALGORITHM

We analyze in what follows the complexity of the *hybrid guess-and-prove* algorithm introduced in [8, §2.2.2]. Recall that it blends algebraic elimination with a guess-and-prove approach inspired by Zeilberger's method [39], see [8, §2.2.1]. For functional equations of arbitrary order, the motivation of this method comes from certain concrete examples for which the involved polynomial systems are difficult to solve (e.g. [14, §3.6]). Let us recall the algorithm:

Hybrid guess-and-prove method

(0) Compute $F(t, a) \bmod t^\sigma$ for some integer $\sigma \geq 1$;
(1) Guess $R \in \mathbb{K}[t, z_0] \setminus \{0\}$ such that $R(t, F(t, a)) = 0 \bmod t^\sigma$;
(2) Check if $R(t, F(t, a)) = 0 \bmod t^{\mathfrak{b}\cdot\deg R+1}$;
(3) If not, then go back to (0) with $\sigma := 2\sigma$; if yes, then return R.

The correctness of this method is a consequence of [8, §2.2.2] and of the existence, under suitable hypothesis, of a nonzero polynomial $R \in \mathbb{K}[t, z_0]$ annihilating $F(t, a)$ with partial degrees bounded by $\mathfrak{b}$. It remains to make those hypotheses completely explicit.

Notation 2. We still assume the existence of k distinct nonconstant solutions $u = U_1(t), \ldots, U_k(t) \neq a$ to (5) and we denote by $\mathcal{P}$ the point of $\overline{\mathbb{K}}[[t^{\frac{1}{\star}}]]^{3k}$ obtained by concatenating the values $\{F(t, U_i(t))\}_{1\leq i\leq k}, \{U_i(t)\}_{1\leq i\leq k}$ and $\{\partial_u^i F(t, a)\}_{0\leq i\leq k-1}$.

Hypothesis 4: The Jacobian matrix Jac of (8), considered in $\underline{x}, \underline{u}, \underline{z}$, is invertible at $\mathcal{P}$. (**H4**)

Lemma 4.1. *Under* (**H1**) *and* (**H4**), *the saturation* $\mathcal{I} : \det(Jac)^\infty$ *is a radical and* 0*-dimensional ideal of* $\mathbb{K}(t)[\underline{x}, \underline{u}, \underline{z}]$. *Hence there exists a nonzero* $R \in \mathcal{I} : \det(Jac)^\infty \cap \mathbb{K}[t, z_0]$ *annihilating* $F(t, a)$ *with partial degrees bounded by* $\mathfrak{b}$.

Proof. The radicality and dimension results are consequences of [8, Lemma 2.10]. The rest of the proof is the same as the one used for proving Proposition 3, with $\mathcal{I}_\infty$ replaced by $\mathcal{I} : \det(\mathrm{Jac})^\infty$. □

This concludes the correctness of the hybrid guess-and-prove method in the case of DDEs of order $k > 1$. Under (**H1**) and (**H4**), we also deduce a complexity estimate generalizing [8, Prop. 2.11].

Proposition 5. Let P be as in (3) and let δ be its total degree. Let us assume that assumptions (**H1**) and (**H4**) hold, and that there exists a straight-line program of length L evaluating P. Then the hybrid guess-and-prove method terminates on input P using

$$\tilde{O}(L \cdot k^3 \cdot \mathfrak{b}^2 + k \cdot \mathfrak{b}^{\theta+1}) \subset \tilde{O}(k \cdot \delta^{10.12\cdot k}/(k-1)!^2)$$

arithmetic operations in $\mathbb{K}$.

Proof. We analyze the last execution of steps (0)–(3), happening with $\sigma = O(\mathfrak{b}^2)$ and $\deg(R) = O(\mathfrak{b})$. Using Hermite-Padé approximation (e.g. [9, 26]), the guessing at step (1) is done in $\tilde{O}(\sigma \cdot \deg_{z_0}(R)^{\theta-1}) \subset \tilde{O}(\mathfrak{b}^{\theta+1})$ ops. in $\mathbb{K}$. The order of $F(t, a)$ and the truncation order $\mathfrak{b} \cdot \deg(R) + 1$ at step (2) are in $O(\mathfrak{b}^2)$. Hence the truncated evaluation of R at $z_0 = F(t, a)$ is computed in $\tilde{O}(\deg(R) \cdot (\mathfrak{b} \cdot \deg(R))) \subset \tilde{O}(\mathfrak{b}^3) \subset \tilde{O}(\mathfrak{b}^{\theta+1})$ ops. in $\mathbb{K}$.

Let V the system given by (8). We compute the truncated series $F(t, a)$ using the classical Newton method, by considering the iteration

$$\mathbf{F} \mapsto \mathcal{N}(\mathbf{F}) := \mathbf{F} - J(\mathbf{F})^{-1} \cdot V^{\mathrm{T}}(\mathbf{F}), \quad (9)$$

where $J = \mathrm{Jac}(V)$ (w.r.t. $\underline{x}, \underline{u}, \underline{z}$) and $\mathbf{F} \in \mathbb{L}[[t^{\frac{1}{k}}]]^{3k}$ denotes an approximation of the solution $\mathcal{F}$ at which J is invertible by assumptions (**H1**) and (**H4**), with $\mathbb{L}/\mathbb{K}$ a finite field extension of degree at most k (by Prop. 1). Before going further, recall that the cost for elementary arithmetic operations in $\mathbb{L}$ can be expressed in terms of elementary arithmetic operations in $\mathbb{K}$: as the field extension is of degree at most k, multiplying and summing two elements of $\mathbb{L}$ can be done in $\tilde{O}(k)$ arithmetic operations in $\mathbb{K}$.

As the number of correct terms is doubled at each iteration of (9), we iterate (9) at most $O(\log(k))$ times to obtain a truncation of $\mathcal{F}$ mod t (because of the ramification appearing in the Puiseux series U_i). Hence we perform this precomputation before doubling the integer power in t.

By the Baur-Strassen theorem [4], a straight-line program of length $O(L \cdot k)$ evaluating V can be obtained from the one evaluating P. By iterating this argument, one also finds a straight-line program of length $O(L \cdot k)$ that evaluates the Jacobian matrix. Consequently, there is also one in $O(L \cdot k)$ for its inverse. Evaluating V and J^{-1} at $\mathbf{F}$ of some order N requires consequently $\tilde{O}(L \cdot k \cdot N)$ arithmetic operations in $\mathbb{L}$, because of the fact that the cardinality of the support of U_i mod t^N is in $O(k \cdot N)$. This is also the cost of a Newton iteration. All in all, one obtains a complexity for step (0) in $\tilde{O}(L \cdot k^2 \cdot \sigma)$ arithmetic operations in $\mathbb{L}$. Summing all complexities, the hybrid guess-and-prove complexity is in $\tilde{O}(L \cdot k^2 \cdot \mathfrak{b}^2 + \mathfrak{b}^{\theta+1})$ ops. in $\mathbb{L}$. This gives the global complexity of $\tilde{O}(L \cdot k^3 \cdot \mathfrak{b}^2 + k \cdot \mathfrak{b}^{\theta+1})$ ops. in $\mathbb{K}$. The inclusion is a consequence of the estimate $L \in O(\delta^{k+3})$. ◻

5 APPROACH USING ELIMINATION THEORY

Let $\mathscr{W} \subset \overline{\mathbb{K}(t)}^{k+2}$ be a constructible set defined by polynomial constraints in $\mathbb{K}(t)[x, u, \underline{z}]$. We assume that assumption **(F)** holds. For $i \in \mathbb{N}$, we consider the (possibly infinite) set

$$\mathcal{F}_i(u, \mathscr{W}) := \{\boldsymbol{\alpha} \in \overline{\mathbb{K}(t)}^k \mid \sharp_u(\mathscr{W}, \boldsymbol{\alpha}) \geq i\}.$$

Observe that $\mathcal{F}_{i+1}(u, \mathscr{W}) \subseteq \mathcal{F}_i(u, \mathscr{W})$ for any $i \geq 1$. Adapting easily the proof of Lemma 2.1 yields that $\mathcal{F}_i(u, \mathscr{W})$ is constructible.

In this section, we provide an algorithm that takes as input $i \in \mathbb{N}$ and a polynomial system defining some algebraic set $W \subset \overline{\mathbb{K}(t)}^{k+2}$ and returns a disjunction of conjunctions of polynomial equations and inequations in $\mathbb{K}(t)[\underline{z}]$ whose solution set in $\overline{\mathbb{K}(t)}^k$ is $\mathcal{F}_i(u, W)$. We then show how to apply this algorithm to compute witnesses of algebraicity to solutions of DDEs of order k.

To begin with, we assume that W is given by a polynomial sequence $\boldsymbol{f}$ in $\mathbb{K}[t][x, u, \underline{z}]$ and we denote by $\mathcal{J}$ the ideal it generates in $\mathbb{K}(t)[x, u, \underline{z}]$. To design our algorithm, we leverage advanced results of the theory of Gröbner bases to characterize $\mathcal{F}_i(u, W)$.

Let $\rho_x : (x, u, \underline{z}) \mapsto (u, \underline{z})$ be the canonical projection which forgets the variable x. We denote by G a Gröbner basis for $(\mathcal{J}, \succ)$, where $\succ$ is a lexicographic monomial ordering with $x \succ u \succ \underline{z}$. Let $G_x = G \cap \mathbb{K}(t)[u, \underline{z}]$ and ℓ_x be the leading coefficients w.r.t. the variable x of the polynomials in G which have positive degree w.r.t. x. Finally, we extend the definition of $\mathcal{F}_i(u, \cdot)$ to constructible sets defined with constraints in $\mathbb{K}(t)[u, \underline{z}]$ and we let $\mathscr{W} = \rho_x(W)$.

Lemma 5.1. *The set $\mathcal{F}_i(u, W)$ coincides with $\mathcal{F}_i(u, \mathscr{W})$.*

Proof. Let $\boldsymbol{\alpha} \in \pi(W)$. As the u-coordinates of $W_{\boldsymbol{\alpha}}$ coincide with the u-coordinates of the points in $\mathscr{W}$ projecting on $\boldsymbol{\alpha}$, the conclusion follows from the definitions of $\mathcal{F}_i(u, W)$ and $\mathcal{F}_i(u, \mathscr{W})$. ◻

Lemma 5.2. *The set $\mathscr{W}$ is defined by the vanishing of all polynomials in G_x and the nonvanishing of at least one element in ℓ_x.*

Proof. This follows by applying Fact 1(1) and Fact 1(2). ◻

We use Lemmas 5.1 and 5.2 to compute a polynomial system that encodes $\mathcal{F}_i(u, \mathscr{W})$. Remark that by applying Lemma 5.2, $\mathscr{W}$ is the union of the locally closed sets defined by the vanishing of all polynomials in G_x and the nonvanishing of at least one element of ℓ_x. Note that the vanishing set of G_x is the Zariski closure of $\mathscr{W}$. Furthermore, we denote by G_u the set $G_x \cap \mathbb{K}(t)[\underline{z}]$.

Given a set F of polynomials in $\mathbb{K}(t)[u, \underline{z}]$ and $r \in \mathbb{N}$, we denote by $\mathrm{DEG}_r(F, u)$ (resp. $\mathrm{DEG}_{\leq r}(F, u)$) the subset of polynomials in F of degree r (resp. at most r) in u. For a polynomial $f \in \mathbb{K}(t)[u, \underline{z}]$, we denote by $\mathrm{coeffs}(f, u)$ its coefficients when f is seen in $\mathbb{K}'[u]$ with $\mathbb{K}' := \mathbb{K}(t)[\underline{z}]$.

Lemma 5.3. *We reuse the notation introduced above. Let i be greater than 0. If there is no polynomial in G_x whose degree w.r.t. u is greater than or equal to i, then $\mathcal{F}_i(u, \mathscr{W})$ is empty.*

Proof. Suppose that $\mathcal{F}_i(u, \mathscr{W}) \neq \emptyset$ and pick $\boldsymbol{\alpha} \in \mathcal{F}_i(u, \mathscr{W})$. By [20, Thm. 2, §2, Ch. 3, p. 130], there exists $g \in G_x$ of degree $\leq i-1$ in u and some $1 \leq j \leq \deg_u(g)$ such that: the coefficient of u^j does not vanish at $\boldsymbol{\alpha}$ and the coefficients of u^ℓ vanish at $\boldsymbol{\alpha}$, for all $\ell > j$. There thus exist at most $j < i$ solutions to the equation $g(u, \underline{z} = \boldsymbol{\alpha}) = 0$. This contradicts the fact that the fiber above $\boldsymbol{\alpha}$ has cardinality at least i, and hence that $\boldsymbol{\alpha} \in \mathcal{F}_i(u, \mathscr{W})$. ◻

Let $\ell_u^{(i)}$ be the set of leading coefficients of the polynomials in G_x that have degree at least i w.r.t. u; we denote $\ell_u^{(1)}$ by ℓ_u.

Also for $g \in G_x$ of positive degree i in u, we denote by $\mathrm{Min}_{\mathrm{Her}}(g, i)$ the set in $\mathbb{K}(t)[\underline{z}]$ of all $i \times i$ minors of the Hermite quadratic form associated with g when seen as a polynomial in u. By [3, Thm. 4.57, p. 130], $g(u, \boldsymbol{\alpha})$ has at least i distinct roots when $\boldsymbol{\alpha}$ does not lie in the common zero set of $\mathrm{Min}_{\mathrm{Her}}(g, i)$.

Let $\mathcal{S}^{(i)}$ be the set of points $\boldsymbol{\beta} \in \overline{\mathbb{K}(t)}^{k+1}$ such that the following polynomial constraints are simultaneously satisfied:

- *(a)* all polynomials in G_u vanish at $\boldsymbol{\beta}$;
- *(b)* all polynomials in $\mathrm{coeffs}(f, u)$ for $f \in \mathrm{DEG}_{\leq i-1}(G_x, u)$ vanish at $\boldsymbol{\beta}$;
- *(c)* at least one polynomial $\ell \in \ell_x$ does not vanish at $\boldsymbol{\beta}$;
- *(d)* at least one polynomial $\ell \in \ell_u^{(i)}$ does not vanish at $\boldsymbol{\beta}$;
- *(e)* at least one polynomial in $\mathrm{Min}_{\mathrm{Her}}(g, i)$ does not vanish at $\boldsymbol{\beta}$, for some $g \in G_x$ with degree at least i w.r.t. u.

Further, we denote by *(f)* the disjunction $\vee_{\ell \in \ell_u} \ell \neq 0$.

To give the intuition, conditions *(a), (c)* and *(f)* characterize the projected sets $\mathscr{W}$ and $\pi(W)$. Conditions *(b), (d)* and *(e)* characterize the cardinality of the fiber.

Proposition 5.4. *The projection of $\mathcal{S}^{(i)}$ onto the $\underline{z}$-coordinate space is $\mathcal{F}_i(u, \mathscr{W})$.*

Proof. We start by showing that the set of points which do satisfy *(a), (c)* and *(f)* coincides with $\pi(W)$ which, by definition, contains $\mathcal{F}_i(u, W)$.

By [20, Ch. 3, §2, Thm. 3, p. 156], the Zariski closure of $\pi(W)$ is defined by *(a)*. By Lemma 5.2, $\mathscr{W}$ is defined by the vanishing of all polynomials in G_x and the nonvanishing of at least one element in ℓ_x. Note that $\pi(W)$ coincides with the projection of $\mathscr{W}$ on the $\underline{z}$-coordinate space (which we also denote by $\pi(\mathscr{W})$ by a slight abuse of notation). Note that all points of $\mathscr{W}$ also satisfy *(c)* Applying Fact 1(2) to G_x and the Zariski closure of $\mathscr{W}$ shows that $\pi(\mathscr{W})$

is also contained in the set of points which satisfy *(f)*. To prove the reverse inclusion, it suffices to apply Fact 1(2) by lifting the solutions of *(a)* from the $\underline{z}$-space to points in W.

It remains to show that the extra conditions *(b)*, *(d)* and *(e)* ensure the cardinality condition on the fiber of π. First, it results from Lemma 5.3 that *(b)* is a necessary condition to ensure a fiber of cardinality at least i. Next, it follows from [20, Chap. 3, §5, Thm. 2, p. 156] and *(d)* that the cardinality condition on the fiber is reduced to see under which condition a univariate polynomial $g(u, \underline{z} = \boldsymbol{\alpha})$ (for $\boldsymbol{\alpha} \in \pi(\mathscr{W})$ and $g \in G_x$) admits at least i distinct roots. Finally, it follows from [3, Thm. 4.57] that *(e)* is a necessary and sufficient condition for this. Also, a subtle observation is that *(f)* guarantees that the vanishing set of the possible denominators in the minors in $\mathrm{Min}_{\mathrm{Her}}(g, i)$ is avoided (as they are by construction only powers of $\mathsf{LeadingCoefficient}_u(g)$). □

Hence, the algorithm which relies on Proposition 5.4 consists in:

(1) Computing a Gröbner basis G for $\mathcal{J} \subset \mathbb{K}(t)[x, u, \underline{z}]$ w.r.t. some lexicographic ordering $>$ with $x > u > \underline{z}$;
(2) Computing the relations that define $\mathcal{S}^{(i)}$ as described above;
(3) For each conjunction of constraints defining $\mathcal{S}^{(i)}$: eliminating u from G_x and from the defining equations and eliminating the saturation variables introduced to handle inequations (still, the inequations should be kept in the output).

Note that in step (3), Gröbner bases can be used to perform the elimination. This also has the advantage to determine if there are points which do satisfy both the equations and inequations defining $\mathcal{S}^{(i)}$, hence deciding its emptiness.
It should be noted that, in practice, one can avoid to use $\mathbb{K}(t)$ as a base field and perform the computations in $\mathbb{K}[x, u, \underline{z}, t]$ with an elimination ordering where t is the smallest variable. Specialization properties of Gröbner bases [29] show that one obtains this way a nonreduced Gröbner basis for $\mathcal{J}$. Computing the conditions *(a)-(d)* is straightforward with standard computer algebra systems [25].

For the application to DDEs, we make the following hypothesis.

Hypothesis 3: $\mathcal{F}_k(u, \mathcal{X})$ and $\mathcal{S}_k(\check{z}_1, \mathcal{X})$ are finite sets. **(H3)**

Proposition 5.5. *Let P be as in* (3) *and $a \in \mathbb{K}$. Assume* **(H1)**, **(H3)** *and that P is squarefree. Denote $\mathcal{J} := \langle P, \partial_x P, \partial_u P\rangle : (u - a)^\infty \subset \mathbb{K}(t)[x, u, \underline{z}]$. If $\mathcal{G}$ is the disjunction of conjunction of polynomial equations computed by the algorithm based on Proposition 5.4, then there exists one conjunction in $\mathcal{G}$ from which eliminating all variables but t and z_0 yields some nonzero $R \in \mathbb{K}[t, z_0]$ s.t. $R(t, F(t, a)) = 0$.*

Proof. First, it results from Sard's lemma [33, Prop. B.2, App-8] that if P is squarefree, then $\mathcal{J} \cap \mathbb{K}(t)[\underline{z}]$ is not reduced to 0 (by using the same proof as in [8, Lemma 2.3], for $k > 1$). Note also that by Proposition 5.4, the solution set of $\mathcal{G}$ is $\mathcal{F}_k(u, \mathscr{W})$. Finally, using **(H1)** implies that the projection of $\mathcal{F}_k(u, \mathcal{X})$ onto the z_0-coordinate space contains the value $F(t, a)$. Hence using [20, Thm. 3, §2, Ch. 3], Fact 1(1) and eliminating all variables but t and z_0 in each condition given by $\mathcal{G}$ either yields, by **(H3)**, a nonzero polynomial in $\mathbb{K}[t, z_0]$ or yields the constant polynomial 1. In any case, one of the conditions in $\mathcal{G}$ yields by **(H1)** and **(H3)** a nonzero $R \in \mathbb{K}[t, z_0]$ annihilating $F(t, a)$. □

6 GEOMETRIC APPROACH

Let $\mathscr{V} \subset \overline{\mathbb{K}(t)}^{k+2}$ be an algebraic set associated to an ideal $\mathcal{J}$ of $\mathbb{K}(t)[x, u, \underline{z}]$. For a set of variables (or scalars) $z_0, \ldots, z_{k-1}$, recall that we use the notation $\check{z}_1 := z_0, z_2, \ldots, z_{k-1}$. Also, we consider the canonical inclusion $j : \mathbb{K}(t)[x, u, \underline{z}] \to \mathbb{K}(t, \check{z}_1)[x, u, z_1]$.

In this section, we say that assumption (S) holds if the following assumptions hold:

- ($\check{\mathrm{F}}$) holds (with $\mathscr{W}$ replaced by $\mathscr{V}$),
- the image of $\mathscr{V}$ by $\pi_{\check{z}_1}$ is Zariski dense ($\overline{\pi_{\check{z}_1}(\mathscr{V})} = \overline{\mathbb{K}(t)}^{k-1}$),
- $\mathcal{J}$ has dimension $k - 1$ in $\mathbb{K}(t)[x, u, \underline{z}]$,
- $\mathcal{J}_{z_1} := \langle j(\mathcal{J})\rangle$ has dimension 0 in $\mathbb{K}(t, \check{z}_1)[x, u, z_1]$.

Recall that using Lemma 2.2, the set $\mathcal{S}_k(\check{z_1}, \mathscr{V})$ is constructible. In this section, we design an algorithm with the following specification: it takes as input a finite set of polynomials of $\mathbb{K}(t)[x, u, \underline{z}]$ generating a radical ideal $\mathcal{J}$ satisfying assumption (S) and such that $\mathcal{J} \cap \mathbb{K}(t)[\underline{z}]$ is principal; it returns, under an additional assumption that will be made explicit later, a finite set of polynomial constraints whose solution set is the Zariski closure of $\mathcal{S}_k(\check{z_1}, \mathscr{V})$, for $\mathscr{V} \subset \overline{\mathbb{K}(t)}^{k+2}$ the zero set of $\mathcal{J}$.

To achieve our aim, we first determine algebraic relations which induce a zero set containing $\mathcal{S}_k(\check{z_1}, \mathscr{V})$. The ideal $\mathcal{J}_{z_1}$ having dimension 0, the quotient ring $\mathbb{K}(t, \check{z}_1)[x, u, z_1]/\mathcal{J}_{z_1}$ defines a $\mathbb{K}(t, \check{z}_1)$-vector space of finite dimension. We introduce the multiplication map $m_{z_1} : f \mapsto f \cdot z_1$ which maps $\mathbb{K}(t, \check{z}_1)[x, u, z_1]/\mathcal{J}_{z_1}$ to itself, and consider its characteristic polynomial $\xi \equiv \xi_{z_1} \in \mathbb{K}(t, \check{z}_1)[z_1]$. We denote by $\chi \equiv \chi_{z_1} \in \mathbb{K}(t)[\underline{z}]$ the numerator of ξ w.r.t. $\check{z}_1$ and by $\mathsf{denom}(\xi) \in \mathbb{K}(t)[\underline{z}]$ its denominator. As $\mathsf{denom}(\xi)$ depends only on $k - 1$ variables, $V(\mathsf{denom}(\xi))$ is a priori only defined in $\overline{\mathbb{K}(t)}^{k-1}$. Seeing $\mathsf{denom}(\xi)$ as a polynomial in $\mathbb{K}(t)[x, u, \underline{z}]$ (resp. $\mathbb{K}(t)[u, \underline{z}]$, $\mathbb{K}(t)[\underline{z}]$), its zero set is $\overline{\mathbb{K}(t)}^3 \times V(\mathsf{denom}(\xi))$ (resp. $\overline{\mathbb{K}(t)}^2 \times V(\mathsf{denom}(\xi))$, $\overline{\mathbb{K}(t)} \times V(\mathsf{denom}(\xi))$). With a slight abuse of notation, we denote all these sets by $V(\mathsf{denom}(\xi))$: the precise definition domain will be implicitly dependent on the set with which we intersect/take the complement, etc.

Let $Z := (\overline{\mathbb{K}(t)}^{k+2} \setminus V(\mathsf{denom}(\xi))) \cap \overline{\mathbb{K}(t)}^3 \times \pi_{\check{z}_1}(\mathscr{V}) \subset \overline{\mathbb{K}(t)}^{k+2}$.

Lemma 6.1. *Under* (S) *and assuming the radicality of $\mathcal{J}$, the set Z is a dense subset of $\overline{\mathbb{K}(t)}^{k+2}$ which satisfies $V(\mathcal{J} \cap \mathbb{K}(t)[\underline{z}] + \langle \chi, \partial_{z_1}\chi, \ldots, \partial_{z_1}^{k-1}\chi\rangle) \cap \pi(Z) = \mathcal{S}_k(\check{z}_1, \mathscr{V} \cap Z)$.*

Proof. The density of Z follows from 2 facts: (i) the complement of $V(\mathsf{denom}(\xi))$ is dense in $\overline{\mathbb{K}(t)}^{k-1}$; (ii) by (S), the image of $\mathscr{V}$ by $\pi_{\check{z}_1}$ is Zariski dense.

Now, from the 0-dimensionality of $\mathcal{J}_{z_1}$, the eigenvalues of the endomorphism m_{z_1} of $\mathbb{K}(t, \check{z}_1)[x, u, z_1]/\mathcal{J}_{z_1}$ are, by Fact 1(3), the z_1-coordinates of the zero set $\mathscr{V}_{z_1} \subset \overline{\mathbb{K}(t, \check{z}_1)}^3$ associated to $\mathcal{J}_{z_1}$. Also note that we can specialize $\underline{z}$ in ξ to any point of $\pi(\mathscr{V} \cap Z)$.

We now prove the direct inclusion. We pick $\boldsymbol{\alpha} = (\alpha_0, \ldots, \alpha_{k-1}) \in V(\mathcal{J} \cap \mathbb{K}(t)[\underline{z}] + \langle \chi, \partial_{z_1}\chi, \ldots, \partial_{z_1}^{k-1}\chi\rangle) \cap \pi(Z)$, and we consider the specialized ideal $\mathcal{J}_{\boldsymbol{\alpha}}$ obtained by specialization of $\mathcal{J}$ to $\check{z}_1 = \check{\boldsymbol{\alpha}}$. As $(\check{\boldsymbol{\alpha}}) \in \pi_{\check{z}_1}(Z) \subset \pi_{\check{z}_1}(\mathscr{V})$, it follows $V(\mathcal{J}_{\boldsymbol{\alpha}})$ is not empty and hence that $\mathcal{J}_{\boldsymbol{\alpha}}$ has dimension 0. Moreover, $V(\mathcal{J}_{\boldsymbol{\alpha}})$ corresponds to the zero set of the specialized ideal $\mathcal{J}_{z_1, \boldsymbol{\alpha}}$ obtained after specialization of $\mathcal{J}_{z_1}$ to $\check{z}_1 = \check{\boldsymbol{\alpha}}$. As $\boldsymbol{\alpha} \in V(\chi, \partial_{z_1}\chi, \ldots, \partial_{z_1}^{k-1}\chi)$, we have that $z_1 = \alpha_1$ is a root of multiplicity at least k of the polynomial $\chi(z_1, \check{z}_1 = \check{\boldsymbol{\alpha}})$. By the radicality of $\mathcal{J}$, the use of Fact 1(3) in the 0-dimensional ideal $\mathcal{J}_{z_1,\boldsymbol{\alpha}}$, the correspondence $V(\mathcal{J}_{\boldsymbol{\alpha}}) = V(\mathcal{J}_{z_1,\boldsymbol{\alpha}})$, the fact that $\boldsymbol{\alpha} \notin V(\mathrm{denom}(\xi))$ and $\boldsymbol{\alpha} \in V(\langle \chi, \partial_{z_1}\chi, \ldots, \partial_{z_1}^{k-1}\chi\rangle)$, there exist at least k points in $\mathscr{V} \cap (\cap_{i=0,i\neq 1}^{k-1}\{z_i = \alpha_i\})$. Hence $\alpha \in \mathcal{S}_k(\check{z}_1, \mathscr{V} \cap Z)$.

We now prove the reverse inclusion. Let $\boldsymbol{\alpha} = (\alpha_0, \ldots, \alpha_{k-1}) \in \mathcal{S}_k(\check{z}_1, \mathscr{V} \cap Z)$. By definition of $\mathcal{S}_k(\check{z}_1, \mathscr{V} \cap Z)$, we have that $\boldsymbol{\alpha} \in \pi(\mathscr{V} \cap Z)$. As we have $\pi(\mathscr{V} \cap Z) \subset \pi(\mathscr{V}) \cap \pi(Z)$, it follows that $\boldsymbol{\alpha} \in \pi(Z)$. It remains to show that $\boldsymbol{\alpha} \in V(\mathcal{J} \cap \mathbb{K}(t)[\underline{z}] + \langle \chi, \ldots, \partial_{z_1}^{k-1}\chi\rangle)$. By Fact 1(1), we have that $\boldsymbol{\alpha} \in V(\mathcal{J} \cap \mathbb{K}(t)[\underline{z}])$. Now, as $\pi_{\check{z}_1}(\boldsymbol{\alpha}) \notin V(\mathrm{denom}(\xi))$, we can consider for $0 \leq i \leq k-1$ the well-defined polynomials $\partial_{z_1}^i \chi(z_1, \check{z}_1 = \check{\boldsymbol{\alpha}})$. By the set equality $V(\mathcal{J}_{\boldsymbol{\alpha}}) = V(\mathcal{J}_{z_1,\boldsymbol{\alpha}})$, the fact that there exist at least k points in $\mathscr{V} \cap (\cap_{i=0,i\neq 1}^{k-1}\{z_i = \alpha_i\})$ translate, by the application of Fact 1(3) to the well-defined 0-dimensional ideal $\mathcal{J}_{z_1,\boldsymbol{\alpha}}$, to the vanishings $\partial_{z_1}^i \chi(\underline{z} = \boldsymbol{\alpha}) = 0$, for all $0 \leq i \leq k-1$. □

In all the combinatorial examples that we considered so far, taking $\mathcal{J} := \langle P, \partial_x P, \partial_u P\rangle : (u-a)^\infty$ for P as in (3) always led to $\mathcal{S}_k(\check{z}_1, \overline{\mathcal{X}} \cap Z) = \mathcal{S}_k(\check{z}_1, \overline{\mathcal{X}})$. Hence in order to simplify things and to avoid introducing additional technicalities, we assume in the rest of this section that

$$\mathcal{S}_k(\check{z}_1, \mathscr{V} \cap Z) = \mathcal{S}_k(\check{z_1}, \mathscr{V}). \qquad (\mathcal{Z})$$

From an application viewpoint, working under this new generic assumption is (as mentioned above) harmless.

Lemma 6.2. *Assuming* $(\mathcal{Z})$, (S)*, and the radicality of* $\mathcal{J}$*, the Zariski closure of* $\mathcal{S}_k(\check{z_1}, \mathscr{V})$ *is the zero set of the saturated ideal* $(\mathcal{J} \cap \mathbb{K}(t)[\underline{z}] + \langle \chi, \ldots, \partial_{z_1}^{k-1}\chi\rangle) : \mathrm{denom}(\xi)^\infty$.

Proof. We define $V_1 := V(\mathcal{J} \cap \mathbb{K}(t)[\underline{z}] + \langle \chi, \ldots, \partial_{z_1}^{k-1}\chi\rangle)$. Using $(\mathcal{Z})$ we can replace $\mathcal{S}_k(\check{z_1}, \mathscr{V})$ by $\mathcal{S}_k(\check{z}_1, \mathscr{V} \cap Z)$. Also, Lemma 6.1 implies that the Zariski closure of $\mathcal{S}_k(\check{z_1}, \mathscr{V})$ is equal to the Zariski closure of $V_1 \cap \pi(Z)$. Denote $W := \overline{\mathbb{K}(t)} \times \pi_{\check{z}_1}(\mathscr{V}) \subset \overline{\mathbb{K}(t)} \times \overline{\mathbb{K}(t)}^{k-1}$ (which is dense in $\overline{\mathbb{K}(t)}^k$ as the image of $\mathscr{V}$ by $\pi_{\check{z}_1}$ is assumed to be Zariski dense). By the definition of Z, we have $\overline{V_1 \cap \pi(Z)} = \overline{V_1 \cap (W \setminus \pi(V(d(\xi))))}$. Using the density property of W, we thus have that $\overline{V_1 \cap \pi(Z)} = \overline{V_1 \setminus \pi(V(d(\xi)))}$. The results hence follows as the zero set of $(\mathcal{J} \cap \mathbb{K}(t)[\underline{z}] + \langle \chi, \ldots, \partial_{z_1}^{k-1}\chi\rangle) : d(\xi)^\infty$ is $\overline{V_1 \setminus \pi(V(d(\xi)))}$. □

Applying Lemmas 6.1 and 6.2 and under $(\mathcal{Z})$, our aim is hence to compute $\mathcal{J} \cap \mathbb{K}(t)[\underline{z}] + \langle \chi, \partial_{z_1}\chi, \ldots, \partial_{z_1}^{k-1}\chi\rangle$. Regarding complexities estimates, the use of parametric geometric resolution tools ([36]) allows to prove the following result.

Lemma 6.3. *Assume that* $\mathcal{J}$ *is radical of degree D, of dimension* $k-1$ *and that:* $\mathcal{J} \cap \mathbb{K}(t)[\underline{z}]$ *is principal and* $\mathcal{J}$ *induces an ideal* $\mathcal{J}_{z_1} \subset \mathbb{K}(t, \underline{z})[x, u, z_1]$ *of dimension* 0*. Suppose given a straight-line program of length L evaluating the polynomials defining* $\mathcal{J}$*. Then computing a generator of* $\mathcal{J} \cap \mathbb{K}[t, \underline{z}]$ *and the polynomials* $\chi, \partial_{z_1}\chi, \ldots, \partial_{z_1}^{k-1}\chi$ *can be done in* $\tilde{O}(D^{k+1} \cdot 8^k \cdot (L + k^2) + k \cdot D^{2(k+1)})$ *ops. in* $\mathbb{K}$.

Proof. We first denote by $\mathcal{J}_{z_1}$ the induced ideal of dimension 0 in $\mathbb{K}(t, \check{z}_1)[x, u, z_1]$. Using the radicality and the dimension assumptions, it is possible to compute a parametric geometric resolution of the zero set of $\mathcal{J}_{z_1}$. Applying the algorithm underlying [36, Theorem 2], we compute $A, B \in \mathbb{K}(t, \hat{\underline{z}})[\lambda]$ which give a parametrization $z_1 = A(\lambda)/\partial_\lambda B(\lambda)$ over the field extension defined by $B(\lambda) = 0$. Using [36, Theorem 2], this can be done in $\tilde{O}(D^{k+1} \cdot 8^k \cdot (L + k^2))$ ops. in $\mathbb{K}$. Applying Fact 1(4), χ is equal to the resultant in λ of the numerators of B and $z_1 \cdot \partial_\lambda B - A$. Using now fast computation of bivariate resultants [28, §5] and using the upper bound D [36, Theorem 1] on the partial degrees of the coefficients of both the numerator and denominator of A and B, we obtain that the number of evaluation-interpolation points needed for $t, \check{z}_1$ is $O(D^{2k})$. This gives a cost in $\tilde{O}(D^{2k+1.63})$ ops. in $\mathbb{K}$ for computing the numerator of χ, whose partial degrees are bounded by D^2. Finally, if L' is the length of a straight-line program evaluating χ, Theorem 1 in [4] allows us to compute $\partial_{z_1}\chi, \ldots, \partial_{z_1}^{k-1}\chi$ using $\tilde{O}(k \cdot L') \subset \tilde{O}(k \cdot D^{2(k+1)})$ ops. in $\mathbb{K}$. This yields a final complexity in $\tilde{O}(D^{k+1} \cdot 8^k \cdot (L + k^2) + k \cdot D^{2(k+1)})$ ops. in $\mathbb{K}$. As $\mathcal{J}$ is assumed radical, a generator of $\mathcal{J} \cap \mathbb{K}[t, \underline{z}]$ is given by the squarefree part of χ. The cost of this squarefree part computation is negligible and absorbed in the above complexity. □

Remark 6.1. **(i)** When the numerator of the characteristic polynomial of m_{z_1} generates $\mathcal{J} \cap \mathbb{K}[t, \underline{z}]$, the complexity of Lemma 6.3 drops to $\tilde{O}(D^{k+1} \cdot 8^k \cdot (L + k^2) + k \cdot D^{k+1}) \subset \tilde{O}(D^{k+1} \cdot 8^k \cdot (L + k^2))$.

(ii) Lemma 6.3 allows with the same complexity to compute the characteristic polynomial ξ_u of the multiplication map m_u. Denoting by χ_u the numerator of ξ_u, the refinement of $\mathcal{S}_k(\check{z_1}, \mathscr{V})$ consisting in counting only the distinct solutions w.r.t. u is equivalent to considering the polynomial $m \cdot \mathrm{disc}_u(\chi_u) - 1$ (and then eliminating m). Another useful practical refinement consists in adding to the polynomials defining $\overline{\mathcal{S}_k(\check{z_1}, \mathscr{V})}$ all the polynomials defining $\overline{\mathcal{S}_k(\check{z_i}, \mathscr{V})}$, for all $0 \leq i \leq k-1$ (by a slight adaptation of the present section).

Lemmas 6.2 and 6.3 yield an algorithm whose output characterizes $\overline{\mathcal{S}_k(\check{z_1}, \mathscr{V})}$, and prove its complexity. As most of the combinatorial examples we have encountered so far are stated with $\mathbb{K} = \mathbb{Q}$, our aim is to take in practice the benefit of fast multi-modular arithmetic. We prefer to reduce the computations in $\mathbb{Q}$ instead of $\mathbb{Q}(t)$ by using evaluation-interpolation on the parameter t. In practice, the underlying algorithm makes use of the specialization properties of Gröbner bases [20, Prop. 1, p. 308].

Proposition 6.4. *Let* $P \in \mathbb{K}[x, \underline{z}, t, u]$ *be as in* (3)*,* $a \in \mathbb{K}$ *and define* $\mathcal{J} := \langle P, \partial_x P, \partial_u P\rangle : (u-a)^\infty \subset \mathbb{K}(t)[x, u, \underline{z}]$*. We assume that:* **(H1)**, **(H3)**, $(\mathcal{Z})$ *and* (S) *hold and that the input assumptions of Lemma 6.3 are satisfied by the ideal* $\mathcal{J}$*. Then any nonzero* $R \in (\mathcal{J} \cap \mathbb{K}(t)[\underline{z}] + \langle \chi, \partial_{z_1}\chi, \ldots, \partial_{z_1}^{k-1}\chi\rangle) \cap \mathbb{K}[t, z_0]$ *satisfies* $R(t, F(t, a)) = 0$*.*

Proof. Using the algorithm underlying the proof of Lemma 6.3, we compute a generator of $\mathcal{J} \cap \mathbb{K}(t)[\underline{z}]$ and $\chi, \partial_{z_1}\chi, \ldots, \partial_{z_1}^{k-1}\chi$. Now using Lemma 6.2, the zero set of $(\mathcal{J} \cap \mathbb{K}(t)[\underline{z}] + \langle \chi, \partial_{z_1}\chi, \ldots, \partial_{z_1}^{k-1}\chi\rangle)$ is $\mathcal{S}_k(\check{z}_1, \overline{\mathcal{X}})$. Hence applying [20, Thm. 3, §2, Ch. 3], the zero set of $(\mathcal{J} \cap \mathbb{K}(t)[\underline{z}] + \langle \chi, \partial_{z_1}\chi, \ldots, \partial_{z_1}^{k-1}\chi\rangle) \cap \mathbb{K}[t, z_0]$ is the Zariski closure of the projection of $\mathcal{S}_k(\check{z}_1, \overline{\mathcal{X}})$ onto the z_0-coordinate space, which by **(H1)** contains $F(t, a)$. Hence as by **(H3)** the latter elimination ideal is not reduced to 0, any element of it annihilates $F(t, a)$. □

7 CONCLUSION AND PERSPECTIVES

Extensive practical experiments on DDEs of type (2)–(3) defined by dense polynomials f and Q show that the growth order estimate δ^{3k} for the algebraicity degree of $F(t,a)$ in Prop. 3 is very likely to be sharp in the worst case, and actually reached in the "generic" case. For instance, when $k=1$ we observe that, on random examples, the minimal polynomial $M \in \mathbb{Q}[t,z_0]$ of $F(t,a)$ satisfies $\deg_{z_0} M = \delta(\delta^2-\delta+1)$ and $\deg_t M = 2\delta^3+\delta^2-3\delta+2$. For $k=2$, we managed to compute the degrees in z_0 for $\delta = 4, 7, 10, 13, 16$ (corresponding to $\deg(Q) = \deg(f) \in \{1,2,3,4,5\}$) and obtained successively $\deg_{z_0} M = 1, 38, 870, 5824$ and 24235. This makes us very confident that the asymptotic growth of $\deg_{z_0} M$ is of order $\delta^{3\cdot 2} = \delta^6$. However, we do not have a proof that δ^{3k} indeed matches the right order of magnitude of $\deg_{z_0} M$ and of $\deg_t M$.

Since we believe that the output R of our algorithms has (generically) arithmetic size $A = \deg_{z_0} R \cdot \deg_t R = \delta^{3k} \cdot \delta^{3k} = \delta^{6k}$, exponentiality in k is unavoidable in the complexity estimates: any algorithm for computing R would need at least δ^{6k} ops. From this perspective, the estimate in Prop. 4 is quite good, since it is $O(A^{4/3})$.

Our algorithms are not only fast in theory, but also efficient in practice. Moreover, they allow to solve nontrivial combinatorial applications, as showed by the experimental results in Section 8. Our implementations yielded practical improvements for a large majority of them, and allowed us to solve one (5-constellations) on which the state-of-the-art methods could not terminate.

For future works, we wish to develop complete implementations of the algorithms that we have introduced in the present paper, and to make them available for the combinatorics community. A different, more theoretical direction, is to pursue the geometrical investigation analysis of the problem of computing exceptional fibers initiated in Sections 5 and 6.

8 EXPERIMENTS

Aim. We first report on practical variants of the hybrid guess-and-prove method (hgp) and then provide and analyze tables of our implementations of Sections 3 to 6. The benchmark DDEs on which we test our various implementations have combinatorial origins and the literature qualifies their resolution as a highly nontrivial problem. More precisely, we consider solving: Eq. (4.22) in [6] ("near-triangulations"), Prop. 12 in [11] ("m-constellations", $m \in \{4,5\}$) and Eq. (3) in [10] ("3-Tamari lattices").

Recall that the input of the algorithms in Sections 3 to 6 consists of a polynomial P as in (3) and of a specialization point $a \in \mathbb{K}$, while their output is, under (**H3**) and up to eliminating variables, a nonzero polynomial $R \in \mathbb{K}[t,z_0]$ such that $R(t,F(t,a)) = 0$.

Implementations. The DDEs we consider being defined over $\mathbb{K} = \mathbb{Q}$, we use multi-modular arithmetic and CRT (Chinese Remainder Theorem) for Sections 3, 5 and 6. Also, we reduce the computation from $\mathbb{Q}(t)$ to $\mathbb{Q}$ by performing evaluation-interpolation ("ev.-int.") on either t or z_0. We incorporate (**ii**) of Rmk. 6.1, but do not use the inequalities describing $\mathcal{S}^{(k)}$ in Section 5. Finally, we use standard tools in computer algebra to improve each of our implementations.

The practical variant of the hgp strategy mentioned above has the following motivation. When one performs (say, for a "random" prime p) the computation of a modular image R_p of R by using one of Sections 3, 5 and 6, the computation (if it ends) gives access to the partial degrees of $R \in \mathbb{Q}[t,z_0]$. If either one modular computation or the lift over $\mathbb{Q}$ is too time consuming, the following variant of hgp exploits the knowledge of those partial degrees:

- Pick a random prime $2^{27} < p < 2^{31}$ and $\theta \in \{1,\dots,p-1\}$,
- Compute $R_p(t,\theta) \in \mathbb{F}_p[t]$ and $R_p(\theta,z_0) \in \mathbb{F}_p[z_0]$ using one of Sections 3, 5 and 6; set d_t and d_{z_0} their respective degrees,
- Compute $F(t,a) \bmod t^{2d_t d_{z_0}+1}$,
- Guess $\tilde{R} \in \mathbb{Q}[t,z_0]$ s.t. $\tilde{R}(t,F(t,a)) = O(t^{(d_t+1)(d_{z_0}+1)-1})$,
- Check that $\tilde{R}(t,F(t,a)) = O(t^{d_t \cdot \deg_{z_0}(\tilde{R}) + \deg_t(\tilde{R})\cdot d_{z_0}+1})$.

The above algorithm is a simple extension of the one in [8, §2.2.2], with the total degree replaced by partial degrees. Also, our implementation generates terms of $F(t,a)$ by first computing terms of $F(t,u)$ and then specializing to $u=a$. Any optimization of this step would result in much better timings for the hgp strategy.

In our experiments, we consider the following data:

- **S**: sections (and hence algorithms) used,
- **#$\mathcal{P}$**: number of primes used for the CRT,
- **Z** $\in \{t,z_0\}$ the variable on which we perform ev.-int.,
- **#pts**: number of ev.-int. points needed in Z,
- $\mathbf{d_{cp}}$: critical pairs of maximal degree in GB computations,
- $\mathbf{d_M}$: Macaulay matrix maximal size in GB computations (F4),
- $\mathbf{d}_{\mathcal{I}_\infty}$: degree of the ideal $\mathcal{I}_\infty$ in Section 3,
- $\mathbf{d}_\chi$: degree of $\chi_{z_1} \in \mathbb{Q}[t,\underline{z}]$,
- **T**: total timing needed to obtain an output in $\mathbb{Q}[t,z_0]$,
- $\mathbf{d_Z}$: degree in Z of output $R \in \mathbb{Q}[t,z_0]$ s.t. $R(t,F(t,a)) = 0$,
- σ: truncation order in the expansion of $F(t,a)$,
- **G**: time spent for guessing an annihilating polynomial in $\mathbb{Q}[t,z_0]$,
- **P**: time spent to prove the guess.

The timings are given in seconds (s.), minutes (m.), hours (h.) and days (d.). The symbol ∞ (resp. $-$, $\times$) means that the computation (resp. the data) did not finish (resp. was not known, is not defined) after 5 days.

All computations were conducted using Maple on a computer equipped with Intel® Xeon® Gold CPU 6246R v4 @ 3.40GHz and 1.5TB of RAM with a single thread. All Gröbner bases computations were performed using the C library msolve [7], and all guessing computations were performed using the gfun Maple package [34].

We obtain the following tables:

[6, Proposition 4.3], $k=2$

S	#$\mathcal{P}$	Z	#pts	$\mathbf{d_{cp}}$	$\mathbf{d_M}$	$\mathbf{d}_{\mathcal{I}_\infty}$	$\mathbf{d}_\chi$	T	$\mathbf{d_t}$	$\mathbf{d_{z_0}}$
Section 3	3	t	265	18	$4\cdot10^5 \times 4\cdot10^5$	12	$\times$	55s	132	6
Section 5	3	t	265	206	$2\cdot10^4 \times 2\cdot10^4$	$\times$	$\times$	1m10s	132	6
Section 6	$\times$	$\times$	$\times$	$\times$	$\times$	$\times$	469	30s	1173	33

S	$\mathbf{d_t}$	$\mathbf{d_{z_0}}$	σ	G	P	T
Sections 4 and 6	132 (7m)	6 (0.4s)	mod t^{2048} (∞)	–	–	–

4-constellations, $k=3$

S	#$\mathcal{P}$	Z	#pts	$\mathbf{d_{cp}}$	$\mathbf{d_M}$	$\mathbf{d}_{\mathcal{I}_\infty}$	$\mathbf{d}_\chi$	T	$\mathbf{d_t}$	$\mathbf{d_{z_0}}$
Section 3	3	t	7	9	$3\cdot10^4 \times 3\cdot10^4$	42	$\times$	4m	3	7
Section 5	3	t	7	33	$7\cdot10^3 \times 11\cdot10^3$	$\times$	$\times$	41s	3	7
Section 6	3	t	7	51	$2\cdot10^5 \times 2\cdot10^5$	$\times$	28	83s	3	7

S	$\mathbf{d_t}$	$\mathbf{d_{z_0}}$	σ	G	P	T
Sections 4 and 5	3 (1s)	7 (1.5s)	mod t^{64} (18s)	0.03s	0.001s	20s

3-Tamari, $k=3$

S	#$\mathcal{P}$	Z	#pts	$\mathbf{d_{cp}}$	$\mathbf{d_M}$	$\mathbf{d}_{\mathcal{I}_\infty}$	$\mathbf{d}_\chi$	T	$\mathbf{d_t}$	$\mathbf{d_{z_0}}$
Section 3	4	t	11	11	$3\cdot10^5 \times 3\cdot10^5$	96	$\times$	2d2h	5	16
Section 5	4	z_0	33	64	$10^4 \times 10^4$	$\times$	$\times$	2m	5	16
Section 6	4	t	11	52	$10^4 \times 10^4$	$\times$	31	5m42s	5	16

S	$\mathbf{d_t}$	$\mathbf{d_{z_0}}$	σ	G	P	T
Sections 4 and 5	5 (0.2s)	16 (5s)	mod t^{256} (1h40m)	1s	0.2s	1h40m

5-constellations, $k = 4$

S	$\#\mathcal{P}$	Z	#pts	$\mathrm{d_{cp}}$	$\mathrm{d_M}$	$\mathrm{d}_{\mathcal{I}_\infty}$	d_χ	T	$\mathrm{d_t}$	$\mathrm{d_{z_0}}$
Section 3	–	–	–	–	–	–	×	∞	–	–
Section 5	–	t	53	70	$2 \cdot 10^6 \times 2 \cdot 10^6$	×	×	∞	26	53
Section 6	–	–	–	–	–	×	–	∞	–	–

S	$\mathrm{d_t}$	$\mathrm{d_{z_0}}$	σ	G	P	T
Sections 4 and 5	26 (47m)	53 (45m)	mod t^{256} (4h35m)	0.03s	0.02s	6h7m

Interpretation. A first natural observation is that the algorithms introduced in Sections 3 to 6, as well as their practical variants, are relevant in practice. Moreover, for all the examples, there is always one of the new methods which is more efficient in terms of timings than the state-of-the-art (Section 3). According to the tables, there is generally no unique method that is always better than the others. On the contrary, the experiments show that all the new methods can be useful in practice, depending on the DDEs under study (and hence on the properties of the associated zero sets).

We now explain the tables related to 5-constellations. Note first that neither Section 3 nor Section 6 allow to compute any single specialization (at t or z_0 specialized) of a modular image of R. Now applying Section 5, we manage to compute two specializations (first in t, then in z_0) of R_p, for some "random" prime p. This hence gives all the relevant data of the line except $\#\mathcal{P}$ and **T**. Those two specializations take respectively 45m. and 47m. The degrees obtained being $d_{z_0} = 53$ and $d_t = 26$, we would need approximately $53 \cdot 45\text{min} = 39\text{h}$ for each modular computation. Estimating the number of such modular computations to be 5 (which is very likely optimistic), we would hence need at least 8 days. Instead of this, we use the practical variant of Section 4 mentioned in the current section. As the degree of the guessed polynomial is low ($\deg_t = 2$ and $\deg_{z_0} = 5$), it allows us to compute 256 terms of the series $F(t, 1)$ (here $a = 1$), and to check the guess with the geometric bounds d_t, d_{z_0} obtained previously.

ACKNOWLEDGEMENTS

We thank the reviewers for their very helpful comments and suggestions to improve our paper. The three authors are supported by the French grant DeRerumNatura (ANR-19-CE40-0018) and by the French–Austrian project EAGLES (ANR-22-CE91-0007 & FWF I6130-N). The last author is supported by the joint ANR-FWF ANR-19-CE48-0015 ECARP project, and the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement N. 813211 (POEMA).

REFERENCES

[1] F. Ardila. Algebraic and geometric methods in enumerative combinatorics. In *Handbook of enumerative combinatorics*, Discrete Math. Appl., pages 3–172. CRC Press, 2015.
[2] C. Banderier and P. Flajolet. Basic analytic combinatorics of directed lattice paths. volume 281, pages 37–80. 2002. Selected papers in honour of M. Nivat.
[3] S. Basu, R. Pollack, and M.-F. Roy. *Algorithms in real algebraic geometry*, volume 10 of *Algorithms and Computation in Mathematics*. Springer, second edition, 2006.
[4] W. Baur and V. Strassen. The complexity of partial derivatives. *Theoret. Comput. Sci.*, 22(3):317–330, 1983.
[5] E. A. Bender and E. R. Canfield. The number of degree-restricted rooted maps on the sphere. *SIAM J. Discrete Math.*, 7(1):9–15, 1994.
[6] O. Bernardi. On triangulations with high vertex degree. *Ann. Comb.*, 12(1):17–44, 2008.
[7] J. Berthomieu, C. Eder, and M. Safey El Din. `msolve`: a library for solving polynomial systems. In *ISSAC'21*, pages 51–58. ACM, 2021.
[8] A. Bostan, F. Chyzak, H. Notarantonio, and M. Safey El Din. Algorithms for discrete differential equations of order 1. In *ISSAC'22*, pages 101–110. ACM, 2022.
[9] A. Bostan, C.-P. Jeannerod, and É. Schost. Solving structured linear systems with large displacement rank. *Theoret. Comput. Sci.*, 407(1-3):155–181, 2008.
[10] M. Bousquet-Mélou, E. Fusy, and L.-F. Préville-Ratelle. The number of intervals in the m-Tamari lattices. *Electron. J. Combin.*, 18(2):Paper 31, 26, 2012.
[11] M. Bousquet-Mélou and A. Jehanne. Polynomial equations with one catalytic variable, algebraic series and map enumeration. *J. Combin. Theory Ser. B*, 96(5):623–672, 2006.
[12] M. Bousquet-Mélou and M. Petkovšek. Linear recurrences with constant coefficients: the multivariate case. *Discrete Math.*, 225(1-3):51–75, 2000. *FPSAC'98*.
[13] M. Bousquet-Mélou and G. Schaeffer. Enumeration of planar constellations. *Adv. in Appl. Math.*, 24(4):337–368, 2000.
[14] M. Bousquet-Mélou and M. Wallner. More Models of Walks Avoiding a Quadrant. In *AofA'20*, volume 159 of *Leibniz Int. Proc. Inform. (LIPIcs)*, pages 8:1–8:14, 2020.
[15] W. G. Brown. Enumeration of triangulations of the disk. *Proc. London Math. Soc. (3)*, 14:746–768, 1964.
[16] W. G. Brown. Enumeration of quadrangular dissections of the disk. *Canadian J. Math.*, 17:302–317, 1965.
[17] W. G. Brown. On the existence of square roots in certain rings of power series. *Math. Ann.*, 158:82–89, 1965.
[18] F.-J. Castro-Jiménez, D. Popescu, and G. Rond. Linear nested Artin approximation theorem for algebraic power series. *Manuscripta Math.*, 158(1-2):55–73, 2019.
[19] D. A. Cox. Stickelberger and the eigenvalue theorem. In *Commutative algebra*, pages 283–298. Springer, 2021.
[20] D. A. Cox, J. Little, and D. O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer, fourth edition, 2015. An introduction to computational algebraic geometry and commutative algebra.
[21] M. Drmota. Systems of functional equations. *Random Structures & Algorithms*, 10(1-2):103–124, 1997.
[22] R. Duan, H. Wu, and R. Zhou. Faster matrix multiplication via asymmetric hashing, 2022. Technical Report 2210.10173, arXiv.
[23] J.-C. Faugère and J. Svartz. Solving polynomial systems globally invariant under an action of the symmetric group and application to the equilibria of N vortices in the plane. In *ISSAC'12*, pages 170–178. ACM, 2012.
[24] P. Flajolet and R. Sedgewick. *Analytic combinatorics*. Cambridge University Press, Cambridge, 2009.
[25] J. von zur Gathen and J. Gerhard. *Modern computer algebra*. Cambridge Univ. Press, third edition, 2013.
[26] P. Giorgi, C.-P. Jeannerod, and G. Villard. On the complexity of polynomial matrix computations. In *ISSAC'03*, pages 135–142. ACM, 2003.
[27] J. Heintz. Definability and fast quantifier elimination in algebraically closed fields. *Theoret. Comput. Sci.*, 24(3):239–277, 1983.
[28] S. G. Hyun, V. Neiger, and É. Schost. Implementations of efficient univariate polynomial matrix algorithms and application to bivariate resultants. In *ISSAC'19*, pages 235–242. ACM, 2019.
[29] M. Kalkbrener. On the stability of Gröbner bases under specializations. *J. Symbolic Comput.*, 24(1):51–58, 1997.
[30] D. E. Knuth. *The art of computer programming. Vol. 1: Fundamental algorithms*. Second printing. Addison-Wesley, Reading, MA, 1968.
[31] H. Notarantonio and S. Yurkevich. Effective algebraicity for solutions of systems of functional equations with one catalytic variable. In *FPSAC'23*, to appear.
[32] D. Popescu. General Néron desingularization and approximation. *Nagoya Math. J.*, 104:85–115, 1986.
[33] M. Safey El Din and É. Schost. A nearly optimal algorithm for deciding connectivity queries in smooth and bounded real algebraic sets. *J. ACM*, 63(6):48:1–48:37, 2017. Online supplemental material at https://dl.acm.org/doi/10.1145/2996450.
[34] B. Salvy and P. Zimmermann. Gfun: a Maple package for the manipulation of generating and holonomic functions in one variable. *ACM Trans. Math. Software*, 20(2):163–177, 1994.
[35] G. Schaeffer. Planar maps. In *Handbook of enumerative combinatorics*, Discrete Math. Appl., pages 335–395. CRC Press, 2015.
[36] É. Schost. Computing parametric geometric resolutions. *Appl. Algebra Eng. Commun. Comput.*, 13(5):349–393, 2003.
[37] R. P. Stanley. *Enumerative combinatorics. Vol. 2*, volume 62 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1999.
[38] W. T. Tutte. On the enumeration of planar maps. *Bull. AMS*, 74:64–74, 1968.
[39] D. Zeilberger. A proof of Julian West's conjecture that the number of two-stack-sortable permutations of length n is $2(3n)!/((n+1)!(2n+1)!)$. *Discrete Math.*, 102(1):85–93, 1992.
[40] D. Zeilberger. The umbral transfer-matrix method. I. Foundations. volume 91, pages 451–463. 2000. In memory of Gian-Carlo Rota.