Algorithms for discrete differential equations of order 1

Alin Bostan, Frédéric Chyzak, Hadrien Notarantonio, Mohab Safey El Din

Algorithms for discrete differential equations of order 1

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

Frédéric Chyzak
Inria
Palaiseau, France
frederic.chyzak@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 of order 1 are equations relating polynomially $F(t,u)$, a power series in t with polynomial coefficients in a "catalytic" variable u, and one of its specializations, say $F(t,1)$. Such equations are ubiquitous in combinatorics, notably in the enumeration of maps and walks. When the solution F is unique, a celebrated result by Bousquet-Mélou, reminiscent of Popescu's theorem in commutative algebra, states that F is *algebraic*. We address algorithmic and complexity questions related to this result. In *generic* situations, we first revisit and analyze known algorithms, based either on polynomial elimination or on the guess-and-prove paradigm. We then design two new algorithms: the first has a geometric flavor, the second blends elimination and guess-and-prove. In the *general* case (no genericity assumptions), we prove that the total arithmetic size of the algebraic equations for $F(t,1)$ is bounded polynomially in the size of the input discrete differential equation, and that one can compute such equations in polynomial time.

ACM Reference Format:
Alin Bostan, Frédéric Chyzak, Hadrien Notarantonio, and Mohab Safey El Din. 2022. Algorithms for discrete differential equations of order 1. In *Submitted*. New York, NY, USA, 10 pages.

1 INTRODUCTION

Context and motivation. In enumerative combinatorics, many classes of objects (e.g., walks, maps, permutations) obey various sets of structural constraints (e.g., evolution domains, colorings). A common method to study and understand such classes is to first translate the structural constraints into a *functional equation* in one or several generating functions, then to solve that equation. Very often, if not always, this process intrinsically requires to introduce auxiliary variables—called *catalytic*[1] in what follows—leading to an equation that relates the complete function with the partial functions obtained by specializing the catalytic variables. Solving such equations and understanding the nature of their solutions is an important problem with connections to graph theory [38], theoretical physics [21] and computational geometry [26].

[1]This terminology originates from chemistry, and it was introduced in combinatorics by Zeilberger in 2000 [59, p. 457]. In computer algebra, the wording *catalyst variables* had been used by Bayer and Stillman in 1988 [6, §2], in their description and analysis of the celebrated construction due to Mayr and Meyer [44].

There are many reasons why it is important to be able to predict the nature of the generating function of some class of combinatorial objects. For instance, knowing that a class of objects is counted by an *algebraic function* (i.e., root of a polynomial) suggests that it should be possible to construct these objects recursively by *concatenation* of objects of the same type. For many objects, such a construction is easily found, but for others, among which planar maps and walks, the algebraic structure of the objects is far from clear, and the algebraicity of the generating function gives rise to challenging combinatorial problems. A different type of motivation comes from the fact that the class of algebraic functions is closed under natural operations (sum, product, derivative) that reflect natural operations on combinatorial classes (disjoint union, Cartesian product, pointing–erasing). Finally, the coefficients of algebraic generating functions can be computed fast [14, 28, 29], and their asymptotic behavior can be precisely determined [33, §VII. 7]; this in turn allows for a very efficient enumeration, and also for quick generation of random objects of a given size.

Three examples. The simplest example of a functional equation with catalytic variables arises in the enumeration of *Dyck walks*: these are walks on the half-line $\mathbb{N}$ that start from 0 and consist of unit steps ± 1. If one wants to find the number d_n of Dyck walks of length n (the length counts the number of used steps), or equivalently to understand the generating function $D(t) := \sum_{n\geq 0} d_n t^n$, then a convenient way is to introduce a catalytic variable u that takes into account the abscissa of the endpoint. In other words, one introduces a bivariate power series $F(t,u) := \sum_{n,k} a_{n,k} u^k t^n$, where $a_{n,k}$ is the number of n-step walks that end at abscissa k. Then, $D(t) = F(t,1)$. A step-by-step construction of Dyck walks gives the recurrence relation $a_{n+1,k} = a_{n,k-1} + a_{n,k+1}$, valid for $n \geq 0$ and any k, with initial conditions $a_{0,0} = 1$ and $a_{n,k} = 0$ if $n < 0$ or $k < 0$. Equivalently, the construction yields the equation

$$F(t,u) = 1 + t\left(uF(t,u) + \frac{F(t,u) - F(t,0)}{u}\right). \tag{1}$$

The functional equation (1) is *linear* and *with one catalytic variable*. It clearly defines $F(t,u)$ uniquely as a formal power series in t, with coefficients in $\mathbb{Q}(u)$. In fact, it is easy to see that the unique solution in $\mathbb{Q}(u)[[t]]$ of (1) actually belongs to $\mathbb{Q}[u][[t]]$. This is a consequence of the fact that the *divided difference*, or the *discrete derivative*, operator $\Delta : F(t,u) \mapsto (F(t,u) - F(t,0))/u$ maps $\mathbb{Q}[u][[t]]$ to itself. Rewritten as $F = 1 + t\cdot(u\cdot F + \Delta F)$, equation (1) is a *discrete differential equation* (DDE), linear and of order 1.

A second example is provided by the enumeration of planar maps. If $c_{n,d}$ is the number of such maps with n faces and external face of degree d, then the generating series $F(t,u) := \sum_{n,d} c_{n,d} u^d t^n$ is the unique solution in $\mathbb{Q}[u][[t]]$ of the functional equation

$$F(t,u) = 1 + t\left(u^2 F(t,u)^2 + u\frac{uF(t,u) - F(t,1)}{u-1}\right). \tag{2}$$

Equation (2) is similar to equation (1) as it also involves *a single catalytic variable*, but it is more complicated as it is *nonlinear*. It also admits a unique solution in $\mathbb{Q}[u][[t]]$, due to the fact that the divided difference operator $\Delta_1 : F(t,u) \mapsto (F(t,u)-F(t,1))/(u-1)$ maps $\mathbb{Q}[u][[t]]$ to itself. Equation (2) was written (and solved) in 1968 by Tutte [55], who obtained it by the so-called *recursive method* for maps, based on deletion and contraction of edges: a map is either reduced to a single vertex, or, after deleting its root-edge either two connected components are left (which gives the term $tu^2F(t,u)^2$) or only one is left (giving the term $tu\Delta_1(uF(t,u))$). Rewritten as $F = 1 + tu\cdot(u\cdot F^2 + F + \Delta_1 F)$, eq. (2) is a nonlinear DDE of order 1.

A third example arises from the enumeration of the so-called *intervals in the 2-Tamari lattices* [19, Ex. 2, §2.3]. In that context, the bivariate generating function $F(t,u)$ satisfies the equation

$$F(t,u) = u + \frac{tuF(t,u)}{u-1}\left(F(t,u)\frac{F(t,u)-F(t,1)}{u-1} - F(t,1)\partial_u F(t,1)\right),$$

which can be rewritten as the following nonlinear DDE of order 2:

$$F = u + tu\cdot F\cdot\left((\Delta_1 F)^2 + F\cdot\Delta_1^2 F - (u-1)\cdot\Delta_1 F\cdot\Delta_1^2 F\right). \quad (3)$$

Equations (1), (2) and (3) share the (a priori unexpected) property that their unique solution $F(t,u)$ in $\mathbb{Q}[u][[t]]$ is *algebraic*: this means that in the three cases $F(t,u)$ satisfies a nontrivial polynomial equation $S(F(t,u),t,u) = 0$, for some $S(x,t,u) \in \mathbb{Q}[x,t,u] \setminus \{0\}$. As a consequence, its specialization at $u = 1$ (or some other value) is also algebraic, i.e. a root of a nonzero polynomial in $\mathbb{Q}[x,t]$, namely $S(x,t,1)$ if S is taken irreducible. More precisely, for eq. (1), the generating function of Dyck walks, $F(t,1) = 1 + t + 2t^2 + 3t^3 + 6t^4 + 10t^5 + 20t^6 + \cdots$, is a root of $t\,(2t-1)\,x^2 + (2t-1)\,x + 1$, for eq. (2), the generating function of planar maps, $F(t,1) = 1 + 2t + 9t^2 + 54t^3 + 378t^4 + \cdots$, is a root of $27t^2x^2 + (1-18t)\,x + 16t - 1$, and for eq. (3), the generating function of intervals in the 2-Tamari lattices, $F(t,1) = 1 + t + 6t^2 + 58t^3 + 703t^4 + \cdots$, is a root of

$$t^4x^9 - 16t^3x^7 + 81t^3x^6 + 96t^2x^5 + 4968t^2x^4 + \left(2187t^2 - 256t\right)x^3 + 11664t\,x^2 + \left(256 - 31347t\right)x + 19683t - 256.$$

A general algebraicity result. Bousquet-Mélou and Jehanne [20] proved in 2006 the following general result, which guarantees algebraicity of the solution of any functional equation with one catalytic variable such as (1), (2) or (3).

Theorem 1.1. ([20, 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 $\Delta_a^{(i)}$ the operator obtained by applying i times Δ_a. Then, there exists a unique solution $F \in \mathbb{K}[u][[t]]$ of the equation*

$$F(t,u) = f(u) + t\,Q(F(t,u), \Delta_a F(t,u), \ldots, \Delta_a^{(k)} F(t,u), t, u), \quad (4)$$

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

In short, Theorem 1.1 says that solutions in $\mathbb{K}[u][[t]]$ of *ordinary* discrete differential equations (w.r.t. the catalytic variable u) are necessarily *algebraic*. This result applies to all equations of the form

$$F(t,u) = f(u) + t\,\tilde{Q}(F(t,u), \partial_u F(t,a), \ldots, \partial_u^{k-1} F(t,a), t, u), \quad (5)$$

for any polynomial $\tilde{Q} \in \mathbb{K}[x, z_0, \ldots, z_{k-1}, t, u]$; indeed, (5) is a particular case of (4), since

$$\partial_u^i F(t,a) = i!\cdot\left(\Delta_a^{(i)} F(t,u) - (u-a)\cdot\Delta_a^{(i+1)} F(t,u)\right).$$

Theorem 1.1 does not generalize to *partial* discrete differential equations; for instance, solutions in $\mathbb{K}[u,v][[t]]$ of equations with two catalytic variables u and v may be transcendental. A simple example is the linear equation

$$F(t,u,v) = 1 + t\Big((u+v)F(t,u,v) + \Delta_{u,0}F(t,u,v) + \Delta_{v,0}F(t,u,v)\Big)$$

which occurs in the enumeration of $\{\rightarrow,\uparrow,\leftarrow,\downarrow\}$-walks in $\mathbb{N}^2$. In this case, $F(t,0,0) = 1 + 2t^2 + 10t^4 + 70t^6 + \cdots$ equals $\sum_{n\geq 0} C_n C_{n+1} t^{2n}$, where $C_n = \frac{1}{n+1}\binom{2n}{n}$, hence $F(t,0,0)$ is transcendental [15].

There are however some important extensions of Theorem 1.1. For instance, Theorem 14 in [8, §9] addresses the more general case where $F \in \mathbb{K}[u,u^{-1}][[t]]$ satisfies an equation of the form (4), where f lies in $\mathbb{K}[u,u^{-1}]$ and Q lies in $\mathbb{K}(u)[x, z_0, \ldots, z_{k-1}, t]$. In a different direction, Theorem 16 in [11] addresses the system analogue of (4), and provides a vast generalization of Theorem 1.1. This result is actually a consequence of a deep theorem in commutative algebra, on Artin approximation with nested conditions, due to Popescu [47, Thm. 1.4]. However, while the results in [8, 20] are proved in a constructive fashion, Popescu's theorem, as well as Theorem 16 in [11], are not known to admit constructive proofs.

Setting and main goal. In the rest of the paper, we will restrict to the setting of Theorem 1.1 and only to discrete differential equations of order $k = 1$, that is to equations of the form

$$F(t,u) = f(u) + t\,Q(F(t,u), \Delta_a F(t,u), t, u), \quad (6)$$

where $a \in \mathbb{K}$, $f \in \mathbb{K}[u]$ and $Q \in \mathbb{K}[x,y,t,u]$ are given.

Equation (6) can be written in the equivalent form[2]

$$F(t,u) = f(u) + t\,\tilde{Q}(F(t,u), F(t,a), t, u), \quad (7)$$

where $\tilde{Q} \in \mathbb{K}(u)[x,z,t]$, is given by $\tilde{Q}(x,z,t,u) = Q\left(x, \frac{x-z}{u-a}, t, u\right)$. Upon multiplying by a sufficiently high power of $(u-a)$, equation (7) can itself be rewritten as

$$P(F(t,u), F(t,a), t, u) = 0, \quad (8)$$

for some nonzero polynomial $P \in \mathbb{K}[x,z,t,u]$.

By Theorem 1.1, equations (6)–(8) admit a unique solution $F \in \mathbb{K}[u][[t]]$, and this solution is *algebraic* over $\mathbb{K}(t,u)$. In particular, $F(t,a)$ is algebraic over $\mathbb{K}(t)$. The main goal of the paper is to review, design and analyze several algorithms for computing a nonzero polynomial $R \in \mathbb{K}[z,t]$ such that $R(F(t,a),t) = 0$. (See Ex. 5.1.)

For each algorithm for computing such an R starting from P defining equations (6)–(8), we aim at giving complexity estimates, expressed in terms of $\delta := \deg P$. As an intermediate step, we will provide upper bounds on the degrees of the output polynomial R.

Previous work. For DDEs, either linear or nonlinear, algebraicity of solutions is granted by Popescu's aforementioned theorem [47]. However, the proof of this *existential and qualitative* result is not constructive. Hence, to go further, towards *constructive and quantitative* results, different approaches are needed. One such effective

[2] Note that in order to simplify notation, we renamed y_1 into y, and z_0 into z.

method, called the *kernel method* (terminology coined in [4]), applies uniformly to any *linear* DDE. This case can be considered as fully understood, mathematically and algorithmically.

We therefore restrict to the nonlinear case in what follows. Since F satisfies equation (8) if and only if it satisfies it with P replaced by its squarefree part, we make the following global assumption in the remaining part of the paper.

$$\underline{\text{Global Hypothesis:}}\ \deg_x(P) \geq 2 \text{ and } P \text{ is squarefree.} \qquad \textbf{(GH)}$$

(All subsequent assumptions will implicitly contain assumption **GH**.)

The first *non-linear* equations of the form (2) appeared in the early sixties, in the work of Tutte and Brown on (various kinds of) planar maps [23, 24, 54, 55]. All of them have order $k = 1$, hence the form (8), with $P \in \mathbb{Q}[x, z, t, u]$. The first proofs of Tutte and Brown were based on a rudimentary (still, very powerful) form of the so-called *guess-and-prove* paradigm [46], which only applies when one is able to guess an explicit closed formula F_a for $F(t, a)$, the proving step being based on showing that $P(F(t, u), F_a(t), t, u) = 0$ admits a root in $\mathbb{Q}[u][[t]]$. In 1965, Brown invented the so-called *quadratic method* which allows to solve, in a systematic way, all equations (8) with $\deg(P) = 2$. Many years later, in 1994, Bender and Canfield [7] applied Brown's method to the general equation (4) of arbitrary order k, and with $\deg(Q) = 2$. A decade later, Bousquet-Mélou and Jehanne proposed in [20] a far-reaching extension (Thm 1.1) of both the kernel method and of the quadratic method, which applies in principle to any equation of the form (8), and more generally, to any order-k DDE of the form (4). The question is reduced to a (highly structured) algebraic elimination problem.

Coming back to our case $k = 1$, two more methods should be mentioned. One is a *guess-and-prove* algorithm of Gessel and Zeilberger [37], which is to our knowledge the only one fully implemented. It is an improvement of another guess-and-prove method used by Zeilberger in [58] on a particular functional equation, related to the enumeration of two-stack-sortable permutations. A second one is based on [20, Theorem 14], and shows that, under a genericity assumption, a polynomial equation for $F(t, a)$ is provided by the discriminant (in u) of the discriminant (in x) of P in (8).

Complexity basics. We estimate the cost of algorithms by counting arithmetic operations $(+, -, \times, \div)$ in the base field $\mathbb{K}$ at unit cost. We use standard complexity notation, such as $\mathbf{M}(d)$ for the cost of degree-d multiplication in $\mathbb{K}[x]$ and θ for feasible exponents of matrix multiplication. The best known upper bound is $\theta < 2.37286$ [2]. Most arithmetic operations on univariate polynomials of degree d in $\mathbb{K}[x]$ can be performed in quasi-linear complexity $\tilde{O}(d)$: multiplication, shift, interpolation, gcd, resultant, squarefree part, *etc*[3]. A key feature of these results is the reduction to fast polynomial multiplication, which can be performed in time $\mathbf{M}(d) = O(d \log d \log\log d)$ [25, 50]. An excellent general reference for these questions is the book by von zur Gathen and Gerhard [36].

Main results. In Section 2 we analyze, under various genericity assumptions, the complexity of several algorithms for computing a polynomial R annihilating $F(t, a)$. We first prove (Prop. 2.4) the correctness of (a variant of) the iterated discriminant algorithm, and show (Prop. 2.5) that it delivers an R of total arithmetic size $O(\delta^8)$ in $\tilde{O}(\delta^{10})$ ops. in $\mathbb{K}$. Then, we propose (Prop. 2.8 and Prop. 2.9) a new algorithm, with a geometric flavor, that computes a smaller R, of total arithmetic size $O(\delta^6)$, in $\tilde{O}(L \cdot \delta^6 + \delta^{7.89}) \subseteq \tilde{O}(\delta^{10})$ ops. in $\mathbb{K}$, where L is the size of an arithmetic circuit (or, straight-line program) for evaluating P. We also discuss the complexity of guess-and-prove algorithms: we first show (§2.2.1) that the classical approach needs at least $\tilde{O}(\delta^{15})$ ops. in $\mathbb{K}$, and we propose (§2.2.2) a new hybrid guess-and-prove algorithm of complexity $\tilde{O}(L \cdot \delta^6 + \delta^{3\theta+3}) \subseteq \tilde{O}(\delta^{10.12})$. In Section 3, we prove that, in the general case, the polynomial R in Theorem 1.1 has polynomial size $O(\delta^6)$, and that it can be computed in polynomial time $\tilde{O}(L \cdot \delta^9 + \delta^{10.89}) \subseteq \tilde{O}(\delta^{14})$ ops.

Notation. We collect here a few notations that we will freely use throughout the article. As usual, 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 $\mathbb{K}$. Additionally, we will work with the ring $\mathbb{K}[[t^{1/\star}]] := \bigcup_{d\geq 1} \mathbb{K}[[t^{1/d}]]$ of "fractional power series", that is series of the form $U = \sum_{n\geq 0} u_n t^{n/d}$ for some integer $d \geq 1$. We write $\partial_x f$ and alike for the partial derivative of a function f with respect to x, we denote by $\mathrm{Res}_x(p, q)$, resp. by $\mathrm{disc}_x(p)$, the resultant, resp. discriminant, with respect to a variable x. For a polynomial p in n variables over $\mathbb{K}$, we write $V(p)$ for the zero locus of p in $\overline{\mathbb{K}}^n$.

2 SOLVING GENERIC DDEs

2.1 Using polynomial elimination

Bousquet-Mélou and Jehanne proposed in [20] several methods for computing polynomial equations for $F(t, a)$, based on algebraic elimination. These methods work under the following assumption:

$$\underline{\text{Hypothesis 1:}}\ \deg_u(\partial_x P(x, z, 0, u)) \geq 1 \text{ and } \partial_x P(F(t, c), F(t, a), t, c) \neq 0 \text{ for all } c \in \mathbb{K}. \qquad \textbf{(H1)}$$

We recall the general common principle of these methods, which is also the first main ingredient of the proof of Theorem 1.1. It is based on the idea of creating, from the input equation (8), two additional polynomial equations, such that the resulting polynomial system admits a solution with $F(t, a)$ for its z-coordinate. Then, a polynomial $R \in \mathbb{K}[t, z] \setminus \{0\}$ annihilating $F(t, a)$ is computed by algebraic elimination algorithms. Let us give a few more details.

First, from part 1 of assumption (**H1**) and from [20, Thm. 2], there exists a fractional power series $U(t)$ in $\overline{\mathbb{K}}[[t^{1/\star}]]$ satisfying

$$\partial_x P(F(t, U(t)), F(t, a), t, U(t)) = 0. \tag{9}$$

Now, differentiating equation (8) with respect to u yields

$$\partial_u F(t, u) \cdot \partial_x P(F(t, u), F(t, a), t, u) + \partial_u P(F(t, u), F(t, a), t, u) = 0.$$

Plugging $u = U(t)$ into this equation and using (9) implies that the following constraints hold in $\overline{\mathbb{K}}[[t^{1/\star}]]$

$$\begin{cases} P(F(t, U(t)), F(t, a), t, U(t)) = 0, \\ \partial_x P(F(t, U(t)), F(t, a), t, U(t)) = 0, \\ \partial_u P(F(t, U(t)), F(t, a), t, U(t)) = 0, \end{cases} \quad U(t) \neq a. \tag{10}$$

(The first equation is a trivial consequence of (8), while $U(t) \neq a$ is a consequence of part 1 of assumption (**H1**).) In other terms,

$$P = \partial_x P = \partial_u P = 0, \quad u \neq a, \tag{$\mathcal{S}$}$$

[3] As usual, the notation $\tilde{O}(\cdot)$ is used to hide polylogarithmic factors in the argument.

admits $(x,z,u) = (F(t,U(t)), F(t,a), U(t)) \in \overline{\mathbb{K}}[[t^{1/\star}]] \times \mathbb{K}[[t]] \times \overline{\mathbb{K}}[[t^{1/\star}]]$ as solution. Let $\mathcal{I} \subset \mathbb{K}(t)[x,z,u]$ be the saturation with respect to $u-a$ of the ideal generated by $P, \partial_x P$ and $\partial_u P$, i.e.

$$\mathcal{I} = \left\{ f \in \mathbb{K}(t)[x,z,u] \mid \exists N \in \mathbb{N}\ f(u-a)^N \in \langle P, \partial_x P, \partial_u P \rangle \right\}.$$

The rest of the argument works under the following assumption:

Hypothesis 2: the ideal $\mathcal{J} := \mathcal{I} \cap \mathbb{K}[t,z]$ is nonzero. **(H2)**

Now, if R is a nonzero element of $\mathcal{J}$, then it can be written as $(u-a)^N \cdot R = AP + B\partial_x P + C\partial_u P$, for some A, B, C in $\mathbb{K}[x,z,t,u]$ and some $N \in \mathbb{N}$. As $U(t) \neq a$, by specializing this equality at $(x,z,u) = (F(t,U(t)), F(t,a), U(t)) \in \overline{\mathbb{K}}[[t^{1/\star}]] \times \mathbb{K}[[t]] \times \overline{\mathbb{K}}[[t^{1/\star}]]$, we conclude from (10) that $R(F(t,a),t) = 0$. This proves the following:

Proposition 2.1. *Under* **(H1)** *and* **(H2)**, *any* $R \in \mathcal{J} \setminus \{0\}$ *satisfies* $R(F(t,a),t) = 0$.

The remaining parts of this section provide and analyze different methods that allow to compute such a polynomial $R \in \mathcal{J} \setminus \{0\}$, based on different ways of performing the needed polynomial elimination.

2.1.1 Using iterated discriminants. We start by presenting a method based on iterated discriminants, taken from [20, §6].

Let us denote by $\mathrm{disc}_x P \in \mathbb{K}[z,t,u]$ the discriminant of P with respect to x, and denote as before by $U(t)$ a fractional power series satisfying equation (9). It is then shown in [20, Thm. 14] that $U(t)$ is a multiple root of $(\mathrm{disc}_x P)(F(t,a),t,u) \in \mathbb{K}[[t]][u]$. As a consequence, $U(t)$ is also a root of $\partial_u(\mathrm{disc}_x P)(F(t,a),t,u)$ and it follows that $F(t,a)$ is a root of the iterated discriminant $\mathrm{disc}_u(\mathrm{disc}_x P) \in \mathbb{K}[t][z]$. To summarize, Bousquet-Mélou and Jehanne proved in [20, §6] the following:

Proposition 2.2. *Under* **(H1)**, $\mathrm{disc}_u(\mathrm{disc}_x P)(F(t,a),t) = 0$.

Unfortunately, it may happen that $\mathrm{disc}_x P$ has multiple roots w.r.t. u, in which case the equality in Proposition 2.2 is trivially satisfied, hence useless. This is illustrated by the following example. (See Example 5.2.) However, on this example, taking first the squarefree part of $\mathrm{disc}_x P$, and only then taking the discriminant w.r.t. u delivers a polynomial that annihilates $F(t,0) = 1 + 31t - 775t^2 - \cdots$. It is natural to wonder whether this is a general fact. We will prove that this is indeed so, under the following genericity assumption:

Hypothesis R: $V(P) \subset \overline{\mathbb{K}}^4$ is smooth outside $\{u = a\}$ **(R)**

We will first prove that this assumption is stronger than **(H2)**.

Lemma 2.3. *Assumption* **(R)** *implies Assumption* **(H2)**.

Proof. The Zariski closure of the algebraic set defined by the system $(\mathcal{S})$ is the algebraic set defined by $\mathcal{I}$. Geometrically, since P is squarefree (by **(GH)**), this algebraic set is the union of:

(1) the Zariski closure of the set of regular critical points of the restriction of the projection on the (z,t)-space to $V(P)$
(2) and the singular points which do satisfy $u \neq a$.

By Sard's theorem [48, Prop. B.2], the projection of (1) in the (z,t)-space is enclosed in a Zariski-closed subset of codimension ≥ 1. By **(R)**, there is no singular point which satisfies $u \neq a$. We deduce that the algebraic set associated to $\mathcal{J}$ is contained in a proper Zariski closed subset of $\overline{\mathbb{K}}^2$. This implies that $\mathcal{J}$ contains a nonzero polynomial, as claimed. □

We are now ready to state and analyze a first algorithm, which is a variant of the iterated discriminant method proposed in [20, §6].

Proposition 2.4. *Let* $P \in \mathbb{K}[x,z,t,u]$ *be as in* (8), *and satisfying* **(H1)** *and* **(R)**. *Set* $D_0 := \mathrm{disc}_x P$, $D_1 := \mathsf{SqFreePart}(D_0)$ *and* $D_2 := \mathrm{disc}_u D_1$. *Then,* $R := \mathsf{SqFreePart}(D_2)$ *is a nonzero polynomial in* $\mathbb{K}[t,z]$ *such that* $R(t,F(t,a)) = 0$.

Proof. We denote by V' the Zariski closure of the solution set in $\overline{\mathbb{K}}^4$ of $\{P = \partial_x P = 0,\ u \neq a\}$, and by V'' the Zariski closure of the solution set of the system $(\mathcal{S})$. We consider W (resp. W'') the Zariski closure of the projection $\pi_{z,t,u}$ (resp. $\pi_{z,t}$) on the (z,t,u)-space (resp. (z,t)-space) of V' (resp. V''). Let Z be an irreducible component of W''. By the elimination theorem, Z is the algebraic set attached to some minimal prime associated to $\mathcal{J}$. By definition of $\mathcal{J}$ and $\mathcal{I}$, there exists a Zariski-dense subset Z' of Z such that any $(\zeta,\vartheta) \in Z'$ is the projection of some point $\alpha = (\xi,\mu,\zeta,\vartheta) \in V(\mathcal{I})$ which satisfies $u \neq a$. Since we assume **(R)**, we deduce that α is a regular point in $V(P)$. Let T be the tangent space to $V(P)$ at α. Observe that the projection of T on the (z,t)-space is not fully dimensional (it is orthogonal to the line supported by the gradient of P evaluated at α, since α is a regular point).

Following [43], we prove further that D_1 and $\partial_u D_1$ vanish at $\beta = (\mu,\zeta,\vartheta)$. This implies that D_2 and its squarefree part R vanish at (ζ,ϑ). Since (by construction) D_1 is squarefree, D_2 and R are not zero. Hence, all in all, R vanishes on a Zariski-dense subset of W'' and we deduce that R lies in the radical of $\mathcal{J}$. Recall that we assume **(H1)** and **(R)**. Lemma 2.3 implies that **(H2)** then holds and we can then conclude using Proposition 2.1 that $R(F(t,a),t) = 0$.

First, we prove that β belongs to W. This is clear since $\alpha \in V(\mathcal{I}) \setminus V(u-a) \subset V' \setminus V(u-a)$, β is the projection of α and W is the Zariski-closure of the projection of V'. Next, we prove that any point in W cancels D_1. This is clear since $\mathrm{disc}_x P$ lies in the ideal generated by $P, \partial_x P$. We denote by Δ the vanishing set of D_1. We prove now that $\partial_u D_1$ vanishes at β.

If β is a singular point of Δ, this is immediate. Assume now that β is a regular point of Δ. Then the tangent space T' to Δ at β is the projection of the tangent space T on the (u,z,t)-space [43, Prop. 9]. We deduce that the projection of T' on the (z,t)-space is not fully dimensional since this is the case for T and projections are nested. Since D_1 is squarefree by definition, by the Jacobian criterion [32, Theorem 16.19], we deduce that T' is orthogonal to the line supported by the gradient of D_1 evaluated at β. Consequently, $\partial_u D_1$ vanishes at β, as requested. □

Proposition 2.4 yields an algorithm and proves its correctness. In what follows, we will refer to it as Algorithm 2.4. A variant of this algorithm further factors the polynomial R and identifies the minimal polynomial of $F(t,a)$ among its factors. (See Example 5.3.)

Example 5.4 shows that without assumption **(H1)**, Algorithm 2.4 may return a wrong answer. Let us now analyze its complexity.

Proposition 2.5. *Assume* $P \in \mathbb{K}[x,z,t,u]$ *as in* (8) *satisfies* **(H1)** *and* **(R)**, *and let* $\delta \geq 2$ *be an upper bound on its total degree. Then, the output* $R \in \mathbb{K}[t,z]$ *of Algorithm 2.4 has total degree at most* $2\delta^4$ *and degree in each variable at most* δ^4. *Moreover, R can be computed with a probabilistic algorithm in* $\tilde{O}(\delta^{10})$ *arithmetic operations in* $\mathbb{K}$.

Before proving Proposition 2.5, we need the following lemma, whose proof is omitted (see [57] for similar statements.)

Lemma 2.6. *Let $G \in \mathbb{K}[x, t_1, \ldots, t_\lambda]$ be a polynomial of degree bounded by N. Then the squarefree part of $\mathrm{disc}_x G$ can be computed in $\tilde{O}(\lambda N^{2\lambda+1})$ operations in $\mathbb{K}$.*

Proof of Prop. 2.5. First, applying Lemma 2.6 to D_0 and to D_1 in Prop. 2.4, with P of degree δ and $\lambda = 3$, gives a complexity in $\tilde{O}(\delta^7)$ operations in $\mathbb{K}$. Further, both partial degrees of D_1 are bounded by δ^2. A second application to D_2 and R in Proposition 2.4, with D_2 of degree at most δ^2 and $\lambda = 2$, gives a complexity in $\tilde{O}(\delta^{10})$ operations in $\mathbb{K}$. Moreover, using the partial degrees of $\mathrm{disc}_x P$, one finds that R has partial degrees bounded by δ^4. □

2.1.2 Using direct elimination. Yet another strategy is proposed in [20, Section 3] to compute a non zero element of $\mathcal{J} := \mathcal{I} \cap \mathbb{K}[t, z]$. We investigate in this section the complexity of computing such an element in $\mathcal{J}$ using various algorithms for algebraic elimination.

We start with a new assumption.

Hypothesis 3: the ideal $\mathcal{I}$ in $\mathbb{K}(t)[x, z, u]$ is radical and has dimension zero over $\mathbb{K}(t)$. **(H3)**

The next lemma clarifies the link between (**H3**) and (**H2**).

Lemma 2.7. *Assumption* (**H3**) *implies assumption* (**H2**).

Proof. We need to prove that there exists a nonzero element in $\mathcal{I} \cap \mathbb{K}[t, z]$. Since $\mathcal{I} \subset \mathbb{K}(t)[x, z, u]$ is zero-dimensional by (**H3**), the quotient ring $\mathbb{K}(t)[x, z, u]/\mathcal{I}$ is a $\mathbb{K}(t)$-vector space of finite dimension. By Stickelberger's theorem (see e.g. [31]), the characteristic polynomial $\xi(z)$ of the multiplication map $f \mapsto z \cdot f$ lies in $\mathcal{I}$ and, by design, is not zero and in $\mathbb{K}(t)[z]$. Hence, multiplying $\chi(z)$ by the least common multiple of its coefficients yields a nonzero element in $\mathcal{J} = \mathcal{I} \cap \mathbb{K}[t, z]$, as requested. □

Proposition 2.8. *Let P be as in* (8) *and let δ be its total degree. Assume that* (**H1**) *and* (**H3**) *hold. Then, there exists a nonzero polynomial R in $\mathbb{K}[z, t]$ such that $R(F(t, a), t) = 0$ with $\deg_z(R) \le \delta^3$ and $\deg_t(R) \le \delta^3$. Such an R can be taken irreducible.*

Proof. By Lemma 2.7, we deduce that assumption (**H2**) holds, since (**H3**) holds by assumption. Since we also assume (**H1**), we can then apply Proposition 2.1 and deduce that any nonzero polynomial in $\mathcal{J} = \mathcal{I} \cap \mathbb{K}[t, z]$ satisfies $R(F(t, a), t) = 0$.
We identify one such polynomial and prove the claimed degree bounds for it. The proof of Lemma 2.7 suggests to consider the squarefree part $\chi(z) \in \mathbb{K}(t)[z]$ of the characteristic polynomial of the multiplication map $f \mapsto z \cdot f$ in the quotient ring $\mathbb{K}(t)[x, u, z]/\mathcal{I}$ (this makes sense since, by assumption (**H3**), $\mathcal{I}$ is zero-dimensional). By Bézout's theorem, the dimension of $\mathbb{K}(t)[x, u, z]/\mathcal{I}$ as a $\mathbb{K}(t)$-vector space is bounded by δ^3. Multiplying χ by the least common multiple of the denominators of its coefficients yields $R \in \mathbb{K}[t, z]$ which also lies in $\mathcal{J}$, by Stickelberger's theorem, since by (**H3**) is radical and consequently $\mathcal{J}$ is. We aim at bounding the degrees of R. Note that it is squarefree, and that clearly $\deg_z(R) \le \delta^3$. It remains to prove that $\deg_t(R) \le \delta^3$ as well. The degree of R in t is the same as the degree of the polynomial R_ζ obtained by specializing z to a random value, say ζ, in $\mathbb{K}$. Since ζ is chosen randomly, we may assume that R_ζ is squarefree. By a slight abuse of notation, we still denote by $\mathcal{I}$ the intersection of $\mathcal{I}$ with $\mathbb{K}[x, z, t, u]$. Since R_ζ lies in $\mathcal{I}_\zeta = \mathcal{I} + \langle z - \zeta \rangle$ in $\mathbb{K}[x, u, z, t]$, we deduce by Bézout's theorem that the algebraic set defined by this ideal has degree at most δ^3. Since ζ is chosen randomly, we may assume by applying the Principal Ideal Theorem that $\mathcal{I}_\zeta$ has dimension at most 0. We deduce that the squarefree part of the characteristic polynomial χ_ζ of the multiplication map $f \mapsto t \cdot f$ in the ring $\mathbb{K}[x, u, z, t]/\mathcal{I}_\zeta$ is squarefree (by definition) and has degree at most δ^3. Note also that it divides R_ζ. Finally, remark that all roots of R_ζ are the projections on the t variable of the roots of $\mathcal{I}_\zeta$. Hence, we deduce that up to a multiplication by a constant in $\mathbb{K} \setminus \{0\}$, the polynomials R_ζ and χ_ζ coincide. All in all, we conclude that $\deg_t(R) \le \delta^3$. □

Proposition 2.9. *Let P be as in* (8) *and let δ be its total degree. Assume that* (**H1**) *and* (**H3**) *hold. There exists an algorithm which takes as input $a \in \mathbb{K}$ and a straight-line program of length L evaluating P, and computes a non-zero element R in $\mathcal{J}$ such that $R(F(t, a), t) = 0$ using $\tilde{O}(L\delta^6 + \delta^{7.89}) \subseteq \tilde{O}(\delta^{10})$ arithmetic operations in $\mathbb{K}$.*

Proof. We aim at computing the polynomial R defined in (the proof of) Proposition 2.8 (which applies since we assume (**H1**) and (**H3**)), that is, the squarefree part $\chi(z) \in \mathbb{K}(t)[z]$ of the characteristic polynomial of the multiplication map $f \mapsto z \cdot f$ in the quotient ring $\mathbb{K}(t)[x, u, z]/\mathcal{I}$. We proceed by first using the algorithm in [51] to compute the squarefree part of the characteristic polynomial of the multiplication map $f \mapsto (\lambda_1 x + \lambda_2 z + \lambda_3 u) \cdot f$ where $\lambda_i \in \mathbb{K}$ for $1 \le i \le 3$ are chosen randomly, as well as some extra data encoding the solutions of $\mathcal{I}$. From this, we use evaluation-interpolation techniques and the degree bounds of Proposition 2.8 to deduce $\chi(z)$, which we then multiply by the least common multiple of its coefficients.

Since (**H3**) holds, one can apply, as a first step, the algorithm on which [51, Theorem 2] relies. This takes as input a straight-line program evaluating $P, \partial_x P, \partial_u P$ and $u - a$. By the Baur-Strassen theorem [5], such a straight-line program of length $O(L)$ can be obtained from the one which evaluates P. The next parameter to control the complexity of this algorithm is the degree of the ideal $\mathcal{I}$ (which is bounded by δ^3) and the degree of the algebraic set defined as the Zariski closure of the solution set of the system ($\mathcal{S}$). Using again Bézout's theorem, this is dominated by δ^3. The algorithm computes a *rational parametrization* of the solutions of $\mathcal{I}$ with coefficients in $\mathbb{K}(t)$: $x = \widetilde{V}_3(t, \lambda)/\widetilde{W}'(t, \lambda)$, $u = \widetilde{V}_2(t, \lambda)/\widetilde{W}'(t, \lambda)$, $z = \widetilde{V}_1(t, \lambda)/\widetilde{W}'(t, \lambda)$, over the extension defined by $\widetilde{W}(t, \lambda) = 0$ where λ is a new variable, $\widetilde{W}$ monic and squarefree, $\widetilde{W}' = \partial\widetilde{W}/\partial\lambda$, $\deg(\widetilde{V}_i) < \deg(\widetilde{W})$ and $\sum_{i=1}^3 \lambda_i \widetilde{V}_i = \lambda\widetilde{W}' \mod \widetilde{W}$ (for some $\lambda_i \in \mathbb{K}$). Theorem 2 from [51] shows that such a computation can be done using $O((L + 1)\delta^6)$ arithmetic operations.

Actually, the above definition of rational parametrization implies that for any $\vartheta \in \mathbb{K}$ such that $\widetilde{W}(\lambda, \vartheta)$ remains squarefree, specializing t to ϑ in the rational parametrization yields a univariate one which encodes the solutions of $\mathcal{I}_{|t=\vartheta}$. Observe that one can then compute the inverse E of $\widetilde{W}'(\lambda, \vartheta)$ modulo $\widetilde{W}$ and deduce a lexicographic Gröbner basis $x - Q_3(\lambda), u - Q_2(\lambda), z - Q_1(\lambda), \widetilde{W}(\lambda, \vartheta)$ of the ideal $\mathcal{I}_{t=\vartheta} + \langle \lambda - \lambda_3 x - \lambda_2 u - \lambda_1 z \rangle$ (here $Q_i = E\widetilde{V}_i(\lambda, \vartheta) \mod \widetilde{W}(\lambda, \vartheta)$). Hence the resultant of $z - Q_1(\lambda)$ and $\widetilde{W}(\lambda, \vartheta)$ is the characteristic polynomial of the map $f \mapsto z \cdot f$ in the quotient ring defined by the above ideal. Following [41, §5], this can be done

using $\tilde{O}(\delta^{4.89})$ operations in $\mathbb{K}$. Using the above degree bounds of Proposition 2.8, we need to perform this computation $O(\delta^3)$ times. All in all, we deduce the arithmetic cost is then $\tilde{O}(L\delta^6 + \delta^{7.89})$. Noticing that L can be bounded by δ^4 ends the proof. □

2.2 Using Guess-and-Prove methods

2.2.1 Zeilberger's method. To find an annihilating polynomial for $F(t,a)$, where $F(t,u)$ is the unique solution of equation (6)–(8), Zeilberger proposed in [58] a guess-and-prove strategy, that he further refined with Gessel in [37]. The main steps are the following.

Zeilberger's method

(0) Compute the expansion of $F(t,u) \bmod t^\sigma$ for some integer σ;
(1) Guess $S \in \mathbb{K}[x,t,u]\backslash\{0\}$ such that $S(F(t,u),t,u) = 0 \bmod t^\sigma$;
(2) Prove that there exists a unique power series G in $\mathbb{K}[u][[t]]$ such that $S(G(t,u),t,u) = 0$;
(3) Prove that G satisfies $P(G(t,u),G(t,a),t,u) = 0$;
(4) Return $R(z,t) := S(z,t,a)$.

This is a typical guess-and-prove process, which proceeds in three basic parts: data generation (step 0), guessing part (step 1) and proving part (steps 2–4). To be historically fair, it should be mentioned that this general strategy was used already in the early 60's by Tutte and Brown on many examples coming from the enumeration of various types of maps. For instance, in his 1962 study of planar triangulations, Tutte [54, §4] solves his equation (3.7)–(3.8) (see also eq. (4) in [20]) using this approach. Shortly after, in his 1963 paper on non-separable planar maps, Brown [22, §4] solves his equation (3.6) in a similar fashion, and the same happens in the joint paper by Brown and Tutte [24] with their eq. (3.8). A few years later, Tutte [55] solves equation (2) by guess-and-prove too.

Assuming that steps (1)–(3) have succeeded well, the correctness of this method relies on the observation that both $F(t,u)$ and $G(t,u)$ are solutions in $\mathbb{K}[u][[t]]$ of eq. (8). By uniqueness, $F(t,u)$ coincides with $G(t,u)$, which is algebraic by design, and root of S. Hence $S(F(t,u),t,u) = 0$; in particular $R(F(t,a),t) = S(F(t,a),t,a) = 0$.

The strength of guess-and-prove is that it is a very general and robust method, which works even for more general equations, for which algebraicity is not known beforehand, e.g. [17]; in such cases, algebraicity is discovered (and proved) along the way.

In our setting, algebraicity is granted by Theorem 1.1. In order to get realistic estimates on the complexity of the method, we will (implicitly) make in the next paragraphs the assumptions that allow to get a priori bounds on the bidegree of the output $R(z,t)$, e.g. Prop. 2.8, but these assumptions are not necessary for the guess-and-prove approach to work.

Step (0) was taken for granted in [58] and [37]. Although it is a simple step from the mathematical viewpoint, it can be very time consuming: it can actually be the one with the highest computational complexity. It takes as input σ, and it outputs the truncation modulo t^σ of the unique solution F in $\mathbb{K}[u][[t]]$ of equation (8). This solution can be computed in several ways, starting from the equivalent fixed-point-type equation (6). One way is to iterate

$$F_{k+1}(t,u) := f(u) + t\,Q(F_k(t,u), \Delta_a F_k(t,u), t, u) \mod t^{k+1},$$

for $k \geq 0$, starting from $F_0 := f(u)$. If $F(t,u) = \sum_{n\geq 0} f_n(u)t^n$, one can show by induction that $\deg(f_n) = O(\delta^2 n)$, hence the total size of $F(t,u) \bmod t^\sigma$ is $O(\delta^2\sigma^2)$ (and this bound is generically tight).

The guessing of Step (1) can be performed in different ways. Zeilberger [58] uses an Ansatz and linear algebra; a better idea is to use evaluation-interpolation with respect to u, and for each $u_0 \in \mathbb{K}$, perform Hermite-Padé (algebraic) approximation on the univariate series $F(t,u_0)$. In both cases, a precision σ of order $\deg_x S \cdot \deg_t S$ is required, which is $O(\delta^8)$ (see below). An even better idea, proposed in [37], is to first guess the polynomial $R(z,t)$ annihilating $F(t,a)$; for this, it is enough to use a precision linear in $\deg_z R \cdot \deg_t R$, which by Prop. 2.8 is of order δ^6 only. Then, S is taken to be the resultant w.r.t. z of $P(x,z,t,u)$ and $R(z,t)$, which is of total degree $O(\delta^4)$. Using the fastest known algorithms for Hermite-Padé approximation, either based on polynomial matrices (e.g. [39]), or on structured scalar matrices (e.g. [16]), guessing the polynomial R takes $\tilde{O}(\sigma \cdot (\deg_z R)^{\theta-1}) = \tilde{O}(\delta^{3\theta+3})$ operations in $\mathbb{K}$. Using evaluation-interpolation and fast univariate resultants, S can be computed in $\tilde{O}(\delta^{15})$ operations in $\mathbb{K}$. Note in retrospect that the total arithmetic size of $F(t,u) \bmod t^\sigma$ computed in Step (0) with this variant is of order $\delta^2\sigma^2 = \delta^{14}$.

Remark, for the sake of comparison, that constructing S directly by evaluation-interpolation w.r.t. u and by $O(\delta^4)$ Hermite-Padé approximants of univariate power series $F(t,\star)$ would require $\sigma = O(\delta^8)$ (and therefore an object of total arithmetic size $O(\delta^{18})$ in Step (0)) and would take $\tilde{O}(\delta^{4\theta+8})$ operations in $\mathbb{K}$, which is at least $\tilde{O}(\delta^{16})$ even if θ would be equal to 2.

Step (2) was taken for granted in [58] and [37]. However, it is both mathematically and algorithmically non-trivial. It is generally easy to prove the existence of a G in $\mathbb{K}(u)[[t]]$, but it could be much less easy to prove that the coefficients of G are *polynomials* in u. Note that it is enough to relax the requirement that the coefficients of G are in $\mathbb{K}[u]$, by just asking that they are rational functions in $\mathbb{K}(u)$ with no pole at $u = a$. However, this may also be a non-trivial task[4], related to the process of *desingularisation*, either algebraic [10, 56] or differential [1, 27]. Because of this, the complexity is difficult to estimate, and is possibly not polynomial in δ (in the worst case). In the particular case when the curve defined by $S(x,t,u_0)$ has genus 0 for (almost) all $u_0 \in \mathbb{K}$, it is possible to use rational parametrizations in order to prove the existence of a root G in $\mathbb{K}[u][[t]]$. This idea is frequently used in the combinatorics community, e.g. by Tutte and Brown [22, 24, 54, 55]. However, although computing rational parametrizations is known to be decidable and implemented in many computer algebra systems [34, 35, 49, 52], its complexity may have an exponential dependence with respect to δ [45, 53].

In [58], Step (3) is also quite laborious, and is treated using a nonlinear ODE satisfied by $F(t,u)$. The approach seems difficult to analyze fully from the complexity viewpoint.

In [37], Gessel and Zeilberger proposed a different approach for Step (3). Since $G(t,u)$ is algebraic over $\mathbb{K}(t,u)$ (by design), $G(t,a)$ is algebraic $\mathbb{K}(t)$, hence $M(t,u) := P(G(t,u),G(t,a),t,u)$ is also algebraic over $\mathbb{K}(t,u)$. Being algebraic, $M(t,u) = \sum_{n\geq 0} M_n(u)t^n$ is D-finite (w.r.t. t), hence the sequence of polynomials $(M_n(u))_{n\geq 0}$ is P-recursive. To prove that M is identically zero, it is enough to check that a finite amount of polynomials $M_n(u)$ are identically zero, for $n = 0,\ldots,N$, for some integer N. However, N is potentially exponentially large in δ, as it is related to the largest integer root of an indicial polynomial of the corresponding recurrence.

[4] An example of application can be found in the proof of Prop. 17 of [12].

An alternative way is to check Step (3) using algebraic elimination tools: one computes the intersection of $\mathbb{K}[T,t,u]$ and the ideal of $\mathbb{K}[T,x,z,t,u]$ generated by $S(x,t,u)$, $S(z,t,a)$ and $T-P(x,z,t,u)$ and extract from it a polynomial annihilating $P(G(t,u),G(t,a),t,u)$; this polynomial is of the form $T^m \cdot A(T,t,u)$ with $m \geq 1$ and it is sufficient to check that A does not cancel the first terms of $P(G(t,u),G(t,a),t,u) = O(t)$. (See Example 5.5.)

The conclusion is that Zeilberger's method, and its various variants and improvements, is a complex process, which for generic polynomials P of degree δ requires at least $\tilde{O}(\delta^{15})$ operations in $\mathbb{K}$.

2.2.2 A new hybrid method. We propose here a new approach of the type "guess-and-prove" which blends ingredients inspired from both the elimination method (§2.1) and Zeilberger's method (§2.2.1).

Hybrid method

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

Assuming that some R is returned at step (3), the correctness of this method relies on the following reasoning. (Note the similarity with the so-called "multiplicity lemma" in number theory [9, 18, 30]; a similar approach was already used in computer algebra, in several contexts: polynomial factorization [42]; rational solutions of algebraic ODEs [3]; differential equations for algebraic functions [14]; first integrals and Darboux polynomials [13].) We know in advance (by Prop. 2.8) that there exists an irreducible polynomial $M \in \mathbb{K}[z,t] \setminus \{0\}$ of degree at most $2\delta^3$ such that $M(F(t,a),t) = 0$. Then, the resultant $A(t)$ with respect to z of $R(z,t)$ and $M(z,t)$ writes $A = UR+VM$ for U, V in $\mathbb{K}[z,t]$. Hence, replacing $z = F(t,a)$ in this equality yields that $A(t) = U(F(t,a),t)\cdot R(F(t,a),t)$ is either zero, or it has a valuation at least that of $R(F(t,a),t)$, which is larger than $\delta^3\cdot\deg R$ by the successful check of Step (2). On the other hand, $A(t)$ is a polynomial of degree at most $\deg M\cdot\deg R \leq \delta^3\cdot\deg R$. The conclusion is that $A(t)$ is identically zero, and since M is irreducible, this implies that M divides R in $\mathbb{K}[z,t]$, hence $R(F(t,a),t) = 0$.

The method is guaranteed to succeed, because at some point the precision σ will be large enough so that the guessing part (Step (1)) captures (a multiple of) the minimal polynomial of $F(t,a)$. The terminating σ will be not more than twice the degree of this minimal polynomial, which is at most the degree of the polynomial R predicted by Prop. 2.8, implying $\sigma \in O(\deg_z R\cdot\deg_t R) \subseteq O(\delta^6)$.

We now introduce a notion and a new regularity assumption in more generality, as they will be used repeatedly, in the next proposition then in §3.1. Let $\mathbf{K}$ be a field. For $H = (H_1,\ldots,H_n) \subset \mathbf{K}[s_1,\ldots,s_n]$, the Jacobian matrix of the tuple H is the matrix $\mathrm{Jac}_{s_1,\ldots,s_n}(H_1,\ldots,H_n) = \left[\frac{\partial H_i}{\partial s_j}\right]_{i,j=1}^n$. Write $\mathcal{D}_H$ for the determinant of this matrix. We say that H satisfies (**J**) when it satisfies:

Hypothesis J: There exists $\boldsymbol{s} \in V(H)$ such that $\mathcal{D}_H(\boldsymbol{s}) \neq 0$. (**J**)

Lemma 2.10. *Let H be as above and assume that (**J**) holds. Then the saturation ideal $\langle H\rangle : \mathcal{D}_H^\infty$ is zero-dimensional and radical.*

Proof. Since (**J**) holds, the Hilbert Nullstellensatz implies that the saturation of the ideal generated by H with $\mathcal{D}_H$ is not reduced to $\mathbf{K}[s_1,\ldots,s_n]$. Applying [32, Theorem 16.19], we deduce that it is radical of co-dimension n (and hence of dimension 0). □

In particular, for $\mathbf{K} = \mathbb{K}(t)$ and $(s_1,s_2,s_3) := (x,z,u)$, (**J**) implies (**H3**).

Proposition 2.11. *Let P be as in (8) and let δ be its total degree. Assume that (**H1**) holds and that $(P,\partial_x P,\partial_u P)$ satisfies (**J**) (w.r.t. x,z,u). Assume further that there exists a straight-line program of length L evaluating P. Then, the new hybrid method terminates on input P using $\tilde{O}(L\cdot\delta^6 + \delta^{3\theta+3}) \subseteq \tilde{O}(\delta^{10.12})$ arithmetic operations in $\mathbb{K}$.*

Proof. Consider the last execution of (0)–(3), which happens with $\sigma \in O(\delta^6)$ and $\deg(R) \in O(\delta^3)$. As in §2.2.1, the guessing at Step (1) takes $\tilde{O}(\sigma\cdot(\deg_z R)^{\theta-1}) \subseteq \tilde{O}(\delta^{3\theta+3})$ operations in $\mathbb{K}$. The order σ of $F(t,a)$ and the truncation order $\delta^3\cdot\deg R+1$ at Step (2) are both $O(\delta^6)$, so the truncated evaluation of R requires $\tilde{O}(\deg(R)\cdot(\delta^3\cdot\deg(R))) \subseteq \tilde{O}(\delta^9) \subseteq \tilde{O}(\delta^{3\theta+3})$ operations in $\mathbb{K}$. The truncation of $F(t,a)$ at Step (0) is computed by the classical Newton–Hensel method [e.g., 40, §4.1] applied to the polynomial system (10), in the form of the Newton iteration

$$\mathbf{F} \mapsto \mathcal{N}(\mathbf{F}) := \mathbf{F} - J(\mathbf{F})^{-1}\cdot V^{\mathrm{T}}(\mathbf{F}), \tag{11}$$

where $V = [P,\partial_x P,\partial_u P]$, $J = \mathrm{Jac}_{x,z,u}(P,\partial_x P,\partial_u P)$, and $\mathbf{F} \in \mathbb{K}[[t]]^3$ denotes an approximation of a solution $(F(t,U(t)),F(t,a),U(t))$. Let (**J**) provide (α,β,γ) at which J is invertible. Because (11) doubles the number of correct terms in an approximate series solution to (10), the iteration starting from the initial point for $\mathbf{F} = (\alpha,\beta,\gamma)$ is well defined. By the Baur–Strassen theorem [5], a straight-line program of length $O(L)$ evaluating V can be obtained from the one evaluating P, and by iterating the process, another straight-line program of length $O(L)$ is found to evaluate the Jacobian matrix; by the fixed dimension 3, there is also one for its inverse. Now, evaluating V and J^{-1} at series $\mathbf{F}$ of some order N requires $\tilde{O}(L\cdot N)$ arithmetic operations in $\mathbb{K}$, which is also the cost of one Newton iteration. After taking a geometric sum, it follows that the overall cost of Step (0) is $\tilde{O}(L\cdot\sigma) \subseteq \tilde{O}(L\cdot\delta^6)$ arithmetic operations in $\mathbb{K}$. Therefore, Steps (0)–(3) can be executed using $\tilde{O}(L\cdot\delta^6 + \delta^{3\theta+3})$ arithmetic operations in $\mathbb{K}$. The proposition finally follows after summation over $\log\sigma \in O(\log\delta)$ executions of Steps (0)–(3). □

An application of the hybrid method is given as Example 5.6.

3 SOLVING GENERAL DDEs

3.1 Deformation method

We now recall the second main ingredient, introduced by Bousquet-Mélou and Jehanne in [20, §4], and used by them to prove Theorem 1.1 in full generality (with no assumptions on f, Q, P).

The approach relies on a symbolic homotopy method, via the introduction of an extra variable ϵ in order to "deform" (6) into a functional equation that always satisfies assumptions (**H1**) and (**J**).

Starting from (6), one defines the deformed equation

$$G(h,u,\epsilon) = f(u)+\epsilon\, h\,\Delta_a G(h,u,\epsilon)+h^2\, Q(G(h,u,\epsilon),\Delta_a G(h,u,\epsilon),h^2,u), \tag{12}$$

which can also be rewritten as $P_\epsilon(G(h,u,\epsilon),G(h,a,\epsilon),t,u,\epsilon) = 0$ for some $P_\epsilon \in \mathbb{K}[x,z,h,u,\epsilon]$. This new equation enjoys the following properties (proved in [20, p. 635–638]):

- it satisfies assumption (**H1**), with P replaced by P_ϵ;
- it admits a unique solution $G(h,u,\epsilon)$ in $\mathbb{K}[u,\epsilon][[h]]$;
- $G(h,u,0) = F(h^2,u)$, where $F(t,u)$ is the solution of (6)–(8).

In particular, for $R_0 \in \mathbb{K}[z,h]\setminus\{0\}$ such that $R_0(G(h,a,0),h)=0$, we get for free the nonzero polynomial $R(z,t) := R_0(z,\sqrt{t})\cdot R_0(z,-\sqrt{t})$ in $\mathbb{K}[z,t]$ that annihilates $F(t,a)$.

Moreover, there exists a unique $U(h,\epsilon) \in \overline{\mathbb{K}}[\epsilon][[h]]$ such that:

- it satisfies (10) with P replaced by P_ϵ, and $F(t,u)$ by $G(h,u,\epsilon)$;
- the Jacobian matrix of $P_\epsilon, \partial_x P_\epsilon, \partial_u P_\epsilon$ evaluated at the "point" $(x,z,u) = (G(h,U(h,\epsilon),\epsilon), G(h,a,\epsilon), U(h,\epsilon))$ has full rank.

We consider the ideal $\mathcal{I}_\epsilon$ obtained by saturating $\langle P_\epsilon, \partial_x P_\epsilon, \partial_u P_\epsilon\rangle$ with the determinant $\mathcal{D}$ of the Jacobian matrix $\mathrm{Jac}_{x,z,u}(P_\epsilon, \partial_x P_\epsilon, \partial_u P_\epsilon)$.

Note that $V(\mathcal{I}_\epsilon)$ contains the point

$$(x,z,u) = (G(h,U(h,\epsilon),\epsilon),\ G(h,a,\epsilon),\ U(h,\epsilon)) \in \overline{\mathbb{K}}[\epsilon][[h]]^3.$$

By Corollary 2.10 applied to $(P_\epsilon, \partial_x P_\epsilon, \partial_u P_\epsilon)$, Assumption (**H3**) holds and then Assumption (**H2**) holds (Lemma 2.7). Recall that (**H1**) holds. Hence, applying Proposition 2.1 to these data, we deduce that every element of $\mathcal{J}_\epsilon = \mathcal{I}_\epsilon \cap \mathbb{K}[z,h,\epsilon]$, annihilates $G(h,a,\epsilon)$.

From such an element, setting ϵ to 0 yields the desired $R_0 \in \mathbb{K}[z,h]\setminus\{0\}$ annihilating $G(h,a,0)$. (See Example 5.7.)

3.2 A polynomial time algorithm

In this section, we prove a quantitative version of Theorem 1.1 for DDEs of order $k=1$. More precisely, we will show that for P as in (8), of degree δ, there exists a nonzero polynomial annihilating $F(t,a)$ with total arithmetic size polynomial in δ, and moreover, that this polynomial can be computed in polynomial time in δ.

To do this, we rely on the deformation method recalled in §3.1. We start by bounding the degrees of P_ϵ. The proof follows the same pattern as the one of Proposition 3.1 by investigating algebraic objects related to the ideals $\mathcal{I}_\epsilon$ and $\mathcal{J}_\epsilon$ defined in §3.1.

Proposition 3.1. *Assume $P_\epsilon \in \mathbb{K}[x,z,h,u,\epsilon]$ has total degree δ_ϵ. Then, there exists a nonzero element R_ϵ in $\mathcal{J}_\epsilon \cap \mathbb{K}[z,h,\epsilon]$ such that $\deg_z(R_\epsilon) \le \delta_\epsilon^3$, $\deg_h(R_\epsilon) \le \delta_\epsilon^3$ and $\deg_\epsilon(R_\epsilon) \le \delta_\epsilon^3$.*

Proof. Let $\chi(z) \in \mathbb{K}(h,\epsilon)[z]$ be the squarefree part of the characteristic polynomial of the multiplication map by z in the quotient ring $\mathbb{K}(h,\epsilon)[x,u,z]/\mathcal{I}_\epsilon$ (this makes sense since, by Corollary 2.10, $\mathcal{I}_\epsilon$ is zero-dimensional over $\mathbb{K}(h,\epsilon)$). Multiplying χ by the lcm of the denominators of its coefficients yields $R_\epsilon \in \mathbb{K}[z,h,\epsilon]$ which also lies in $\mathcal{J}_\epsilon$ by Stickelberger's theorem. Note that R_ϵ is squarefree, and that $\deg_z(R_\epsilon) \le \delta_\epsilon^3$. It remains to prove that $\deg_h(R_\epsilon) \le \delta_\epsilon^3$, $\deg_\epsilon(R_\epsilon) \le \delta_\epsilon^3$ as well. The degree of R_ϵ in h is the same as the degree of the polynomial $R(h,\zeta_1,\zeta_2)$ obtained by specializing (z,ϵ) to a random point, say $\zeta = (\zeta_1,\zeta_2)$, in $\mathbb{K}^2$. Since ζ is chosen randomly, we can assume that $R(h,\zeta_1,\zeta_2)$ is squarefree. We consider the ideal generated by the intersection of $\mathcal{I}_\epsilon$ with $\mathbb{K}[x,z,u,h,\epsilon]$. By an abuse of notation, we still denote this ideal by $\mathcal{I}_\epsilon$. Since $R(h,\zeta_1,\zeta_2)$ lies in $\mathcal{K}_\zeta = \mathcal{I}_\epsilon + \langle z-\zeta_1, \epsilon-\zeta_2\rangle$ in $\mathbb{K}[x,u,z,h,\epsilon]$, Bézout's theorem implies that the algebraic set this ideal defines has degree at most δ_ϵ^3. Since ζ is chosen randomly, we may assume by applying the Principal Ideal Theorem that $\mathcal{K}_\zeta$ has dimension at most 0. We deduce that the squarefree part of the characteristic polynomial χ_ζ of the multiplication map by h in the ring $\mathbb{K}[x,u,z,h,\epsilon]/\mathcal{K}_\zeta$ is squarefree (by definition) and has degree at most δ_ϵ^3. Note also that it divides $R(h,\zeta_1,\zeta_2)$. Finally, remark that all roots of $R(h,\zeta_1,\zeta_2)$ are the projections on the h variable of the roots of $\mathcal{K}_\zeta$. Hence, we deduce that up to a multiplication by a constant in $\mathbb{K}\setminus\{0\}$, the polynomials $R(h,\zeta_1,\zeta_2)$ and χ_ζ coincide. We conclude that $\deg_h(R_\epsilon) \le \delta_\epsilon^3$. Proving $\deg_\epsilon(R_\epsilon)$ is done in a symmetric way by considering the specialization of (z,h) to a random point as above. □

We now turn to the computation of the polynomial R_ϵ defined in (the proof of) Proposition 3.1, that is, the squarefree part $\chi(z) \in \mathbb{K}(h,\epsilon)[z]$ of the characteristic polynomial of the multiplication map $f \mapsto z\cdot f$ in the quotient ring $\mathbb{K}(t)[x,u,z]/\mathcal{I}_\epsilon$.

Let us denote by L_ϵ the length of a straight-line program for evaluating P_ϵ. Clearly, $L_\epsilon \le \delta^5$.

Proposition 3.2. *Under the assumption of Proposition 3.1, there exists an algorithm that takes on input a straight-line program of length L_ϵ for P_ϵ and that returns a non-zero element $R_\epsilon \in \mathcal{J}_\epsilon$, using $\tilde{O}(L_\epsilon\delta_\epsilon^9 + \delta_\epsilon^{10.89}) \subseteq \tilde{O}(\delta_\epsilon^{14})$ arithmetic operations in $\mathbb{K}$.*

Proof. We follow the lines of the proof of Proposition 2.9. Since $\mathcal{I}_\epsilon \subset \mathbb{K}(h,\epsilon)[x,z,u]$ is zero-dimensional and radical, one can apply [51, Theorem 2] and the algorithm on which it relies. By the Baur-Strassen theorem [6], a straight-line program of length $O(L_\epsilon)$ evaluating $P_\epsilon, \partial_x P_\epsilon, \partial_u P_\epsilon$ can be obtained from the one which evaluates P. With this straight-line program as input, the algorithm underlying [51, Theorem 2] computes a rational parametrization $x = \widetilde{V_3}(h,\epsilon,\lambda)/\widetilde{W'}(h,\epsilon,\lambda)$, $u = \widetilde{V_2}(h,\epsilon,\lambda)/\widetilde{W'}(h,\epsilon,\lambda)$ and $z = \widetilde{V_1}(h,\epsilon,\lambda)/\widetilde{W'}(h,\epsilon,\lambda)$ over the extension defined by $\widetilde{W}(h,\epsilon,\lambda)=0$ in $O\left((L_\epsilon+1)\delta_\epsilon^9\right)$ operations in $\mathbb{K}$. Without loss of generality, we may assume that $\widetilde{W}, \widetilde{W'}$ and $\widetilde{V_i}$ have coefficients in $\mathbb{K}[h,\epsilon]$. In this setting, λ encodes the values of a linear form $\lambda_1 x + \lambda_2 u + \lambda_3 z$ (with $\lambda_i \in \mathbb{K}$); hence, when specializing h,ϵ to some generic point $\vartheta = (\vartheta_1,\vartheta_2) \in \mathbb{K}^2$ in $\widetilde{W}$, the roots of $\widetilde{W}_{|h=\vartheta_1,\,\varepsilon=\vartheta_2}$ are the evaluations of the above linear form at the roots of $P_\epsilon = \partial_x P_\epsilon = \partial_u P_\epsilon = 0, h = \vartheta_1, \varepsilon = \vartheta_2, \mathcal{D} \neq 0$, where $\mathcal{D}$ is the determinant of the Jacobian matrix associated to $P_\epsilon, \partial_x P_\epsilon, \partial_u P_\epsilon$ w.r.t. x,z,u. By Proposition 3.1, the degree of these polynomials is bounded above by δ_ϵ^3 and the degree of their coefficients is bounded by δ_ϵ^3 too.
Besides, the polynomial W is nothing else than the squarefree part of the minimal polynomial of the multiplication map $f \mapsto f\cdot\lambda$ in the quotient ring $\mathbb{K}(h,\epsilon)[x,u,z]/(\mathcal{I}_\epsilon + \langle -\lambda + \lambda_1 x + \lambda_2 u + \lambda_3 z\rangle)$ and the above parametrization is valid outside the vanishing set of $\widetilde{W'}$. We next compute from this data the squarefree part R_ϵ of the characteristic polynomial of the map $f \mapsto f\cdot z$ in the above quotient algebra. We proceed by evaluation-interpolation as in Proposition 2.9, using again [41, §5] for the resultant computation needed after transforming the specialized parametrization as a lexicographic Gröbner basis. The only difference is that the interpolation is done to retrieve bivariate coefficients. The degrees of R_ϵ in h and ϵ are bounded above by δ_ϵ^3 from Proposition 3.1 which implies that we need $O(\delta_\epsilon^6)$ evaluation points. We then deduce that this step used $\tilde{O}(\delta_\epsilon^{10.89})$ operations in $\mathbb{K}$. Using $L_\epsilon \le \delta_\epsilon^5$ concludes the proof. □

We are now in position to prove our main result.

Theorem 3.3. *For P as in (8) of degree δ, there exists a polynomial $R \in \mathbb{K}[z,t]\setminus\{0\}$ annihilating $F(t,a)$, of total arithmetic size $O(\delta^6)$. Moreover, one can compute R in $\tilde{O}(\delta^{14})$ arithmetic operations in $\mathbb{K}$.*

Proof. One first deforms equation (6) as in §3.1. Then, the proof follows from Propositions 3.1 and 3.2 and from $\delta_\epsilon = O(\delta)$. □

4 CONCLUSION AND FUTURE WORK

This article is just a first preliminary step towards a good understanding of effectivity issues related to Theorem 1.1. Many things remain to be done. Already in the case $k = 1$, we plan to address the optimality (size of the objects / complexity) of the exponents in our estimates, as well as to implement and compare the practical performances of the various algorithms, and to use them in order to treat challenging combinatorial examples. We also plan to extend our study to the case $k > 1$.

ACKNOWLEDGEMENTS

This work has been supported by the French ANR grant DeRerum-Natura, ANR-19-CE40-0018.

REFERENCES

[1] S. A. Abramov and M. van Hoeij. Desingularization of linear difference operators with polynomial coefficients. In *ISSAC'99*, pages 269–275. ACM, 1999.
[2] J. Alman and V. Vassilevska Williams. A refined laser method and faster matrix multiplication. In *SODA'21*, pages 522–539. SIAM, 2021.
[3] J. M. Aroca, J. Cano, R. Feng, and X. S. Gao. Algebraic general solutions of algebraic ordinary differential equations. In *ISSAC'05*, pages 29–36. ACM, 2005.
[4] C. Banderier and P. Flajolet. Basic analytic combinatorics of directed lattice paths. volume 281, pages 37–80. 2002. Selected papers in honour of Maurice Nivat.
[5] W. Baur and V. Strassen. The complexity of partial derivatives. *Theoret. Comput. Sci.*, 22(3):317–330, 1983.
[6] D. Bayer and M. Stillman. On the complexity of computing syzygies. *J. Symbolic Comput.*, 6(2-3):135–147, 1988. Computational aspects of commutative algebra.
[7] 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.
[8] O. Bernardi and M. Bousquet-Mélou. Counting colored planar maps: algebraicity results. *J. Combin. Theory Ser. B*, 101(5):315–377, 2011.
[9] D. Bertrand and F. Beukers. Équations différentielles linéaires et majorations de multiplicités. *Ann. Sci. École Norm. Sup. (4)*, 18(1):181–192, 1985.
[10] E. Bierstone, D. Grigoriev, P. Milman, and J. a. Włodarczyk. Effective Hironaka resolution and its complexity. *Asian J. Math.*, 15(2):193–228, 2011.
[11] N. Bonichon, M. Bousquet-Mélou, P. Dorbec, and C. Pennarun. On the number of planar Eulerian orientations. *European J. Combin.*, 65:59–91, 2017.
[12] A. Bostan, M. Bousquet-Mélou, M. Kauers, and S. Melczer. On 3-dimensional lattice walks confined to the positive octant. *Ann. Comb.*, 20(4):661–704, 2016.
[13] A. Bostan, G. Chèze, T. Cluzeau, and J.-A. Weil. Efficient algorithms for computing rational first integrals and Darboux polynomials of planar polynomial vector fields. *Math. Comp.*, 85(299):1393–1425, 2016.
[14] A. Bostan, F. Chyzak, G. Lecerf, B. Salvy, and E. Schost. Differential equations for algebraic functions. In *ISSAC'07*, pages 25–32. ACM, 2007.
[15] A. Bostan, F. Chyzak, M. van Hoeij, M. Kauers, and L. Pech. Hypergeometric expressions for generating functions of walks with small steps in the quarter plane. *European J. Combin.*, 61:242–275, 2017.
[16] A. Bostan, C.-P. Jeannerod, and E. Schost. Solving structured linear systems with large displacement rank. *Theoret. Comput. Sci.*, 407(1-3):155–181, 2008.
[17] A. Bostan and M. Kauers. Automatic classification of restricted lattice walks. In *FPSAC'09*, pages 201–215. Assoc. Discrete Math. Theor. Comput. Sci., 2009.
[18] A. Bostan, T. Rivoal, and B. Salvy. Explicit degree bounds for right factors of linear differential operators. *Bull. Lond. Math. Soc.*, 53(1):53–62, 2021.
[19] 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.
[20] 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.
[21] E. Brézin, C. Itzykson, G. Parisi, and J. B. Zuber. Planar diagrams. *Comm. Math. Phys.*, 59(1):35–51, 1978.
[22] W. G. Brown. Enumeration of non-separable planar maps. *Canadian J. Math.*, 15:526–545, 1963.
[23] W. G. Brown. On the existence of square roots in certain rings of power series. *Math. Ann.*, 158:82–89, 1965.
[24] W. G. Brown and W. T. Tutte. On the enumeration of rooted non-separable planar maps. *Canadian J. Math.*, 16:572–577, 1964.
[25] D. G. Cantor and E. Kaltofen. On fast multiplication of polynomials over arbitrary algebras. *Acta Inform.*, 28(7):693–701, 1991.
[26] L. Castelli Aleardi, O. Devillers, and G. Schaeffer. Optimal succinct representations of planar maps. In *Computational geometry (SCG'06)*, pages 309–318. ACM, 2006.
[27] S. Chen, M. Kauers, and M. F. Singer. Desingularization of Ore operators. *J. Symbolic Comput.*, 74:617–626, 2016.
[28] D. V. Chudnovsky and G. V. Chudnovsky. On expansion of algebraic functions in power and Puiseux series. I. *J. Complexity*, 2(4):271–294, 1986.
[29] D. V. Chudnovsky and G. V. Chudnovsky. Approximations and complex multiplication according to Ramanujan. In *Ramanujan revisited (Urbana-Champaign, Ill., 1987)*, pages 375–472. Academic Press, Boston, MA, 1988.
[30] G. V. Chudnovsky. Rational and Padé approximations to solutions of linear differential equations and the monodromy theory. In *Complex analysis, microlocal calculus and relativistic quantum theory*, volume 126 of *LNP*, pages 136–169. Springer, 1980.
[31] D. A. Cox. Stickelberger and the eigenvalue theorem. *arXiv preprint arXiv:2007.12573*, 2020.
[32] D. Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, 1995. With a view toward algebraic geometry.
[33] P. Flajolet and R. Sedgewick. *Analytic combinatorics*. Cambridge University Press, Cambridge, 2009.
[34] M. van Hoeij. Computing parameterizations of rational algebraic curves. In *ISSAC'94*, page 187–190. ACM, 1994.
[35] M. van Hoeij. Rational parametrizations of algebraic curves using a canonical divisor. *J. Symbolic Comput.*, 23(2-3):209–227, 1997.
[36] J. von zur Gathen and J. Gerhard. *Modern computer algebra*. Cambridge Univ. Press, third edition, 2013.
[37] I. M. Gessel and D. Zeilberger. An Empirical Method for Solving (Rigorously!) Algebraic-Functional Equations of the Form $F(P(x, t), P(x, 1), x, t) = 0$, 2014. Published in the Personal Journal of Shalosh B. Ekhad and Doron Zeilberger, https://sites.math.rutgers.edu/~zeilberg/mamarim/mamarimhtml/funeq.html.
[38] O. Giménez and M. Noy. Asymptotic enumeration and limit laws of planar graphs. *J. AMS*, 22(2):309–329, 2009.
[39] P. Giorgi, C.-P. Jeannerod, and G. Villard. On the complexity of polynomial matrix computations. In *ISSAC'03*, pages 135–142. ACM, 2003.
[40] M. Giusti, G. Lecerf, and B. Salvy. A Gröbner free alternative for polynomial system solving. *J. Complexity*, 17(1):154–211, 2001.
[41] S. G. Hyun, V. Neiger, and E. Schost. Implementations of efficient univariate polynomial matrix algorithms and application to bivariate resultants. In *ISSAC'19*, pages 235–242. ACM, 2019.
[42] E. Kaltofen. Polynomial-time reductions from multivariate to bi- and univariate integral polynomial factorization. *SIAM J. Comput.*, 14(2):469–489, 1985.
[43] D. Lazard and S. McCallum. Iterated discriminants. *J. Symbolic Comput.*, 44(9):1176–1193, 2009.
[44] E. W. Mayr and A. R. Meyer. The complexity of the word problems for commutative semigroups and polynomial ideals. *Adv. in Math.*, 46(3):305–329, 1982.
[45] M. Mňuk, J. R. Sendra, and F. Winkler. On the complexity of parametrizing curves. *Beiträge Algebra Geom.*, 37(2):309–328, 1996.
[46] G. Pólya. Guessing and proving. *The Two-Year College Mathematics Journal*, 9(1):21–27, 1978.
[47] D. Popescu. General Néron desingularization and approximation. *Nagoya Math. J.*, 104:85–115, 1986.
[48] 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.
[49] J. Schicho. On the choice of pencils in the parametrization of curves. *J. Symbolic Comput.*, 14(6):557–576, 1992.
[50] A. Schönhage. Schnelle Multiplikation von Polynomen über Körpern der Charakteristik 2. *Acta Informatica*, 7:395–398, 1977.
[51] É. Schost. Computing parametric geometric resolutions. *Appl. Algebra Eng. Commun. Comput.*, 13(5):349–393, 2003.
[52] J. R. Sendra and F. Winkler. Symbolic parametrization of curves. *J. Symbolic Comput.*, 12(6):607–631, 1991.
[53] J. R. Sendra and F. Winkler. Parametrization of algebraic curves over optimal field extensions. *J. Symbolic Comput.*, 23(2-3):191–207, 1997.
[54] W. T. Tutte. A census of planar triangulations. *Canadian J. Math.*, 14:21–38, 1962.
[55] W. T. Tutte. On the enumeration of planar maps. *Bull. AMS*, 74:64–74, 1968.
[56] O. Villamayor U. On constructive desingularization. *J. Symbolic Comput.*, 39(3-4):465–491, 2005.
[57] D. Y. Y. Yun. On square-free decomposition algorithms. In *SYMSAC'76*, pages 26–35. ACM, 1976.
[58] 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.
[59] D. Zeilberger. The umbral transfer-matrix method. I. Foundations. volume 91, pages 451–463. 2000. In memory of Gian-Carlo Rota.

5 EXAMPLES

Example 5.1. For planar maps, the bivariate generating function $F(t,u)$ satisfies the DDE (2). In this case, $a=1$, $f(u)=1$ and

$$Q = u^2x^2 + ux + uy, \quad \tilde{Q} = u^2x^2 + ux + \frac{u\,(x-z)}{u-1}, \qquad (13)$$
$$P = t\,u^2\,(u-1)\,x^2 + \left(t\,u^2 - u + 1\right)x - tuz + u - 1.$$

The algorithms presented in the paper will compute, by different means, the polynomial $R(z,t) = 27t^2z^2 + (1-18t)\,z + 16t - 1$ (or a multiple of it) as an annihilating polynomial for $F(t,1)$.

Example 5.2. Taking (7) with $f(u)=1$, $a=0$ and $Q := 97t^2 - 73u^2 - 56x^2 - 62y^2 + 87x$ gives the polynomial equation (8), with

$$\operatorname{disc}_x P = -16352t^2u^6 + \left(21728t^4 - 10535t^2 + 50t + 1\right)u^4 + 248t\left(97t^3 - 56t\,z^2 + 87tz - z + 1\right)u^2,$$

which has a double root at $u=0$.

Example 5.3 (continued). For P as in (13), Algorithm 2.4 computes

$$D_0 = D_1 = t\,(4tz + t - 4)\,u^4 - 2t\,(2tz - 3)\,u^3 + (1-2t)\,u^2 - 2u + 1,$$

then it computes the polynomial of bi-degree $(8,4)$ in (t,z)

$$D_2 = -6912t^8z^4 + 256t^6\,(72t-1)\,z^3 - 512t^5\left(8t^2 + 31t - 1\right)z^2 + 256\left(32t^2 + 16t - 1\right)t^4z - 256\,(16t-1)\,t^4,$$

and it finally returns the polynomial of bi-degree $(4,3)$ in (t,z)

$$R = 27t^4z^3 - t^2\,(45t-1)\,z^2 + t\left(16t^2 + 17t - 1\right)z - t\,(16t-1).$$

If one further completely factors the bivariate polynomial R,

$$R = t\,(tz-1)\left(27t^2z^2 - 18tz + 16t + z - 1\right),$$

one concludes that $F(t,1)$ is a root of $27t^2z^2 + (1-18t)\,z + 16t - 1$, as announced in the introduction.

Example 5.4. Consider the functional equation

$$F(t,u) = 1 + t(uF(t,u)^2 + F(t,u) - F(t,0)). \qquad (14)$$

Here, $\tilde{Q} = u\,x^2 + x - z$ and $P = 1 - x + t(ux^2 + x - z)$. Therefore, $\partial_x P(x,z,0,u) = -1$, hence assumption (**H1**) is violated. Now, Algorithm 2.4 computes $\operatorname{disc}_x P = 4t\,(tz-1)\,u + (t-1)^2$, then its discriminant in u, which is the constant polynomial 1. The output of Algorithm 2.4 is $R=1$, which is obviously wrong. In fact, the unique solution $F(t,u)$ of (14) in $\mathbb{Q}[u][[t]]$ satisfies $F(t,0)=1$, and is a root of $tux^2 + (t-1)x + 1 - t$.

Example 5.5 (continued). For P as in (13), Zeilberger's method computes the first 20 terms in the expansion

$$F(t,u) = 1 + (u+1)\,ut + \left(2u^3 + 3u^2 + 2u + 2\right)ut^2 + \cdots,$$

and from there it guesses a polynomial $S = 27t^3u^4\,(u-1)^2\,x^4 + 54t^2u^2\,(u-1)\left(u^2t - u + 1\right)x^3 + \cdots$ of degree $(4,3,6)$ in (x,t,u). Alternatively, the Gessel-Zeilberger variant computes the first 8 terms of $F(t,u)$, then deduces that $F(t,1) = 1 + 2t + 9t^2 + 54t^3 + 378t^4 + \cdots$, from where it guesses the polynomial $R = 27t^2z^2 + (1-18t)\,z + 16t - 1$ that cancels (conjecturally) $F(t,1)$, and then takes its resultant with P from (13); this gives $t \cdot S$. Then, Step (2) is a non-trivial one: one way to prove the existence of a root G in $\mathbb{K}[u][[t]]$ of S is to use rational parametrizations, but this proof requires human cleverness, in addition to nontrivial algorithms, see e.g. [8, p. 365]. Finally, Step (3) can be performed by algebraic elimination: the intersection of $\langle S(x,t,u), S(z,t,1), T - P\rangle$ and $\mathbb{Q}[T,t,u]$ is generated by $T\left(1728t^3u^2 + 729T^2t^2 - 432t^2u^2 + 36u^2t - u^2\right)$. Since by construction $P(G(t,u),G(t,1),t,u) = O(t)$ is a root of this polynomial, it is 0. By uniqueness of the solution of (2), one concludes that $F(t,u) = G(t,u)$, and hence $F(t,1)$ is a root of $R = S(z,t,1)$.

Example 5.6 (continued). For P as in (13), the hybrid method loops and eventually (or immediately) uses some $\sigma \geq 8$: one could check that any smaller σ will get rejected at Step (2). With $\sigma = 8$, Step (0) computes the first 8 terms in the expansion $F(t,1) = 1 + 2t + 9t^2 + 54t^3 + 378t^4 + \cdots$, which are enough to guess in Step (1) the polynomial $R = 27t^2z^2 + (1-18t)\,z + 16t - 1$. In Step (2), as $\delta = 4$, one first computes the $\sigma\cdot(2\delta^3) + 1 = 1025$ terms of $F(t,1)$, using the polynomial system (10) and the Newton iteration (11) with initial point $\mathbf{F} = [1,1,1]^{\mathrm{T}}$, where $J = \operatorname{Jac}_{x,z,u}(P, \partial_x P, \partial_u P)$ is the matrix

$$\begin{bmatrix} 2t\,u^2\,(u-1)\,x + t\,u^2 - u + 1 & -ut & 3t\,u^2x^2 - 2xt\,(x-1)\,u - tz - x + 1 \\ 2t\,u^2\,(u-1) & 0 & 6t\,u^2x - 4tux + 2ut - 1 \\ 2ut\,(3u-2)\,x + 2ut - 1 & -t & 2xt\,(3ux - x + 1) \end{bmatrix}$$

which yields the simultaneous expansion of

$$\begin{bmatrix} F(t,U(t)) \\ F(t,1) \\ U(t) \end{bmatrix} = \begin{bmatrix} 1 + 2t + 12t^2 + 90t^3 + 756t^4 + 6804t^5 + \cdots \\ 1 + 2t + 9t^2 + 54t^3 + 378t^4 + 2916t^5 + \cdots \\ 1 + t + 4t^2 + 25t^3 + 190t^4 + 1606t^5 + \cdots \end{bmatrix}.$$

Checking $R(F(t,1),t) \bmod t^{1025} = 0$ *proves* that $R(F(t,1),t) = 0$. The needed precision 1025 is so large because of the very pessimistic a priori bound $2\delta^3 = 128$ on $\deg R = 4$. Any improvement in this bound would result in (much) less computations.

Example 5.7 (continued). Consider the functional equation (14). The corresponding deformed functional equation is

$$G(h,u,\epsilon) = 1 + \epsilon h\Delta_0 G(h,u,\epsilon) + h^2(uG(h,u,\epsilon)^2 + u\Delta_0 G(h,u,\epsilon)).$$

Hence, the deformed polynomial equation is given by

$$P_\epsilon := (1-x)u + \epsilon h(x-z) + uh^2(ux^2 + x - z).$$

The determinant of the Jacobian matrix $\operatorname{Jac}_{x,u,z}(P_\epsilon, \partial_x P_\epsilon, \partial_u P_\epsilon)$ is

$$\mathcal{D} = (8u^3x^2 + 4u^2x - 2u^2z)h^6 + (12\epsilon u^2x^2 + 4\epsilon ux)h^5 + (-4u^2x + 2u^2)h^4 + (-8\epsilon ux - \epsilon)h^3 + \epsilon h.$$

From there, one determines $\mathcal{I}_\epsilon$ and computes $\mathcal{J}_\epsilon \cap \mathbb{K}[z,h,\epsilon]$. A generator of the principal ideal $\mathcal{J}_\epsilon \cap \mathbb{K}[z,h,\epsilon]$ is

$$R_\epsilon := 16\epsilon^2h^6z^3 + (-\epsilon h^7 + 20\epsilon h^5 + 8\epsilon h^3)z^2 + (-18\epsilon h^5 - h^6 - 36\epsilon h^3 + 3h^4 - 3h^2 + 1)z + h^6 + 27\epsilon h^3 - 3h^4 + 3h^2 - 1.$$

Specializing ϵ to 0 gives $R_0 = -(h-1)^3(h+1)^3(z-1)$. From there, we recover that $z-1$ annihilates $F(t,0) = 1$.