Fast Algorithms for Discrete Differential Equations

Journées Nationales de Calcul Formel 2023 CIRM, Luminy, 6—10 March 2023

Hadrien Notarantonio (Inria Saclay)

Joint work with:
Alin Bostan (Inria Saclay)
Mohab Safey El Din (Sorbonne Université)

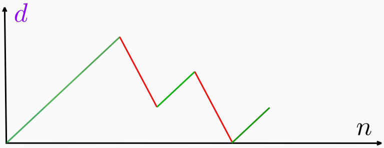
Motivation: Enumerating discrete structures...

Counting walks in $\mathbb{N}$ with steps in $\{+1, -2\}$

$c_n := \#\{n$ steps walks starting at 0 and ending at height $0\}$

$\updownarrow$

$G(t) := \sum_{n=0}^{\infty} c_n t^n$ generating function



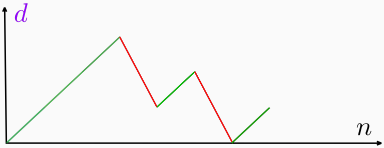
Motivation: Enumerating discrete structures...

Counting walks in $\mathbb{N}$ with steps in $\{+1, -2\}$

$c_n := \#\{n$ steps walks starting at 0 and ending at height $0\}$

$\updownarrow$

$G(t) := \sum_{n=0}^{\infty} c_n t^n$ generating function



Enumeration refinement

$c_{n,d} := \# \{n$ steps walks starting at 0 and ending at height $d\}$

$\updownarrow$

$F(t, u) := \sum_{n=0}^{\infty} \sum_{d=0}^{n} c_{n,d} u^d t^n$ complete generating function

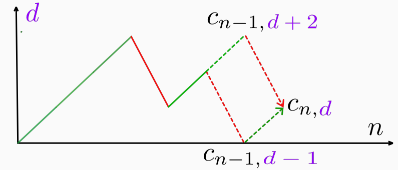
Motivation: Enumerating discrete structures...

Counting walks in $\mathbb{N}$ with steps in $\{+1, -2\}$

$c_n := \#\{n$ steps walks starting at 0 and ending at height $0\}$

$\updownarrow$

$G(t) := \sum_{n=0}^{\infty} c_n t^n$ generating function



Enumeration refinement

$c_{n,d} := \#\ \{n$ steps walks starting at 0 and ending at height $d\}$

$\updownarrow$

$F(t,u) := \sum_{n=0}^{\infty} \sum_{d=0}^{n} c_{n,d} u^d t^n$
complete generating function

DDE of order 2

$$c_{n,d} = c_{n-1,d-1} + c_{n-1,d+2}$$

$\updownarrow$

$$F(t,u) = 1 + t \cdot u \cdot F(t,u) + t \cdot \frac{F(t,u) - F(t,0) - u \cdot \partial_u F(t,0)}{u^2}$$

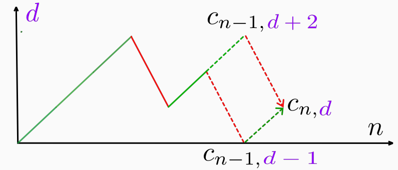
Motivation: Enumerating discrete structures...

Counting walks in $\mathbb{N}$ with steps in $\{+1, -2\}$

$c_n := \#\{n$ steps walks starting at 0 and ending at height $0\}$

$$\updownarrow$$

$G(t) := \sum_{n=0}^{\infty} c_n t^n$ generating function



Enumeration refinement

$c_{n,d} := \#\ \{n$ steps walks starting at 0 and ending at height $d\}$

$$\updownarrow$$

$F(t,u) := \sum_{n=0}^{\infty} \sum_{d=0}^{n} c_{n,d} u^d t^n$
complete generating function

DDE of order 2

$$c_{n,d} = c_{n-1,d-1} + c_{n-1,d+2}$$

$$\updownarrow$$

$$F(t,u) = 1 + t \cdot u \cdot F(t,u) + t \cdot \frac{F(t,u) - F(t,0) - u \cdot \partial_u F(t,0)}{u^2}$$

$$c_{n,0} = c_n \implies F(t,0) = G(t)$$

... yields challenging computational problems

$\mathbb{K}$ effective field of characteristic 0. $\mathbb{K} = \mathbb{Q}, \mathbb{Q}(y), \ldots$

Starting point: $F \in \mathbb{K}[u][[t]]$, solution of the discrete differential equation of order **2**

$$F(t,u) = 1 + t \cdot u \cdot F(t,u) + t \cdot \Delta^{(2)} F(t,u),$$

where $\Delta F(t,u) := \frac{F(t,u) - F(t,0)}{u}$ and $\Delta^{(2)} F(t,u) = \frac{F(t,u) - F(t,0) - u \cdot \partial_u F(t,0)}{u^2}$.

... yields challenging computational problems

$\mathbb{K}$ effective field of characteristic 0. $\mathbb{K} = \mathbb{Q}, \mathbb{Q}(y), \ldots$

Starting point: $F \in \mathbb{K}[u][[t]]$, solution of the discrete differential equation of order **2**

$$F(t,u) = 1 + t \cdot u \cdot F(t,u) + t \cdot \Delta^{(2)} F(t,u),$$

where $\Delta F(t,u) := \frac{F(t,u) - F(t,0)}{u}$ and $\Delta^{(2)} F(t,u) = \frac{F(t,u) - F(t,0) - u \cdot \partial_u F(t,0)}{u^2}$.

Interest: Nature of $F(t,0)$.

… yields challenging computational problems

$\mathbb{K}$ effective field of characteristic 0. $\mathbb{K} = \mathbb{Q}, \mathbb{Q}(y), \dots$

Starting point: $F \in \mathbb{K}[u][[t]]$, solution of the discrete differential equation of order **2**

$$F(t, u) = 1 + t \cdot u \cdot F(t, u) + t \cdot \Delta^{(2)} F(t, u),$$

where $\Delta F(t, u) := \frac{F(t,u) - F(t,0)}{u}$ and $\Delta^{(2)} F(t, u) = \frac{F(t,u) - F(t,0) - u \cdot \partial_u F(t,0)}{u^2}$.

Interest: Nature of $F(t, 0)$.

Classical: F, $F(t, 0)$ and $\partial_u F(t, 0)$ are algebraic. [Bousquet-Mélou, Jehanne '06]

... yields challenging computational problems

$\mathbb{K}$ effective field of characteristic 0. $\mathbb{K} = \mathbb{Q}, \mathbb{Q}(y), \dots$

Starting point: $F \in \mathbb{K}[u][[t]]$, solution of the discrete differential equation of order **2**

$$F(t,u) = 1 + t \cdot u \cdot F(t,u) + t \cdot \Delta^{(2)} F(t,u),$$

where $\Delta F(t,u) := \frac{F(t,u) - F(t,0)}{u}$ and $\Delta^{(2)} F(t,u) = \frac{F(t,u) - F(t,0) - u \cdot \partial_u F(t,0)}{u^2}$.

Interest: Nature of $F(t,0)$.

Classical: F, $F(t,0)$ and $\partial_u F(t,0)$ are algebraic. [Bousquet-Mélou, Jehanne '06]

Goals:

- Compute a polynomial $R \in \mathbb{K}[t, z_0] \setminus \{0\}$ such that $R(t, F(t,0)) = 0$.
- Estimate the size of R for such DDEs.
- Complexity estimates (ops. in $\mathbb{K}$) for the computation of R.

State of the art

Let $k \geq 1$, $f \in \mathbb{K}[u]$ and $Q \in \mathbb{K}[x, y_1, \ldots, y_k, t, u]$. For $F \in \mathbb{K}[u][[t]]$, define $\Delta(F) := (F - F(t,0))/u \in \mathbb{K}[u][[t]]$ and $\Delta^{(i)}(F) := \Delta \circ \Delta^{(i-1)}(F)$.

Theorem [Bousquet-Mélou, Jehanne '06]
There exists a unique solution $F \in \mathbb{K}[u][[t]]$ to

$$F(t,u) = f(u) + t \cdot Q(F, \Delta(F), \ldots, \Delta^{(k)}(F), t, u), \quad \textbf{(DDE)}$$

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

State of the art

Let $k \geq 1$, $f \in \mathbb{K}[u]$ and $Q \in \mathbb{K}[x, y_1, \ldots, y_k, t, u]$. For $F \in \mathbb{K}[u][[t]]$, define $\Delta(F) := (F - F(t,0))/u \in \mathbb{K}[u][[t]]$ and $\Delta^{(i)}(F) := \Delta \circ \Delta^{(i-1)}(F)$.

Theorem [Bousquet-Mélou, Jehanne '06]
There exists a unique solution $F \in \mathbb{K}[u][[t]]$ to

$$F(t,u) = f(u) + t \cdot Q(F, \Delta(F), \ldots, \Delta^{(k)}(F), t, u), \qquad \textbf{(DDE)}$$

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

[Tutte, Brown 60's], [Zeilberger '92]:	Guess-and-prove
[Gessel, Zeilberger '14]:	Guess-and-prove
[Brown '65], [Bender, Canfield '94]:	Quadratic method
[Knuth '68], [Banderier, Flajolet '02], [Bousquet-Mélou, Petkovšek '00]:	Kernel method (linear case)
[Bousquet-Mélou, Jehanne '06]:	Polynomial elimination
[Bostan, Chyzak, Notarantonio, Safey El Din '22]:	Polynomial elimination, Hybrid guess-and-prove

Modelization: from (DDE) of order k to structured polynomial systems

We write $P(u) \equiv P(F(t,u), F(t,0), \dots, \partial_u^{k-1} F(t,0), t, u)$ and $\overline{\mathbb{K}}[[t^{\frac{1}{\star}}]] \equiv \bigcup_{d \geq 1} \overline{\mathbb{K}}[[t^{\frac{1}{d}}]]$

[Bousquet-Mélou, Jehanne '06]:

Discrete Differential Equation (DDE)

$\Downarrow$ numer

$$P(u) = 0$$

$\Downarrow$ ∂_u

$$\partial_u F(t,u) \cdot \partial_1 P(u) + \partial_u P(u) = 0$$

Modelization: from (DDE) of order k to structured polynomial systems

We write $P(u) \equiv P(F(t,u), F(t,0), \dots, \partial_u^{k-1}F(t,0), t, u)$ and $\overline{\mathbb{K}}[[t^{\frac{1}{\star}}]] \equiv \bigcup_{d\geq 1} \overline{\mathbb{K}}[[t^{\frac{1}{d}}]]$

[Bousquet-Mélou, Jehanne '06]:

Discrete Differential Equation (DDE)

$\Downarrow$ numer

$P(u) = 0$

$\Downarrow \partial_u$

$\partial_u F(t,u) \cdot \partial_1 P(u) + \partial_u P(u) = 0$

General idea:

$\mathbf{U(t)} \in \overline{\mathbb{K}}[[t^{\frac{1}{\star}}]] \setminus \overline{\mathbb{K}}$ solution in u of $\partial_1 P(u) = 0$

$\Downarrow$

$(x,u) = (F(t,\mathbf{U}), \mathbf{U})$ is a solution of

$$\begin{cases} P(x, F(t,0), \dots, \partial_u^{k-1}F(t,0), t, \mathbf{u}) = 0, \\ \partial_1 P(x, F(t,0), \dots, \partial_u^{k-1}F(t,0), t, \mathbf{u}) = 0, \\ \partial_u P(x, F(t,0), \dots, \partial_u^{k-1}F(t,0), t, \mathbf{u}) = 0. \end{cases}$$

Modelization: from (DDE) of order k to structured polynomial systems

We write $P(u) \equiv P(F(t,u), F(t,0), \ldots, \partial_u^{k-1} F(t,0), t, u)$ and $\overline{\mathbb{K}}[[t^{\frac{1}{\star}}]] \equiv \bigcup_{d \geq 1} \overline{\mathbb{K}}[[t^{\frac{1}{d}}]]$

[Bousquet-Mélou, Jehanne '06]:

Discrete Differential Equation (DDE)

$\Downarrow$ numer

$P(u) = 0$

$\Downarrow \partial_u$

$$\partial_u F(t,u) \cdot \partial_1 P(u) + \partial_u P(u) = 0$$

General idea:

$\mathbf{U}(\mathbf{t}) \in \overline{\mathbb{K}}[[t^{\frac{1}{\star}}]] \setminus \overline{\mathbb{K}}$ solution in u of $\partial_1 P(u) = 0$

$\Downarrow$

$(x, u) = (F(t, \mathbf{U}), \mathbf{U})$ is a solution of

$$\begin{cases} P(x, F(t,0), \ldots, \partial_u^{k-1} F(t,0), t, \mathbf{u}) = 0, \\ \partial_1 P(x, F(t,0), \ldots, \partial_u^{k-1} F(t,0), t, \mathbf{u}) = 0, \\ \partial_u P(x, F(t,0), \ldots, \partial_u^{k-1} F(t,0), t, \mathbf{u}) = 0. \end{cases}$$

$\mathbf{U}_1(\mathbf{t}), \ldots, \mathbf{U}_\ell(\mathbf{t}) \in \overline{\mathbb{K}}[[t^{\frac{1}{\star}}]] \setminus \overline{\mathbb{K}}$ distinct solutions in u of $\partial_1 P(u) = 0$ $\rightarrow$

Modelization: from (DDE) of order k to structured polynomial systems

We write $P(u) \equiv P(F(t,u), F(t,0), \ldots, \partial_u^{k-1}F(t,0), t, u)$ and $\overline{\mathbb{K}}[[t^{\frac{1}{\star}}]] \equiv \bigcup_{d\geq 1} \overline{\mathbb{K}}[[t^{\frac{1}{d}}]]$

[Bousquet-Mélou, Jehanne '06]:

Discrete Differential Equation (DDE)

$\Downarrow$ numer

$P(u) = 0$

$\Downarrow \partial_u$

$\partial_u F(t,u) \cdot \partial_1 P(u) + \partial_u P(u) = 0$

General idea:

$\mathbf{U}(\mathbf{t}) \in \overline{\mathbb{K}}[[t^{\frac{1}{\star}}]] \setminus \overline{\mathbb{K}}$ solution in u of $\partial_1 P(u) = 0$

$\Downarrow$

$(x, u) = (F(t, \mathbf{U}), \mathbf{U})$ is a solution of

$$\begin{cases} P(x, F(t,0), \ldots, \partial_u^{k-1}F(t,0), t, \mathbf{u}) = 0, \\ \partial_1 P(x, F(t,0), \ldots, \partial_u^{k-1}F(t,0), t, \mathbf{u}) = 0, \\ \partial_u P(x, F(t,0), \ldots, \partial_u^{k-1}F(t,0), t, \mathbf{u}) = 0. \end{cases}$$

$\mathbf{U_1}(\mathbf{t}), \ldots, \mathbf{U}_\ell(\mathbf{t}) \in \overline{\mathbb{K}}[[t^{\frac{1}{\star}}]] \setminus \overline{\mathbb{K}}$ distinct solutions in u of $\partial_1 P(u) = 0$

$\rightarrow$

The **points**

$(x_1, \mathbf{u_1}) = (F(t, \mathbf{U_1}), \mathbf{U_1}), \ldots, (x_\ell, \mathbf{u}_\ell) = (F(t, \mathbf{U}_\ell), \mathbf{U}_\ell) \in \overline{\mathbb{K}}[[t^{\frac{1}{\star}}]]^2$ are solutions of the conditions:

$$\forall\, 1 \leq i \leq \ell, \quad \begin{cases} P(x_i, F(t,0), \ldots, \partial_u^{k-1}F(t,0), t, \mathbf{u_i}) = 0, \\ \partial_1 P(x_i, F(t,0), \ldots, \partial_u^{k-1}F(t,0), t, \mathbf{u_i}) = 0, \\ \partial_u P(x_i, F(t,0), \ldots, \partial_u^{k-1}F(t,0), t, \mathbf{u_i}) = 0. \end{cases}$$

and $\prod_{i\neq j} (\mathbf{u_i} - \mathbf{u_j}) \neq 0$.

Modelization: from (DDE) of order k to structured polynomial systems

We write $P(u) \equiv P(F(t,u), F(t,0), \dots, \partial_u^{k-1}F(t,0), t, u)$ and $\overline{\mathbb{K}}[[t^{\frac{1}{\star}}]] \equiv \bigcup_{d \geq 1} \overline{\mathbb{K}}[[t^{\frac{1}{d}}]]$

[Bousquet-Mélou, Jehanne '06]:

Discrete Differential Equation (DDE)

$\Downarrow$ numer

$P(u) = 0$

$\Downarrow \partial_u$

$$\partial_u F(t,u) \cdot \partial_1 P(u) + \partial_u P(u) = 0$$

General idea:

$\mathbf{U(t)} \in \overline{\mathbb{K}}[[t^{\frac{1}{\star}}]] \setminus \overline{\mathbb{K}}$ solution in u of $\partial_1 P(u) = 0$

$\Downarrow$

$(x, u) = (F(t, \mathbf{U}), \mathbf{U})$ is a solution of

$$\begin{cases} P(x, F(t,0), \dots, \partial_u^{k-1}F(t,0), t, \mathbf{u}) = 0, \\ \partial_1 P(x, F(t,0), \dots, \partial_u^{k-1}F(t,0), t, \mathbf{u}) = 0, \\ \partial_u P(x, F(t,0), \dots, \partial_u^{k-1}F(t,0), t, \mathbf{u}) = 0. \end{cases}$$

$\mathbf{U_1(t)}, \dots, \mathbf{U_\ell(t)} \in \overline{\mathbb{K}}[[t^{\frac{1}{\star}}]] \setminus \overline{\mathbb{K}}$ distinct solutions in u of $\partial_1 P(u) = 0$

$\rightarrow$

The **points**

$(x_1, \mathbf{u_1}) = (F(t, \mathbf{U_1}), \mathbf{U_1}), \dots, (x_\ell, \mathbf{u_\ell}) = (F(t, \mathbf{U_\ell}), \mathbf{U_\ell}) \in \overline{\mathbb{K}}[[t^{\frac{1}{\star}}]]^2$ are solutions of the conditions:

$$\forall\, 1 \leq i \leq \ell, \quad \begin{cases} P(x_i, F(t,0), \dots, \partial_u^{k-1}F(t,0), t, \mathbf{u_i}) = 0, \\ \partial_1 P(x_i, F(t,0), \dots, \partial_u^{k-1}F(t,0), t, \mathbf{u_i}) = 0, \\ \partial_u P(x_i, F(t,0), \dots, \partial_u^{k-1}F(t,0), t, \mathbf{u_i}) = 0. \end{cases}$$

and $\prod_{i \neq j} (\mathbf{u_i} - \mathbf{u_j}) \neq 0$. $\ell = k \implies$ **$3k$ equations and $3k$ unknowns!**

Our contributions

$$F(t,u) = f(u) + t \cdot Q(F, \Delta(F), \ldots, \Delta^{(k)}(F), t, u), \qquad \textbf{(DDE)}$$

where $\Delta(F) := \frac{F(t,u) - F(t,0)}{u}$.

Input: $P :=$ numerator(DDE),

Goal: Compute $R \in \mathbb{K}[t, z_0] \setminus \{0\}$ s.t. $R(t, F(t,0)) = 0$.

Our contributions

$$F(t,u) = f(u) + t \cdot Q(F, \Delta(F), \dots, \Delta^{(k)}(F), t, u), \qquad \textbf{(DDE)}$$
$$\text{where } \Delta(F) := \frac{F(t,u) - F(t,0)}{u}.$$

Input: $P :=$ numerator(DDE),
Goal: Compute $R \in \mathbb{K}[t, z_0] \setminus \{0\}$ s.t. $R(t, F(t,0)) = 0$.

1. **Geometric analysis** of Bousquet-Mélou and Jehanne's algorithm yielding:
   - Theoretical estimate for the degree of $R \in \mathbb{K}[t, z_0]$ s.t. $R(t, F(t,0)) = 0$,
   - Arithmetic complexity.
2. **New algorithm** based on **algebraic elimination** + Gröbner bases,
3. **Implementations** yielding practical improvements.

Example: (walks in $\mathbb{N}$ with steps in $\{+1, -2\}$)

We consider $P(F(t,u), F(t,0), \partial_u F(t,0), t, u) = 0$

$$u^2 - (u^2 - t(1+u^3)) \cdot F(t,u) - t \cdot F(t,0) - t \cdot u \cdot \partial_u F(t,0) = 0$$

An experimental observation... (Contribution 1)

Example: (walks in $\mathbb{N}$ with steps in $\{+1, -2\}$)

We consider $P(F(t,u), F(t,0), \partial_u F(t,0), t, u) = 0$

$$u^2 - (u^2 - t(1+u^3)) \cdot F(t,u) - t \cdot F(t,0) - t \cdot u \cdot \partial_u F(t,0) = 0$$

Study the solutions of $\partial_1 P(F(t,u), F(t,0), \partial_u F(t,0), t, u) = 0$

$$u^2 = t(1+u^3) \implies u = U_1(t), U_2(t) \in \{\sqrt{t} + O(t), -\sqrt{t} + O(t)\}$$

An experimental observation... (Contribution 1)

Example: (walks in $\mathbb{N}$ with steps in $\{+1, -2\}$)

We consider $P(F(t,u), F(t,0), \partial_u F(t,0), t, u) = 0$

$$u^2 - (u^2 - t(1+u^3)) \cdot F(t,u) - t \cdot F(t,0) - t \cdot u \cdot \partial_u F(t,0) = 0$$

Study the solutions of $\partial_1 P(F(t,u), F(t,0), \partial_u F(t,0), t, u) = 0$

$$u^2 = t(1+u^3) \implies u = U_1(t), U_2(t) \in \{\sqrt{t} + O(t), -\sqrt{t} + O(t)\}$$

Hence $(x_1, u_1, x_2, u_2) = (F(t, U_1), U_1, F(t, U_2), U_2)$ is a solution of the constraints $\mathcal{T}$

$$\mathcal{T}: \quad \text{For } 1 \le i \le 2, \begin{cases} P(x_i, F(t,0), \partial_u F(t,0), t, u_i) & = 0, \\ \partial_1 P(x_i, F(t,0), \partial_u F(t,0), t, u_i) & = 0, \\ \partial_u P(x_i, F(t,0), \partial_u F(t,0), t, u_i) & = 0. \end{cases} \quad m \cdot (u_1 - u_2) = 1,$$

Example: (walks in $\mathbb{N}$ with steps in $\{+1, -2\}$)

We consider $P(F(t,u), F(t,0), \partial_u F(t,0), t, u) = 0$

$$u^2 - (u^2 - t(1+u^3)) \cdot F(t,u) - t \cdot F(t,0) - t \cdot u \cdot \partial_u F(t,0) = 0$$

Study the solutions of $\partial_1 P(F(t,u), F(t,0), \partial_u F(t,0), t, u) = 0$

$$u^2 = t(1+u^3) \implies u = U_1(t), U_2(t) \in \{\sqrt{t} + O(t), -\sqrt{t} + O(t)\}$$

Hence $(x_1, u_1, x_2, u_2) = (F(t, U_1), U_1, F(t, U_2), U_2)$ is a solution of the constraints $\mathcal{T}$

$$\mathcal{T}: \quad \text{For } 1 \leq i \leq 2, \begin{cases} P(x_i, F(t,0), \partial_u F(t,0), t, u_i) & = 0, \\ \partial_1 P(x_i, F(t,0), \partial_u F(t,0), t, u_i) & = 0, \\ \partial_u P(x_i, F(t,0), \partial_u F(t,0), t, u_i) & = 0. \end{cases} \quad m \cdot (u_1 - u_2) = 1,$$

Permuting (x_1, u_1) and (x_2, u_2) does not change the solution set
$\implies \mathfrak{S}_2$ acts on $V(\mathcal{T})$ and preserves the $\{z_0, z_1, t\}$-coordinate space.

Example: (walks in $\mathbb{N}$ with steps in $\{+1,-2\}$)

We consider $P(F(t,u), F(t,0), \partial_u F(t,0), t, u) = 0$

$$u^2 - (u^2 - t(1+u^3)) \cdot F(t,u) - t \cdot F(t,0) - t \cdot u \cdot \partial_u F(t,0) = 0$$

Study the solutions of $\partial_1 P(F(t,u), F(t,0), \partial_u F(t,0), t, u) = 0$

$$u^2 = t(1+u^3) \implies u = U_1(t), U_2(t) \in \{\sqrt{t} + O(t), -\sqrt{t} + O(t)\}$$

Hence $(x_1, u_1, x_2, u_2) = (F(t, U_1), U_1, F(t, U_2), U_2)$ is a solution of the constraints $\mathcal{T}$

$$\mathcal{T}: \quad \text{For } 1 \leq i \leq 2, \quad \begin{cases} P(x_i, F(t,0), \partial_u F(t,0), t, u_i) &= 0, \\ \partial_1 P(x_i, F(t,0), \partial_u F(t,0), t, u_i) &= 0, \\ \partial_u P(x_i, F(t,0), \partial_u F(t,0), t, u_i) &= 0. \end{cases} \quad m \cdot (u_1 - u_2) = 1,$$

Permuting (x_1, u_1) and (x_2, u_2) does not change the solution set
$\implies \mathfrak{S}_2$ acts on $V(\mathcal{T})$ and preserves the $\{z_0, z_1, t\}$-coordinate space.

Impact of this group action?

... yielding theoretical improvements (Contribution 1)

Denote by $\mathcal{I}$ the ideal generated by the k duplications of $(P, \partial_1 P, \partial_u P)$ and $m \cdot \prod_{i \neq j}(u_i - u_j) - 1 = 0$.

Assume that:

- there exist k distinct solutions $u = U_1, \ldots, U_k \in \overline{\mathbb{K}}[[t^{\frac{1}{\star}}]]$ of $\partial_1 P(u) = 0$,
- $\mathcal{I}$ is radical and of dimension 0 over $\mathbb{K}(t)$. (3k equations and 3k unknowns)

Denote by $\mathcal{I}$ the ideal generated by the k duplications of $(P, \partial_1 P, \partial_u P)$ and $m \cdot \prod_{i \neq j}(u_i - u_j) - 1 = 0$.

Assume that:

- there exist k distinct solutions $u = U_1, \ldots, U_k \in \overline{\mathbb{K}}[[t^{\frac{1}{\star}}]]$ of $\partial_1 P(u) = 0$,
- $\mathcal{I}$ is radical and of dimension 0 over $\mathbb{K}(t)$. (3k equations and 3k unknowns)

Theorem [Bostan, N., Safey El Din '23]

- Let $\delta := \deg(P)$. There exists a nonzero polynomial $R \in \mathbb{K}[t, z_0]$ whose partial degrees are bounded by $\delta^{\mathbf{k}}(\delta - \mathbf{1})^{\mathbf{2k}}/\mathbf{k}!$ and such that $R(t, F(t,0)) = 0$.
- There exists an algorithm computing R in $\tilde{\mathbf{O}}(\delta^{\mathbf{6k}}(\mathbf{k}^{\mathbf{2}}\delta^{\mathbf{k+3}} + \delta^{\mathbf{1.89k}}/\mathbf{k}!))$ ops. in $\mathbb{K}$.

Ideas of the proof:

→ Bézout bound + $\mathfrak{S}_k$ acts on $V(\mathcal{I}_{\text{dup}})$ and preserves the z_0-coordinate space.

→ Parametric geometric resolution [Schost '03], [Giusti, Lecerf, Salvy '01]

$$z_0 = V(t,\lambda)/\partial_\lambda W(t,\lambda), W(t,\lambda) = 0$$

→ Change of monomial ordering:
Stickelberger's theorem [Cox '21] $\quad R = \text{Sqfree}(\text{Res}_\lambda(z_0 \cdot \partial_\lambda W - V, W))$
+ bivariate resultants [Villard '18], [van der Hoeven, Lecerf '21]

Summary of the initial problem: $\underline{z} \equiv z_0, \ldots, z_{k-1}$; $P =$ "numer"$(DDE) \in \mathbb{K}(t)[x, \mathbf{u}, \underline{z}]$

There exist k solutions $(x, \mathbf{u}) \in \overline{\mathbb{K}(t)}^2$ with **distinct** $\mathbf{u}$-coordinates to

$$\begin{cases} P(x, \mathbf{u}, F(t,0), \ldots, \partial_u^{k-1} F(t,0)) & = 0, \\ \partial_1 P(x, \mathbf{u}, F(t,0), \ldots, \partial_u^{k-1} F(t,0)) & = 0, \quad \mathbf{u} \neq 0, \\ \partial_u P(x, \mathbf{u}, F(t,0), \ldots, \partial_u^{k-1} F(t,0)) & = 0. \end{cases}$$

Summary of the initial problem: $\underline{z} \equiv z_0, \ldots, z_{k-1}$; $P =$ "numer"$(DDE) \in \mathbb{K}(t)[x, \mathbf{u}, \underline{z}]$

There exist k solutions $(x, \mathbf{u}) \in \overline{\mathbb{K}(t)}^2$ with **distinct** $\mathbf{u}$-coordinates to

$$\begin{cases} P(x, \mathbf{u}, F(t,0), \ldots, \partial_u^{k-1} F(t,0)) & = 0, \\ \partial_1 P(x, \mathbf{u}, F(t,0), \ldots, \partial_u^{k-1} F(t,0)) & = 0, \quad \mathbf{u} \neq 0, \\ \partial_u P(x, \mathbf{u}, F(t,0), \ldots, \partial_u^{k-1} F(t,0)) & = 0. \end{cases}$$

Define

$$\pi_x : (x, \mathbf{u}, \underline{z}) \in \overline{\mathbb{K}(t)}^{k+2} \mapsto (\mathbf{u}, \underline{z}) \in \overline{\mathbb{K}(t)}^{k+1},$$

$$\pi_u : (\mathbf{u}, \underline{z}) \in \overline{\mathbb{K}(t)}^{k+1} \mapsto (\underline{z}) \in \overline{\mathbb{K}(t)}^{k},$$

and consider $\mathbf{W} := \pi_x(V(P, \partial_1 P, \partial_u P) \setminus V(\mathbf{u}))$.

Summary of the initial problem: $\underline{z} \equiv z_0, \dots, z_{k-1}$; $P =$ "numer"$(DDE) \in \mathbb{K}(t)[x, \mathbf{u}, \underline{z}]$

There exist k solutions $(x, \mathbf{u}) \in \overline{\mathbb{K}(t)}^2$ with **distinct** $\mathbf{u}$-coordinates to

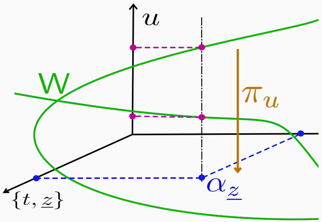
$$\begin{cases} P(x, \mathbf{u}, F(t,0), \dots, \partial_u^{k-1} F(t,0)) &= 0, \\ \partial_1 P(x, \mathbf{u}, F(t,0), \dots, \partial_u^{k-1} F(t,0)) &= 0, \quad \mathbf{u} \neq 0, \\ \partial_u P(x, \mathbf{u}, F(t,0), \dots, \partial_u^{k-1} F(t,0)) &= 0. \end{cases}$$

Define

$$\pi_x : (x, \mathbf{u}, \underline{z}) \in \overline{\mathbb{K}(t)}^{k+2} \mapsto (\mathbf{u}, \underline{z}) \in \overline{\mathbb{K}(t)}^{k+1},$$

$$\pi_u : (\mathbf{u}, \underline{z}) \in \overline{\mathbb{K}(t)}^{k+1} \mapsto (\underline{z}) \in \overline{\mathbb{K}(t)}^{k},$$

and consider $\mathbf{W} := \pi_x(V(P, \partial_1 P, \partial_u P) \setminus V(\mathbf{u}))$.



$$\# \, \pi_u^{-1}(\alpha_{\underline{z}}) \cap W = 2$$

Summary of the initial problem: $\underline{z} \equiv z_0, \ldots, z_{k-1}$; $P =$ "numer"$(DDE) \in \mathbb{K}(t)[x, \mathbf{u}, \underline{z}]$

There exist k solutions $(x, \mathbf{u}) \in \overline{\mathbb{K}(t)}^2$ with **distinct** $\mathbf{u}$-coordinates to

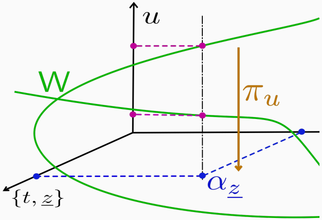
$$\begin{cases} P(x, \mathbf{u}, F(t,0), \ldots, \partial_u^{k-1} F(t,0)) &= 0, \\ \partial_1 P(x, \mathbf{u}, F(t,0), \ldots, \partial_u^{k-1} F(t,0)) &= 0, \quad \mathbf{u} \neq 0, \\ \partial_u P(x, \mathbf{u}, F(t,0), \ldots, \partial_u^{k-1} F(t,0)) &= 0. \end{cases}$$

Define

$$\pi_x : (x, \mathbf{u}, \underline{z}) \in \overline{\mathbb{K}(t)}^{k+2} \mapsto (\mathbf{u}, \underline{z}) \in \overline{\mathbb{K}(t)}^{k+1},$$

$$\pi_u : (\mathbf{u}, \underline{z}) \in \overline{\mathbb{K}(t)}^{k+1} \mapsto (\underline{z}) \in \overline{\mathbb{K}(t)}^{k},$$

and consider $\mathbf{W} := \pi_x(V(P, \partial_1 P, \partial_u P) \setminus V(\mathbf{u}))$.



$\# \, \pi_u^{-1}(\alpha_{\underline{z}}) \cap \mathbf{W} = 2$

Objective:

Characterize with polynomial constraints

$\mathcal{F}_k := \{\alpha_{\underline{z}} \in \overline{\mathbb{K}(t)}^k \mid \# \, \pi_u^{-1}(\alpha_{\underline{z}}) \cap \mathbf{W} \geq k\}$

Example: (Walks in $\mathbb{N}$ with steps in $\{+1, -2\}$)

$$P := (1-x)u^2 + tu^3x + t(x - z_0 - uz_1) \in \mathbb{K}(t)[x, u, z_0, z_1], \qquad k = 2.$$

G_u Gröbner basis of $\langle P, \partial_1 P, \partial_u P, mu - 1\rangle \cap \mathbb{K}[u, t, z_0, z_1]$ for $\{u\} \succ_{lex} \{t, z_0, z_1\}$:

Getting some intuition through our toy example... (Contribution 2)

Example: (Walks in $\mathbb{N}$ with steps in $\{+1, -2\}$)

$P := (1-x)u^2 + tu^3x + t(x - z_0 - uz_1) \in \mathbb{K}(t)[x, u, z_0, z_1]$, $\qquad k = 2.$

G_u Gröbner basis of $\langle P, \partial_1 P, \partial_u P, mu - 1\rangle \cap \mathbb{K}[u, t, z_0, z_1]$ for $\{u\} \succ_{lex} \{t, z_0, z_1\}$:

$$
\begin{aligned}
&\mathbf{B_0}: \quad \gamma_0 \\
&\mathbf{B_1}: \begin{cases} \beta_1 \cdot u + \gamma_1 \\ \vdots \\ \beta_r \cdot u + \gamma_r \end{cases} \quad , \gamma_i, \beta_j \in \mathbb{K}[t, z_0, z_1] \\
&\mathbf{B_2}: \quad g_2 := u^2 + \beta_{r+1} \cdot u + \gamma_{r+1}
\end{aligned}
$$

"At (z_0, z_1) fixed in $\overline{\mathbb{K}(t)}^2$, there exist two distinct roots in u"

Example: (Walks in $\mathbb{N}$ with steps in $\{+1, -2\}$)

$P := (1-x)u^2 + tu^3x + t(x - z_0 - uz_1) \in \mathbb{K}(t)[x, u, z_0, z_1]$, $k = 2$.

G_u Gröbner basis of $\langle P, \partial_1 P, \partial_u P, mu - 1\rangle \cap \mathbb{K}[u, t, z_0, z_1]$ for $\{u\} \succ_{lex} \{t, z_0, z_1\}$:

$$\mathbf{B_0} : \quad \gamma_0$$

$$\mathbf{B_1} : \begin{cases} \beta_1 \cdot u + \gamma_1 \\ \vdots \\ \beta_r \cdot u + \gamma_r \end{cases}, \gamma_i, \beta_j \in \mathbb{K}[t, z_0, z_1]$$

$$\mathbf{B_2} : \quad g_2 := u^2 + \beta_{r+1} \cdot u + \gamma_{r+1}$$

"At (z_0, z_1) fixed in $\overline{\mathbb{K}(t)}^2$, there exist two distinct roots in u"

Necessary condition:
At $\alpha \in V(G_u \cap \mathbb{K}[t, z_0, z_1])$ fixed, there exist two roots in u
$\implies \beta_i, \gamma_j = 0$ (equations)

Getting some intuition through our toy example... (Contribution 2)

Example: (Walks in $\mathbb{N}$ with steps in $\{+1, -2\}$)

$$P := (1-x)u^2 + tu^3x + t(x - z_0 - uz_1) \in \mathbb{K}(t)[x, u, z_0, z_1], \qquad k = 2.$$

G_u Gröbner basis of $\langle P, \partial_1 P, \partial_u P, mu - 1\rangle \cap \mathbb{K}[u, t, z_0, z_1]$ for $\{u\} \succ_{lex} \{t, z_0, z_1\}$:

$\mathbf{B_0}$: γ_0

$$\mathbf{B_1} : \begin{cases} \beta_1 \cdot u + \gamma_1 \\ \vdots \\ \beta_r \cdot u + \gamma_r \end{cases}, \gamma_i, \beta_j \in \mathbb{K}[t, z_0, z_1]$$

$\mathbf{B_2}$: $g_2 := u^2 + \beta_{r+1} \cdot u + \gamma_{r+1}$

"At (z_0, z_1) fixed in $\overline{\mathbb{K}(t)}^2$, there exist two distinct roots in u"

Necessary condition:
At $\alpha \in V(G_u \cap \mathbb{K}[t, z_0, z_1])$ fixed, there exist two roots in u
$\Longrightarrow \beta_i, \gamma_j = 0$ (equations)

Extension theorem:
The pre-image of α by π_u is well-defined
$\Longrightarrow \mathrm{LeadingCoeff}_u(g_2) \neq 0$
Distinct roots in u $\Longrightarrow \mathrm{disc}_u(g_2) \neq 0$ (inequations)

Getting some **intuition** through our toy example... (Contribution 2)

Example: (Walks in $\mathbb{N}$ with steps in $\{+1, -2\}$)

$$P := (1-x)u^2 + tu^3x + t(x - z_0 - uz_1) \in \mathbb{K}(t)[x, u, z_0, z_1], \qquad k = 2.$$

G_u Gröbner basis of $\langle P, \partial_1 P, \partial_u P, mu - 1\rangle \cap \mathbb{K}[u, t, z_0, z_1]$ for $\{u\} \succ_{lex} \{t, z_0, z_1\}$:

$$\mathbf{B_0}: \quad \gamma_0$$

$$\mathbf{B_1}: \begin{cases} \beta_1 \cdot u + \gamma_1 \\ \vdots \\ \beta_r \cdot u + \gamma_r \end{cases}, \gamma_i, \beta_j \in \mathbb{K}[t, z_0, z_1]$$

$$\mathbf{B_2}: \quad g_2 := u^2 + \beta_{r+1} \cdot u + \gamma_{r+1}$$

"At (z_0, z_1) fixed in $\overline{\mathbb{K}(t)}^2$, there exist two distinct roots in u"

Necessary condition:
At $\alpha \in V(G_u \cap \mathbb{K}[t, z_0, z_1])$ fixed, there exist two roots in u
$\implies \beta_i, \gamma_j = 0$ (equations)

Extension theorem:
The pre-image of α by π_u is well-defined
$\implies \text{LeadingCoeff}_u(g_2) \neq 0$
Distinct roots in u $\implies \text{disc}_u(g_2) \neq 0$ (inequations)

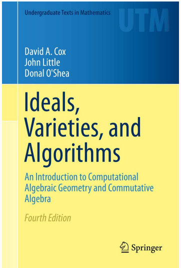
After adding these constraints to G_u and eliminating u and z_1:
$\mathbf{R(t, z_0) = t^3 z_0^3 - z_0 + 1}$ satisfies $\mathbf{R(t, F(t, 0)) = 0}$

… yields an algorithm based on elimination theory (Contribution 2)

- **Projecting**: Elimination theorem
- **Lifting points of the projections**: Extension theorems

Cardinality conditions on the fibers:

- Extension theorem (Gröbner bases version)
- $g(u, \alpha_{\underline{z}}) \in \overline{\mathbb{K}(t)}[u]$ of degree $k+j$ has at least k distinct roots $\iff$ One of the $(k \times k)$-minors of the Hermite quadratic form associated with g does not vanish at $\alpha_{\underline{z}}$

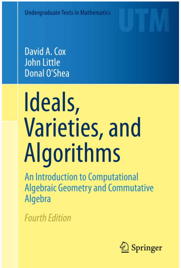


... yields an algorithm based on elimination theory (Contribution 2)

- **Projecting**: Elimination theorem
- **Lifting points of the projections**: Extension theorems

Cardinality conditions on the fibers:

- Extension theorem (Gröbner bases version)
- $g(u, \alpha_{\underline{z}}) \in \overline{\mathbb{K}(t)}[u]$ of degree $k+j$ has at least k distinct roots
  $\iff$ One of the $(k \times k)$-minors of the Hermite quadratic form associated with g does not vanish at $\alpha_{\underline{z}}$



[Bostan, N., Safey El Din '23] :
Conjunctions of polynomial equations and inequations whose zero set is $\mathcal{F}_k$

First implementations yielding practical improvements (Contribution 3)

3-Tamari, $k = 3$

A	T	d_t	d_{z_0}
D	2d2h	5	16
DE	2m	5	16
HGP + DE	1h40m	5	16

5-constellations, $k = 4$

A	T	d_t	d_{z_0}
D	∞	—	—
DE	∞	26 •	53 •
HGP + DE	6h7m	2	5

•: data obtained after a computation mod $p = 65521$.

- **A**: Algorithm used (D: duplication, DE: direct elimination, HGP: Hybrid Guess-and-Prove [Bostan, Chyzak, N., Safey El Din '22]),
- **T**: total timing needed to obtain an output in $\mathbb{Q}[t, z_0]$,
- $\mathbf{d_Z}$: degree in $Z \in \{t, z_0\}$ of output $R \in \mathbb{Q}[t, z_0]$ s.t. $R(t, F(t, a)) = 0$,

Intel® Xeon® Gold CPU 6246R v4 @ 3.40GHz and 1.5TB of RAM with a single thread.
Gröbner bases computations are performed using the C library msolve, and all guessing computations are performed using the gfun Maple package.

Conclusion and future works

Conclusion

- New geometric interpretations of the problem “solving a DDE”,
- New algorithm based on algebraic elimination and Gröbner bases,
- Some promising practical results,
- (In the preprint) New geometric algorithm based on Stickelberger’s theorem.

Future works

- Study the *minimality* and the *genericity* of the introduced assumptions,
- Provide a maple package for solving DDEs, together with a tutorial paper.

Bibliography

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.

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.

A. Bostan, F. Chyzak, H. Notarantonio, and M. S. El Din.
Algorithms for discrete differential equations of order 1.
In *ISSAC'22*, pages 101–110. ACM, New York, [2022] ©2022.

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.

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.

M. Bousquet-Mélou and M. Petkovšek.
Linear recurrences with constant coefficients: the multivariate case.
Discrete Math., 225(1-3):51–75, 2000.
Formal power series and algebraic combinatorics (Toronto, ON, 1998).

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.

D. E. Knuth.
The art of computer programming. Vol. 1: Fundamental algorithms.
Second printing. Addison-Wesley, Reading, MA, 1968.

G. Pólya.
Guessing and proving.
The Two-Year College Mathematics Journal, 9(1):21–27, 1978.

B. Salvy and P. Zimmermann.
Gfun: a Maple package for the manipulation of generating and holonomic functions in one variable.
ACM Transactions on Mathematical Software, 20(2):163–177, 1994.

É. Schost.
Computing parametric geometric resolutions.
Appl. Algebra Eng. Commun. Comput., 13(5):349–393, 2003.

Input: $P(F(t,u), F(t,0), \ldots, \partial_u^{k-1}F(t,0), t, u) = 0$, $\delta := \deg(P)$.

Output: $R \in \mathbb{K}[t, z_0] \setminus \{0\}$ annihilating $F_0 = F(t,0)$, i.e. $R(t, F_0) = 0$.

Input: $P(F(t,u), F(t,0), \dots, \partial_u^{k-1}F(t,0), t, u) = 0$, $\delta := \deg(P)$.
Output: $R \in \mathbb{K}[t, z_0] \setminus \{0\}$ annihilating $F_0 = F(t,0)$, i.e. $R(t, F_0) = 0$.

geometry

(1) Functional equation

↓

(2) Polynomial system

↓

(3) Bounds

- $\deg_t(R) \leq b_t$,
- $\deg_{z_0}(R) \leq b_z$.

Input: $P(F(t,u), F(t,0), \dots, \partial_u^{k-1} F(t,0), t, u) = 0$, $\delta := \deg(P)$.
Output: $R \in \mathbb{K}[t, z_0] \setminus \{0\}$ annihilating $F_0 = F(t,0)$, i.e. $R(t, F_0) = 0$.

geometry

(1) Functional equation

↓

(2) Polynomial system

↓

(3) Bounds

- $\deg_t(R) \leq b_t$,
- $\deg_{z_0}(R) \leq b_z$.

guess-and-prove

(4) Expand F_0

↓

(5) Compute $R \in \mathbb{K}[t, z_0]$ s.t. $R(t, F_0) = O(t^{\sim b_t b_z})$

↓

(6) Certify that $R(t, F_0) = 0$

Input: $P(F(t,u), F(t,0), \ldots, \partial_u^{k-1} F(t,0), t, u) = 0$, $\delta := \deg(P)$.
Output: $R \in \mathbb{K}[t, z_0] \setminus \{0\}$ annihilating $F_0 = F(t,0)$, i.e. $R(t, F_0) = 0$.

geometry

(1) Functional equation
↓
(2) Polynomial system
↓
(3) Bounds
- $\deg_t(R) \leq b_t$,
- $\deg_{z_0}(R) \leq b_z$.

guess-and-prove

(4) Expand F_0
↓
(5) Compute $R \in \mathbb{K}[t, z_0]$ s.t. $R(t, F_0) = O(t^{\sim b_t b_z})$
↓
(6) Certify that $R(t, F_0) = 0$

tools

- Newton iteration

↓

- Algebraic approximants "seriestoalgeq"

↓

- Multiplicity lemma: $R(t, F_0) = O(t^{\sim 2 b_t b_z})$ implies $R(t, F_0) = 0$

Solving our toy example using the Hybrid Guess-and-Prove strategy

Counting walks in $\mathbb{N}$ with steps in $\{+1, -2\}$

$$F(t,u) = 1 + t \cdot u \cdot F(t,u) + t \cdot \frac{F(t,u) - F(t,0) - u \cdot \partial_u F(t,0)}{u^2}$$

- Draw a random $c = 1341$, and a prime number $p = 19541$,
- Using the new algorithm based on elimination theory, we obtain:
  - $R(t,c) \mod p = t^3 + 15794$,
  - $R(c,z_0) \mod p = z_0^3 + 18182z_0 + 1319$.
- Set $b_t = 3$, $b_{z_0} = 3$,
- Compute
  $F(t,0) = 1 + t^3 + 3t^6 + 12t^9 + 55t^{12} + 273t^{15} + 1428t^{18} + O(t^{2 \cdot b_t \cdot b_{z_0} + 1})$
- Guess $A := t^3 z_0^3 - z0 + 1$ such that $A(t, F(t,0)) = O(t^{(b_t+1)\cdot(b_{z_0}+1)-1})$,
- Check that $A(t, F(t,0)) = O(t^{2 \cdot b_t \cdot b_{z_0} + 1})$

The output A is certified.