Solving combinatorial equations via computer algebra

RTCA Topical Day: Elimination for Functional Equations, 11 December 2023

Hadrien Notarantonio (Inria Saclay – Sorbonne Université)

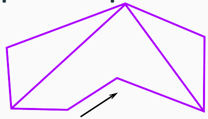
Joint work with:

Alin Bostan (Inria Saclay)

Mohab Safey El Din (Sorbonne Université)

Which type of equations are we looking at?

rooted planar maps

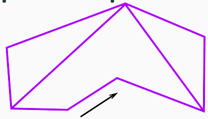


$$F(t,u) = 1 + tu\left(uF(t,u)^2 + \frac{uF(t,u) - F(t,1)}{u-1}\right)$$

[Tutte '68]

Which type of equations are we looking at?

rooted planar maps



$$F(t,u) = 1 + tu\left(uF(t,u)^2 + \frac{uF(t,u) - F(t,1)}{u-1}\right)$$ [Tutte '68]

$a_n := \#\ \{\text{planar maps with } n \text{ edges}\}$

$\downarrow$ refinement

$a_{n,d} := \#\{\text{planar maps with } n \text{ edges, } d \text{ of them on the external face}\}$

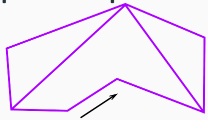
$\sum_{n=0}^{\infty} a_n t^n$ generating function

$\downarrow$ refinement

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

Which type of equations are we looking at?

rooted planar maps



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

[Tutte '68]

$a_n := \#\,\{\text{planar maps with } n \text{ edges}\}$

↓ refinement

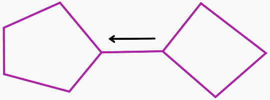
$a_{n,d} := \#\{\text{planar maps with } n \text{ edges, } d \text{ of them on the external face}\}$

$\sum_{n=0}^{\infty} a_n t^n$ generating function

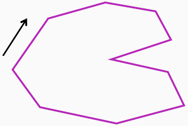
↓ refinement

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

1



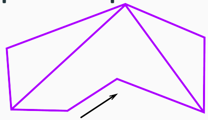
$tu^2 F(t,u)^2$



$tu\frac{uF(t,u) - F(t,1)}{u-1}$

Which type of equations are we looking at?

rooted planar maps



$$F(t,u) = 1 + tu\left(uF(t,u)^2 + \frac{uF(t,u) - F(t,1)}{u-1}\right)$$ [Tutte '68]

$a_n := \#\ \{\text{planar maps with } n \text{ edges}\}$

$\downarrow$ refinement

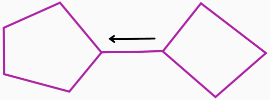
$a_{n,d} := \#\{\text{planar maps with } n \text{ edges},$
$d \text{ of them on the external face}\}$

$\sum_{n=0}^{\infty} a_n t^n$ generating function

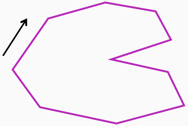
$\downarrow$ refinement

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

1



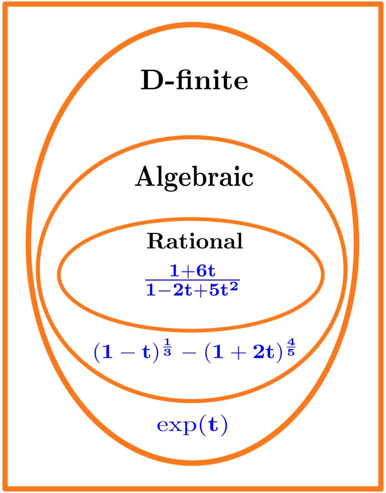
$tu^2F(t,u)^2$



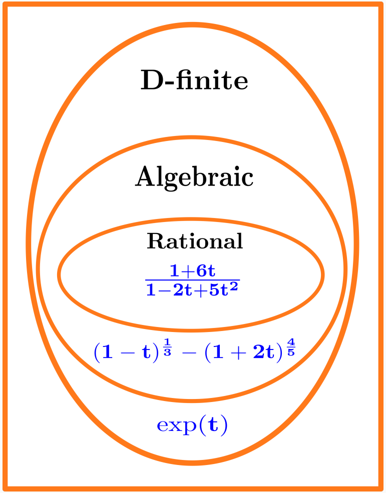
$tu\frac{uF(t,u) - F(t,1)}{u-1}$

$$F(t,1) = \sum_{n=0}^{\infty} a_n t^n$$

Solving functional equations



Solving functional equations



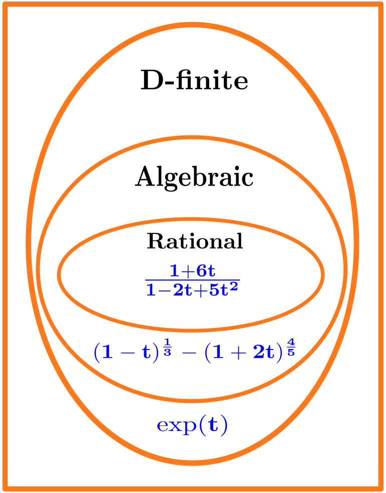
In this talk

Solving $=$ Classifying the initial series $F(t,1)$

$+$ Computing a witness of this classification

(e.g. $R \in \mathbb{Q}[z,t]$ s.t. $R(F(t,1),t) = 0$)

Solving functional equations



In this talk

Solving = Classifying the initial series $F(t,1)$

$+$ Computing a witness of this classification

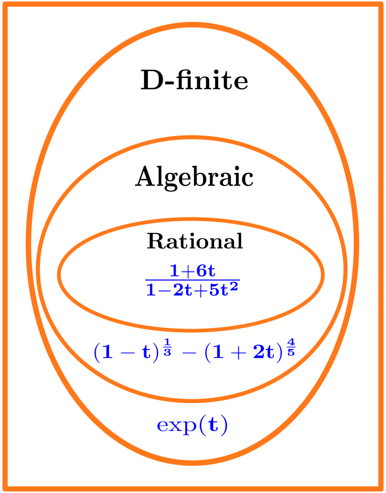
(e.g. $R \in \mathbb{Q}[z,t]$ s.t. $R(F(t,1),t) = 0$)

Going back to our planar maps...

$F(t,1) = 1 + 2t + 9t^2 + 54t^3 + 378t^4 + \cdots \in \mathbb{Q}[[t]]$

annihilated by $R = 27t^2z^2 + (1-18t)z + 16t - 1 \in \mathbb{Q}[z,t]$

Solving functional equations



In this talk

Solving = Classifying the initial series $F(t,1)$

+ Computing a witness of this classification

(e.g. $R \in \mathbb{Q}[z,t]$ s.t. $R(F(t,1),t) = 0$)

Going back to our planar maps...

$F(t,1) = 1 + 2t + 9t^2 + 54t^3 + 378t^4 + \cdots \quad \in \mathbb{Q}[[t]]$

annihilated by $R = 27t^2z^2 + (1-18t)z + 16t - 1 \in \mathbb{Q}[z,t]$

From R:

- **(Recurrence)** $a_0 = 1$ and $(n+3)a_{n+1} - 6(2n+1)a_n = 0$,
- **(Closed-form)** $a_n = 2\frac{3^n(2n)!}{n(n+2)!}$,
- **(Asymptotics)** $a_n \sim 2\frac{12^n}{\sqrt{\pi n^5}}$, when $n \to +\infty$.

Content of the talk

Objectives

- **Introduce** so-called Discrete Differential Equations (DDEs),
- **Determine the nature** of the solutions of DDEs,
- Provide an **efficient algorithm** for computing a witness,
- Implementation in action $\rightsquigarrow$ Solving a problem **previously out of reach**.

Objects of interest: Discrete Differential Equations

Definition

Given $f \in \mathbb{Q}[u]$, $k \geq 1$, and $Q \in \mathbb{Q}[y_0, \ldots, y_k, t, u]$,

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

is a *Discrete Differential Equation*, where $\Delta : F \in \mathbb{Q}[u][[t]] \mapsto \frac{F(t,u) - F(t,1)}{u-1} \in \mathbb{Q}[u][[t]]$, and where for $\ell \geq 1$ we define $\Delta^{\ell+1} = \Delta^{\ell} \circ \Delta$.

Objects of interest: Discrete Differential Equations

Definition

Given $f \in \mathbb{Q}[u]$, $k \geq 1$, and $Q \in \mathbb{Q}[y_0, \ldots, y_k, t, u]$,

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

is a *Discrete Differential Equation*, where $\Delta : F \in \mathbb{Q}[u][[t]] \mapsto \frac{F(t,u)-F(t,1)}{u-1} \in \mathbb{Q}[u][[t]]$, and where for $\ell \geq 1$ we define $\Delta^{\ell+1} = \Delta^{\ell} \circ \Delta$.

Bicolored planar maps: 3-constellations

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

Objects of interest: Discrete Differential Equations

Definition

Given $f \in \mathbb{Q}[u]$, $k \geq 1$, and $Q \in \mathbb{Q}[y_0, \ldots, y_k, t, u]$,

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

is a *Discrete Differential Equation*, where $\Delta : F \in \mathbb{Q}[u][[t]] \mapsto \frac{F(t,u) - F(t,1)}{u-1} \in \mathbb{Q}[u][[t]]$, and where for $\ell \geq 1$ we define $\Delta^{\ell+1} = \Delta^{\ell} \circ \Delta$.

Bicolored planar maps: 3-constellations

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

Theorem [Bousquet-Mélou, Jehanne '06]

The unique solution in $\mathbb{Q}[u][[t]]$ of **(DDE)** *is* algebraic *over $\mathbb{Q}(t,u)$.*

$\rightsquigarrow$ **Constructive proof $\Longrightarrow$ algorithm**

Bousquet-Mélou and Jehanne's algorithm

Input: $F(t,u) = 1 + tu\left(F(t,u)^3 + (2F(t,u) + F(t,1))\frac{F(t,u)-F(t,1)}{u-1} + \frac{F(t,u)-F(t,1)-(u-1)\partial_u F(t,1)}{(u-1)^2}\right)$,

Output: $81t^2F(t,1)^3 - 9t(9t-2)F(t,1)^2 + (27t^2 - 66t + 1)F(t,1) - 3t^2 + 47t - 1 = 0.$

Bousquet-Mélou and Jehanne's algorithm

Input: $F(t,u) = 1 + tu\left(F(t,u)^3 + (2F(t,u) + F(t,1))\frac{F(t,u)-F(t,1)}{u-1} + \frac{F(t,u)-F(t,1)-(u-1)\partial_u F(t,1)}{(u-1)^2}\right)$,

Output: $81t^2F(t,1)^3 - 9t(9t-2)F(t,1)^2 + (27t^2 - 66t + 1)F(t,1) - 3t^2 + 47t - 1 = 0.$

- **Compute** $P \in \mathbb{Q}(t)[x, u, z_0, z_1]$ such that $P(F(t,u), u, F(t,1), \partial_u F(t,1)) = 0$,

Bousquet-Mélou and Jehanne's algorithm

Input: $F(t,u) = 1 + tu\left(F(t,u)^3 + (2F(t,u) + F(t,1))\frac{F(t,u)-F(t,1)}{u-1} + \frac{F(t,u)-F(t,1)-(u-1)\partial_u F(t,1)}{(u-1)^2}\right),$

Output: $81t^2F(t,1)^3 - 9t(9t-2)F(t,1)^2 + (27t^2 - 66t + 1)F(t,1) - 3t^2 + 47t - 1 = 0.$

- **Compute** $P \in \mathbb{Q}(t)[x, u, z_0, z_1]$ such that $P(F(t,u), u, F(t,1), \partial_u F(t,1)) = 0,$
- **Consider**

$$\partial_u F(t,u) \cdot \partial_x P(F(t,u), u, F(t,1), \partial_u F(t,1)) + \partial_u P(F(t,u), u, F(t,1), \partial_u F(t,1)) = 0,$$

Bousquet-Mélou and Jehanne's algorithm

Input: $F(t,u) = 1 + tu\left(F(t,u)^3 + (2F(t,u) + F(t,1))\frac{F(t,u)-F(t,1)}{u-1} + \frac{F(t,u)-F(t,1)-(u-1)\partial_u F(t,1)}{(u-1)^2}\right)$,

Output: $81t^2F(t,1)^3 - 9t(9t-2)F(t,1)^2 + (27t^2 - 66t + 1)F(t,1) - 3t^2 + 47t - 1 = 0.$

- **Compute** $P \in \mathbb{Q}(t)[x,u,z_0,z_1]$ such that $P(F(t,u),u,F(t,1),\partial_u F(t,1)) = 0$,
- **Consider**

$$\partial_u F(t,u) \cdot \partial_x P(F(t,u),u,F(t,1),\partial_u F(t,1)) + \partial_u P(F(t,u),u,F(t,1),\partial_u F(t,1)) = 0,$$

- **Show** that there exist distinct $U_1, U_2 \in \bigcup_{d\geq 1} \overline{\mathbb{Q}}[[t^{\frac{1}{d}}]]$ s.t. $\partial_x P(F(t,U_i),U_i,F(t,1),\partial_u F(t,1)) = 0$,

Bousquet-Mélou and Jehanne's algorithm

Input: $F(t,u) = 1 + tu\left(F(t,u)^3 + (2F(t,u) + F(t,1))\frac{F(t,u)-F(t,1)}{u-1} + \frac{F(t,u)-F(t,1)-(u-1)\partial_u F(t,1)}{(u-1)^2}\right)$,

Output: $81t^2 F(t,1)^3 - 9t(9t-2)F(t,1)^2 + (27t^2 - 66t + 1)F(t,1) - 3t^2 + 47t - 1 = 0.$

- **Compute** $P \in \mathbb{Q}(t)[x, u, z_0, z_1]$ such that $P(F(t,u), u, F(t,1), \partial_u F(t,1)) = 0$,
- **Consider**

$$\partial_u F(t,u) \cdot \partial_x P(F(t,u), u, F(t,1), \partial_u F(t,1)) + \partial_u P(F(t,u), u, F(t,1), \partial_u F(t,1)) = 0,$$

- **Show** that there exist distinct $U_1, U_2 \in \bigcup_{d \geq 1} \overline{\mathbb{Q}}[[t^{\frac{1}{d}}]]$ s.t. $\partial_x P(F(t,U_i), U_i, F(t,1), \partial_u F(t,1)) = 0$,
- **Set up**

$$\text{For } 1 \leq i \leq 2, \begin{cases} P(F(t,U_i), U_i, F(t,1), \partial_u F(t,1)) = 0, \\ \partial_x P(F(t,U_i), U_i, F(t,1), \partial_u F(t,1)) = 0, \\ \partial_u P(F(t,U_i), U_i, F(t,1), \partial_u F(t,1)) = 0, \\ m \cdot (U_1 - U_2) - 1 = 0. \end{cases}$$

Bousquet-Mélou and Jehanne's algorithm

Input: $F(t,u) = 1 + tu\left(F(t,u)^3 + (2F(t,u) + F(t,1))\frac{F(t,u)-F(t,1)}{u-1} + \frac{F(t,u)-F(t,1)-(u-1)\partial_u F(t,1)}{(u-1)^2}\right)$,

Output: $81t^2F(t,1)^3 - 9t(9t-2)F(t,1)^2 + (27t^2 - 66t + 1)F(t,1) - 3t^2 + 47t - 1 = 0.$

- **Compute** $P \in \mathbb{Q}(t)[x, u, z_0, z_1]$ such that $P(F(t,u), u, F(t,1), \partial_u F(t,1)) = 0$,
- **Consider**

$$\partial_u F(t,u) \cdot \partial_x P(F(t,u), u, F(t,1), \partial_u F(t,1)) + \partial_u P(F(t,u), u, F(t,1), \partial_u F(t,1)) = 0,$$

- **Show** that there exist distinct $U_1, U_2 \in \bigcup_{d \geq 1} \overline{\mathbb{Q}}[[t^{\frac{1}{d}}]]$ s.t. $\partial_x P(F(t,U_i), U_i, F(t,1), \partial_u F(t,1)) = 0$,
- **Set up**

For $1 \leq i \leq 2$, $\begin{cases} P(F(t,U_i), U_i, F(t,1), \partial_u F(t,1)) = 0, \\ \partial_x P(F(t,U_i), U_i, F(t,1), \partial_u F(t,1)) = 0, \\ \partial_u P(F(t,U_i), U_i, F(t,1), \partial_u F(t,1)) = 0, \\ m \cdot (U_1 - U_2) - 1 = 0. \end{cases}$

Elimination theory

- Eliminate all series but $F(t,1)$

Bousquet-Mélou and Jehanne's algorithm

Input: $F(t,u) = 1 + tu\left(F(t,u)^3 + (2F(t,u) + F(t,1))\frac{F(t,u)-F(t,1)}{u-1} + \frac{F(t,u)-F(t,1)-(u-1)\partial_u F(t,1)}{(u-1)^2}\right)$,

Output: $81t^2F(t,1)^3 - 9t(9t-2)F(t,1)^2 + (27t^2-66t+1)F(t,1) - 3t^2 + 47t - 1 = 0.$

- **Compute** $P \in \mathbb{Q}(t)[x,u,z_0,z_1]$ such that $P(F(t,u),u,F(t,1),\partial_u F(t,1)) = 0$,
- **Consider**

$$\partial_u F(t,u) \cdot \partial_x P(F(t,u),u,F(t,1),\partial_u F(t,1)) + \partial_u P(F(t,u),u,F(t,1),\partial_u F(t,1)) = 0,$$

- **Show** that there exist distinct $U_1, U_2 \in \bigcup_{d\geq 1} \overline{\mathbb{Q}}[[t^{\frac{1}{d}}]]$ s.t. $\partial_x P(F(t,U_i),U_i,F(t,1),\partial_u F(t,1)) = 0$,
- **Set up**

For $1 \leq i \leq 2$, $\begin{cases} P(F(t,U_i),U_i,F(t,1),\partial_u F(t,1)) = 0, \\ \partial_x P(F(t,U_i),U_i,F(t,1),\partial_u F(t,1)) = 0, \\ \partial_u P(F(t,U_i),U_i,F(t,1),\partial_u F(t,1)) = 0, \\ m\cdot(U_1-U_2) - 1 = 0. \end{cases}$

Elimination theory

- Eliminate all series but $F(t,1)$

$\rightarrow$ **Resultants**

Bousquet-Mélou and Jehanne's algorithm

Input: $F(t,u) = 1 + tu\left(F(t,u)^3 + (2F(t,u) + F(t,1))\frac{F(t,u)-F(t,1)}{u-1} + \frac{F(t,u)-F(t,1)-(u-1)\partial_u F(t,1)}{(u-1)^2}\right)$,

Output: $81t^2F(t,1)^3 - 9t(9t-2)F(t,1)^2 + (27t^2 - 66t + 1)F(t,1) - 3t^2 + 47t - 1 = 0.$

- **Compute** $P \in \mathbb{Q}(t)[x, u, z_0, z_1]$ such that $P(F(t,u), u, F(t,1), \partial_u F(t,1)) = 0$,
- **Consider**

$$\partial_u F(t,u) \cdot \partial_x P(F(t,u), u, F(t,1), \partial_u F(t,1)) + \partial_u P(F(t,u), u, F(t,1), \partial_u F(t,1)) = 0,$$

- **Show** that there exist distinct $U_1, U_2 \in \bigcup_{d\geq 1} \overline{\mathbb{Q}}[[t^{\frac{1}{d}}]]$ s.t. $\partial_x P(F(t,U_i), U_i, F(t,1), \partial_u F(t,1)) = 0$,
- **Set up**

For $1 \leq i \leq 2$, $\begin{cases} P(F(t,U_i), U_i, F(t,1), \partial_u F(t,1)) = 0, \\ \partial_x P(F(t,U_i), U_i, F(t,1), \partial_u F(t,1)) = 0, \\ \partial_u P(F(t,U_i), U_i, F(t,1), \partial_u F(t,1)) = 0, \\ m \cdot (U_1 - U_2) - 1 = 0. \end{cases}$

Elimination theory

- Eliminate all series but $F(t,1)$

$\rightarrow$ **Resultants**

$\rightarrow$ **Gröbner bases**

$$\mathcal{S}: \qquad \text{For } 1 \leq i \leq 2, \begin{cases} P(F(t,U_i), F(t,1), \partial_u F(t,1), t, U_i) = 0, \\ \partial_x P(F(t,U_i), F(t,1), \partial_u F(t,1), t, U_i) = 0, \\ \partial_u P(F(t,U_i), F(t,1), \partial_u F(t,1), t, U_i) = 0, \end{cases} \qquad U_1 - U_2 \neq 0.$$

$$\mathcal{S}: \qquad \text{For } 1 \le i \le 2, \begin{cases} P(F(t,U_i), F(t,1), \partial_u F(t,1), t, U_i) = 0, \\ \partial_x P(F(t,U_i), F(t,1), \partial_u F(t,1), t, U_i) = 0, \\ \partial_u P(F(t,U_i), F(t,1), \partial_u F(t,1), t, U_i) = 0, \end{cases} \qquad U_1 - U_2 \neq 0.$$

Assumptions

- U_1, U_2 are **distinct series**,
- $\mathcal{S}$ has **finitely many solutions** in $\overline{\mathbb{Q}(t)}^6$,
- $\mathcal{S}$ *generates* a **radical ideal** over $\mathbb{Q}(t)$.

$$\mathcal{S}: \qquad \text{For } 1 \leq i \leq 2, \begin{cases} P(F(t,U_i), F(t,1), \partial_u F(t,1), t, U_i) = 0, \\ \partial_x P(F(t,U_i), F(t,1), \partial_u F(t,1), t, U_i) = 0, \\ \partial_u P(F(t,U_i), F(t,1), \partial_u F(t,1), t, U_i) = 0, \end{cases} \qquad U_1 - U_2 \neq 0.$$

Assumptions

- U_1, U_2 are **distinct series**,
- $\mathcal{S}$ has **finitely many solutions** in $\overline{\mathbb{Q}(t)}^6$,
- $\mathcal{S}$ *generates* a **radical ideal** over $\mathbb{Q}(t)$.

Useful properties

- $\mathfrak{S}_2$ acts on $V(\mathcal{S})$ by **permuting** U_1, U_2,
- $\#V(\mathcal{S}) \leq$ **Bézout bound** associated with $\mathcal{S}$,
- Allows to forget $U_1 - U_2 \neq 0$ in the Bézout bound.

Quantitative estimates with A. Bostan and M. Safey El Din

$$\mathcal{S}: \qquad \text{For } 1 \le i \le 2, \begin{cases} P(F(t,U_i), F(t,1), \partial_u F(t,1), t, U_i) = 0, \\ \partial_x P(F(t,U_i), F(t,1), \partial_u F(t,1), t, U_i) = 0, \\ \partial_u P(F(t,U_i), F(t,1), \partial_u F(t,1), t, U_i) = 0, \end{cases} \qquad U_1 - U_2 \neq 0.$$

Assumptions

- U_1, U_2 are **distinct series**,
- $\mathcal{S}$ has **finitely many solutions** in $\overline{\mathbb{Q}(t)}^6$,
- $\mathcal{S}$ *generates* a **radical ideal** over $\mathbb{Q}(t)$.

Useful properties

- $\mathfrak{S}_2$ acts on $V(\mathcal{S})$ by **permuting** U_1, U_2,
- $\#V(\mathcal{S}) \le$ **Bézout bound** associated with $\mathcal{S}$,
- Allows to forget $U_1 - U_2 \neq 0$ in the Bézout bound.

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

Under the above assumptions: $\qquad \delta := \deg(P)$

- There exists some nonzero polynomial $R \in \mathbb{Q}[z_0, t]$ whose partial degrees are upper bounded by $\delta^2(\delta-1)^4/2$, such that $R(F(t,1), t) = 0$.
- There exists an algorithm computing this R in $O_{\log}(\delta^{17})$ ops. in $\mathbb{Q}$.

(We proved a **general version** of this result)

Some preliminaries on Gröbner bases

$\mathcal{A} := \mathbb{Q}[x, \boldsymbol{y}]$ polynomial ring, where $\boldsymbol{y} = y_1, \ldots, y_s$.

Monomial orders

- $x^4 y_1^3 y_2^2 \succ_{lex} x^3 y_1^4 y_2^2$ for a **lexicographic order**,
- $x^4 y_1^2 y_2^3 \succ_{bmon} x^4 y_1^3 y_2$ for a **block monomial order**.

Some preliminaries on Gröbner bases

$\mathcal{A} := \mathbb{Q}[x, \boldsymbol{y}]$ polynomial ring, where $\boldsymbol{y} = y_1, \ldots, y_s$.

Monomial orders

- $x^4 y_1^3 y_2^2 \succ_{lex} x^3 y_1^4 y_2^2$ for a **lexicographic order**,
- $x^4 y_1^2 y_2^3 \succ_{bmon} x^4 y_1^3 y_2$ for a **block monomial order**.

Leading terms for some order $\succ$

For $Q \in \mathcal{A}$, the leading term $\mathrm{LT}_{\succ}(Q)$ of Q is the monomial of **highest weight** for $\succ$.

Some preliminaries on Gröbner bases

$\mathcal{A} := \mathbb{Q}[x, \boldsymbol{y}]$ polynomial ring, where $\boldsymbol{y} = y_1, \ldots, y_s$.

Monomial orders

- $x^4 y_1^3 y_2^2 \succ_{lex} x^3 y_1^4 y_2^2$ for a **lexicographic order**,
- $x^4 y_1^2 y_2^3 \succ_{bmon} x^4 y_1^3 y_2$ for a **block monomial order**.

Leading terms for some order $\succ$

For $Q \in \mathcal{A}$, the leading term $\mathrm{LT}_{\succ}(Q)$ of Q is the monomial of **highest weight** for $\succ$.

Definition

Fix a monomial order $\succ$ on $\mathcal{A}$. A finite subset $G = \{g_1, \ldots, g_t\}$ of an ideal $\mathcal{I} \subset \mathcal{A}$ different from 0 is said to be a **Gröbner basis** if $\langle \mathrm{LT}_{\succ}(g_1), \ldots, \mathrm{LT}_{\succ}(g_t) \rangle = \langle \mathrm{LT}_{\succ}(\mathcal{I}) \rangle$.

Some preliminaries on Gröbner bases

$\mathcal{A} := \mathbb{Q}[x, \boldsymbol{y}]$ polynomial ring, where $\boldsymbol{y} = y_1, \ldots, y_s$.

Monomial orders

- $x^4 y_1^3 y_2^2 \succ_{lex} x^3 y_1^4 y_2^2$ for a **lexicographic order**,
- $x^4 y_1^2 y_2^3 \succ_{bmon} x^4 y_1^3 y_2$ for a **block monomial order**.

Leading terms for some order $\succ$

For $Q \in \mathcal{A}$, the leading term $\mathrm{LT}_{\succ}(Q)$ of Q is the monomial of **highest weight** for $\succ$.

Definition

Fix a monomial order $\succ$ on $\mathcal{A}$. A finite subset $G = \{g_1, \ldots, g_t\}$ of an ideal $\mathcal{I} \subset \mathcal{A}$ different from 0 is said to be a **Gröbner basis** if $\langle \mathrm{LT}_{\succ}(g_1), \ldots, \mathrm{LT}_{\succ}(g_t) \rangle = \langle \mathrm{LT}_{\succ}(\mathcal{I}) \rangle$.

Properties

- Such bases always **exist** and **generate** $\mathcal{I}$,
- Computing Gröbner bases is **NP-hard**,
- Gröbner bases are a **powerful tool** in elimination theory.

New geometric modelling of the problem with A. Bostan and M. Safey El Din

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

$$\begin{cases} \mathbf{P}(\mathbf{x}, \mathbf{u}, \mathbf{F}(\mathbf{t}, \mathbf{0}), \partial_{\mathbf{u}}\mathbf{F}(\mathbf{t}, \mathbf{0})) = \mathbf{0}, \\ \partial_{\mathbf{x}}\mathbf{P}(\mathbf{x}, \mathbf{u}, \mathbf{F}(\mathbf{t}, \mathbf{0}), \partial_{\mathbf{u}}\mathbf{F}(\mathbf{t}, \mathbf{0})) = \mathbf{0}, \quad \mathbf{u} \neq \mathbf{0}, \\ \partial_{\mathbf{u}}\mathbf{P}(\mathbf{x}, \mathbf{u}, \mathbf{F}(\mathbf{t}, \mathbf{0}), \partial_{\mathbf{u}}\mathbf{F}(\mathbf{t}, \mathbf{0})) = \mathbf{0}. \end{cases}$$

New geometric modelling of the problem with A. Bostan and M. Safey El Din

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

$$\begin{cases} \mathbf{P}(\mathbf{x}, \mathbf{u}, \mathbf{F}(\mathbf{t}, \mathbf{0}), \partial_{\mathbf{u}}\mathbf{F}(\mathbf{t}, \mathbf{0})) = \mathbf{0}, \\ \partial_{\mathbf{x}}\mathbf{P}(\mathbf{x}, \mathbf{u}, \mathbf{F}(\mathbf{t}, \mathbf{0}), \partial_{\mathbf{u}}\mathbf{F}(\mathbf{t}, \mathbf{0})) = \mathbf{0}, \quad \mathbf{u} \neq \mathbf{0}, \\ \partial_{\mathbf{u}}\mathbf{P}(\mathbf{x}, \mathbf{u}, \mathbf{F}(\mathbf{t}, \mathbf{0}), \partial_{\mathbf{u}}\mathbf{F}(\mathbf{t}, \mathbf{0})) = \mathbf{0}. \end{cases}$$

$$\pi_x : (x, \mathbf{u}, z_0, z_1) \in \overline{\mathbb{Q}(t)}^4 \mapsto (\mathbf{u}, z_0, z_1) \in \overline{\mathbb{Q}(t)}^3,$$

$$\mathbf{W} := \pi_x(V(\mathbf{P}, \partial_{\mathbf{x}}\mathbf{P}, \partial_{\mathbf{u}}\mathbf{P}) \setminus V(\mathbf{u}))$$

$$\pi_u : (\mathbf{u}, z_0, z_1) \in \overline{\mathbb{Q}(t)}^3 \mapsto (z_0, z_1) \in \overline{\mathbb{Q}(t)}^2,$$

New geometric modelling of the problem with A. Bostan and M. Safey El Din

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

$$\begin{cases} \mathbf{P}(\mathbf{x}, \mathbf{u}, \mathbf{F}(\mathbf{t}, \mathbf{0}), \partial_{\mathbf{u}}\mathbf{F}(\mathbf{t}, \mathbf{0})) = \mathbf{0}, \\ \partial_{\mathbf{x}}\mathbf{P}(\mathbf{x}, \mathbf{u}, \mathbf{F}(\mathbf{t}, \mathbf{0}), \partial_{\mathbf{u}}\mathbf{F}(\mathbf{t}, \mathbf{0})) = \mathbf{0}, \quad \mathbf{u} \neq \mathbf{0}, \\ \partial_{\mathbf{u}}\mathbf{P}(\mathbf{x}, \mathbf{u}, \mathbf{F}(\mathbf{t}, \mathbf{0}), \partial_{\mathbf{u}}\mathbf{F}(\mathbf{t}, \mathbf{0})) = \mathbf{0}. \end{cases}$$

$$\pi_x : (x, \mathbf{u}, z_0, z_1) \in \overline{\mathbb{Q}(t)}^4 \mapsto (\mathbf{u}, z_0, z_1) \in \overline{\mathbb{Q}(t)}^3,$$

$$\mathbf{W} := \pi_x(V(\mathbf{P}, \partial_{\mathbf{x}}\mathbf{P}, \partial_{\mathbf{u}}\mathbf{P}) \setminus V(\mathbf{u}))$$

$$\pi_u : (\mathbf{u}, z_0, z_1) \in \overline{\mathbb{Q}(t)}^3 \mapsto (z_0, z_1) \in \overline{\mathbb{Q}(t)}^2,$$

Characterize with polynomial constraints

$$\mathcal{F}_2 := \{\alpha_{\underline{z}} \in \overline{\mathbb{Q}(t)}^2 \mid \# \, \pi_u^{-1}(\alpha_{\underline{z}}) \cap \mathbf{W} \geq 2\}$$

New geometric modelling of the problem with A. Bostan and M. Safey El Din

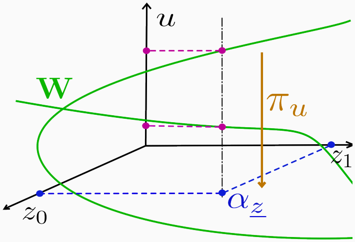
There exist 2 solutions $(x, \mathbf{u}) \in \overline{\mathbb{Q}(t)}^2$ with **distinct** $\mathbf{u}$-coordinates to

$$\begin{cases} \mathbf{P}(\mathbf{x}, \mathbf{u}, \mathbf{F}(\mathbf{t}, \mathbf{0}), \partial_{\mathbf{u}}\mathbf{F}(\mathbf{t}, \mathbf{0})) = \mathbf{0}, \\ \partial_{\mathbf{x}}\mathbf{P}(\mathbf{x}, \mathbf{u}, \mathbf{F}(\mathbf{t}, \mathbf{0}), \partial_{\mathbf{u}}\mathbf{F}(\mathbf{t}, \mathbf{0})) = \mathbf{0}, \quad \mathbf{u} \neq \mathbf{0}, \\ \partial_{\mathbf{u}}\mathbf{P}(\mathbf{x}, \mathbf{u}, \mathbf{F}(\mathbf{t}, \mathbf{0}), \partial_{\mathbf{u}}\mathbf{F}(\mathbf{t}, \mathbf{0})) = \mathbf{0}. \end{cases}$$

$\pi_x : (x, \mathbf{u}, z_0, z_1) \in \overline{\mathbb{Q}(t)}^4 \mapsto (\mathbf{u}, z_0, z_1) \in \overline{\mathbb{Q}(t)}^3,$

$\mathbf{W} := \pi_x(V(\mathbf{P}, \partial_{\mathbf{x}}\mathbf{P}, \partial_{\mathbf{u}}\mathbf{P}) \setminus V(\mathbf{u}))$

$\pi_u : (\mathbf{u}, z_0, z_1) \in \overline{\mathbb{Q}(t)}^3 \mapsto (z_0, z_1) \in \overline{\mathbb{Q}(t)}^2,$



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

Characterize with polynomial constraints

$\mathcal{F}_2 := \{\alpha_{\underline{z}} \in \overline{\mathbb{Q}(t)}^2 \mid \# \, \pi_u^{-1}(\alpha_{\underline{z}}) \cap \mathbf{W} \geq 2\}$

Input: $F(t,u) = 1 + t\left(uF(t,u) + \frac{F(t,u) - F(t,0) - u\partial_u F(t,0)}{u^2}\right)$, **k = 2**

Output: $t^3F(t,0)^3 - F(t,0) + 1 = 0.$

Input: $F(t,u) = 1 + t\left(uF(t,u) + \frac{F(t,u) - F(t,0) - u\partial_u F(t,0)}{u^2}\right)$, **k = 2**

Output: $t^3 F(t,0)^3 - F(t,0) + 1 = 0.$

- **Compute** $P \in \mathbb{Q}(t)[x, u, z_0, z_1]$ such that $P(F(t,u), u, F(t,0), \partial_u F(t,0)) = 0$,

Solving a toy example... with A. Bostan and M. Safey El Din

Input: $F(t,u) = 1 + t\left(uF(t,u) + \frac{F(t,u) - F(t,0) - u\partial_u F(t,0)}{u^2}\right)$, **k = 2**

Output: $t^3 F(t,0)^3 - F(t,0) + 1 = 0.$

- **Compute** $P \in \mathbb{Q}(t)[x,u,z_0,z_1]$ such that $P(F(t,u),u,F(t,0),\partial_u F(t,0)) = 0$,
- **Compute** G_u Gröbner basis of $\langle P, \partial_1 P, \partial_2 P, m\cdot u - 1\rangle \cap \mathbb{Q}(t)[u,z_0,z_1]$ for $\{u\} \succ_{lex} \{z_0,z_1\}$:

Input: $F(t,u) = 1 + t\left(uF(t,u) + \frac{F(t,u) - F(t,0) - u\partial_u F(t,0)}{u^2}\right),$ $\mathbf{k} = \mathbf{2}$

Output: $t^3 F(t,0)^3 - F(t,0) + 1 = 0.$

- **Compute** $P \in \mathbb{Q}(t)[x, u, z_0, z_1]$ such that $P(F(t,u), u, F(t,0), \partial_u F(t,0)) = 0,$
- **Compute** G_u Gröbner basis of $\langle P, \partial_1 P, \partial_2 P, m \cdot u - 1\rangle \cap \mathbb{Q}(t)[u, z_0, z_1]$ for $\{u\} \succ_{lex} \{z_0, z_1\}$:

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

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

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

"At $\boldsymbol{\alpha} \in \pi_u(V(G_u)) \subset \overline{\mathbb{Q}(t)}^2$, there exist two distinct solutions in u"

Solving a toy example... with A. Bostan and M. Safey El Din

Input: $F(t,u) = 1 + t\left(uF(t,u) + \frac{F(t,u) - F(t,0) - u\partial_u F(t,0)}{u^2}\right)$, **k = 2**

Output: $t^3 F(t,0)^3 - F(t,0) + 1 = 0.$

- **Compute** $P \in \mathbb{Q}(t)[x, u, z_0, z_1]$ such that $P(F(t,u), u, F(t,0), \partial_u F(t,0)) = 0$,
- **Compute** G_u Gröbner basis of $\langle P, \partial_1 P, \partial_2 P, m \cdot u - 1\rangle \cap \mathbb{Q}(t)[u, z_0, z_1]$ for $\{u\} \succ_{lex} \{z_0, z_1\}$:

$\mathbf{B_0}$: γ_0

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

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

"At $\alpha \in \pi_u(V(G_u)) \subset \overline{\mathbb{Q}(t)}^2$, there exist two distinct solutions in u"

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

Solving a toy example... with A. Bostan and M. Safey El Din

Input: $F(t,u) = 1 + t\left(uF(t,u) + \frac{F(t,u)-F(t,0)-u\partial_u F(t,0)}{u^2}\right)$, **k = 2**

Output: $t^3 F(t,0)^3 - F(t,0) + 1 = 0$.

- **Compute** $P \in \mathbb{Q}(t)[x,u,z_0,z_1]$ such that $P(F(t,u),u,F(t,0),\partial_u F(t,0)) = 0$,
- **Compute** G_u Gröbner basis of $\langle P, \partial_1 P, \partial_2 P, m \cdot u - 1\rangle \cap \mathbb{Q}(t)[u,z_0,z_1]$ for $\{u\} \succ_{lex} \{z_0,z_1\}$:

$\mathbf{B_0}$: γ_0

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

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

"At $\alpha \in \pi_u(V(G_u)) \subset \overline{\mathbb{Q}(t)}^2$, there exist two distinct solutions in u"

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

[Extension theorem]

$\alpha \in \pi_u(V(G_u)) \implies \mathrm{LeadingCoeff}_u(\mathbf{g_2}) \neq 0$

Distinct solutions in $u \implies \mathrm{disc}_u(\mathbf{g_2}) \neq 0$ (**inequations**)

… yields an algorithm based on elimination theory (ISSAC'23)

Projecting $\Longrightarrow$ Elimination theorem

Lifting points of the projections $\Longrightarrow$ Extension theorem

... yields an algorithm based on elimination theory (ISSAC'23)

Projecting $\Longrightarrow$ Elimination theorem

Lifting points of the projections $\Longrightarrow$ Extension theorem

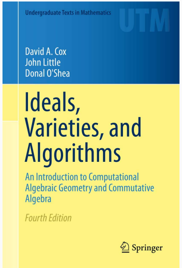
[Proposition] Let $g \in (\mathbb{Q}(t)[z_0, z_1])[u]$. Then g has **at least i distinct solutions** at $\alpha \in \overline{\mathbb{Q}(t)}^2$ **if and only if** the $(i \times i)$-minors of the **Hermite quadratic form** associated with g **do not vanish simultaneously** at α.

$\rightsquigarrow$ Reduces to studying the **multiplication maps** $(M_{u^\ell} : q \mapsto q \cdot u^\ell)_{\ell \geq 1}$ in $(\mathbb{Q}[t, z_0, z_1])[u]/\langle g \rangle$

… yields an algorithm based on elimination theory (ISSAC'23)

Projecting $\Longrightarrow$ Elimination theorem

Lifting points of the projections $\Longrightarrow$ Extension theorem



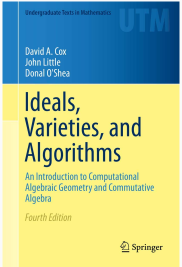
[Proposition] Let $g \in (\mathbb{Q}(t)[z_0, z_1])[u]$. Then g has **at least i distinct solutions** at $\alpha \in \overline{\mathbb{Q}(t)}^2$ **if and only if** the $(i \times i)$-minors of the **Hermite quadratic form** associated with g **do not vanish simultaneously** at α.

$\rightsquigarrow$ Reduces to studying the **multiplication maps** $(M_{u^\ell} : q \mapsto q \cdot u^\ell)_{\ell \geq 1}$ in $(\mathbb{Q}[t, z_0, z_1])[u]/\langle g \rangle$

… yields an algorithm based on elimination theory (ISSAC'23)

Projecting $\Longrightarrow$ Elimination theorem

Lifting points of the projections $\Longrightarrow$ Extension theorem



[Proposition] Let $g \in (\mathbb{Q}(t)[z_0, z_1])[u]$. Then g has **at least** i **distinct solutions** at $\alpha \in \overline{\mathbb{Q}(t)}^2$ **if and only if** the $(i \times i)$-minors of the **Hermite quadratic form** associated with g **do not vanish simultaneously** at α.

$\rightsquigarrow$ Reduces to studying the **multiplication maps** $(M_{u^\ell} : q \mapsto q \cdot u^\ell)_{\ell \geq 1}$ in $(\mathbb{Q}[t, z_0, z_1])[u]/\langle g \rangle$

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

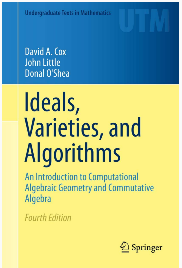
Disjunction of conjunctions of polynomial equations and inequations whose zero set is $\mathcal{F}_2$

(Our strategy works in the **general case**)

… yields an algorithm based on elimination theory (ISSAC'23)

Projecting $\Longrightarrow$ Elimination theorem

Lifting points of the projections $\Longrightarrow$ Extension theorem



[Proposition] Let $g \in (\mathbb{Q}(t)[z_0, z_1])[u]$. Then g has **at least** i **distinct solutions** at $\alpha \in \overline{\mathbb{Q}(t)}^2$ **if and only if** the $(i \times i)$-minors of the **Hermite quadratic form** associated with g **do not vanish simultaneously** at α.

$\rightsquigarrow$ Reduces to studying the **multiplication maps** $(M_{u^\ell} : q \mapsto q \cdot u^\ell)_{\ell \geq 1}$ in $(\mathbb{Q}[t, z_0, z_1])[u]/\langle g \rangle$

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

Disjunction of conjunctions of polynomial equations and inequations whose zero set is $\mathcal{F}_2$

(Our strategy works in the **general case**)

[5—constellations $k = 4$]

Strategy	Timing	(d_{z_0}, d_t)
Duplication	> 5d	?
Elimination	**2d21h**	$(9, 3)$

Conclusion and perspectives

- **Decidability**: **geometry-driven algorithm** computing $R \in \mathbb{Q}[z,t] \setminus \{0\}$ s.t. $R(F(t,1),t) = 0$,
- **Resolution** of the DDE of 5-constellations in an **automatic fashion**,

Conclusion and perspectives

- **Decidability**: **geometry-driven algorithm** computing $R \in \mathbb{Q}[z,t] \setminus \{0\}$ s.t. $R(F(t,1),t) = 0$,
- **Resolution** of the DDE of 5-constellations in an **automatic fashion**,

- **Implementing** the algorithm in a *Maple* package?
  Available in 3 weeks!
- Work in progress with S. Yurkevich for systems of DDEs.
- More **nested** catalytic variables?
  (Work in progress with M. Bousquet-Mélou)