Solving combinatorial equations via computer algebra

Combinatorics and Arithmetic for Physics, 15-17 November 2023

Hadrien Notarantonio (Inria Saclay – Sorbonne Université)

Based on joint works with:

Alin Bostan (Inria Saclay)

Mohab Safey El Din (Sorbonne Université)

Sergey Yurkevich (University of Vienna)





Which type of equations are we looking at?

rooted planar maps



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

Which type of equations are we looking at?

rooted planar maps



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

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

Which type of equations are we looking at?

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

fixed-point in $F \rightsquigarrow$ unique solution in $\mathbb{Q}[u][[t]]$

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

$$\begin{cases} F(t, u) = x - y + G(t, u) + tu \left(uF(t, u)^2 + \frac{uF(t, u) - F(t, 1)}{u - 1} \right) \\ G(t, u) = y + tsu \left(F(t, u)G(t, u) + \frac{G(t, u) - G(t, 1)}{u - 1} \right) \end{cases}$$

rooted planar maps



$$F(t,u)=1+tuigg(uF(t,u)^2+rac{uF(t,u)-F(t,1)}{u-1}igg)$$

[Tutte '68]

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]

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

↓ refinement

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

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

generating function

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

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]

generating function

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

↓ refinement

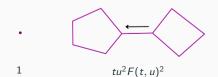
 $a_{n,d}:=\#\{ ext{planar maps with } n ext{ edges,}$

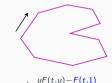
d of them on the external face}

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

↓ refinement

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





rooted planar maps



$$F(t,u)=1+tuigg(uF(t,u)^2+rac{uF(t,u)-F(t,1)}{u-1}igg)$$

[Tutte '68]

generating function

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

 \downarrow refinement

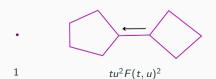
 $a_{n,d} := \#\{ ext{planar maps with } n ext{ edges,}$ $d ext{ of them on the external face} \}$

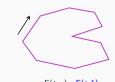
 $\sum_{n=0}^{\infty} a_n t^n$

. .

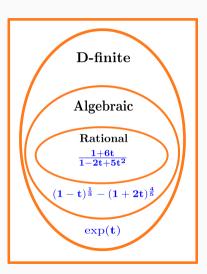
 \downarrow refinement

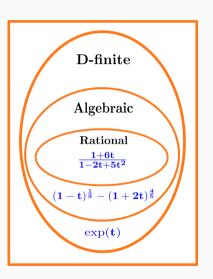
 $F(t, u) := \sum_{n=0}^{\infty} \sum_{d=0}^{n} a_{n,d} u^{d} t^{n}$ complete generating function





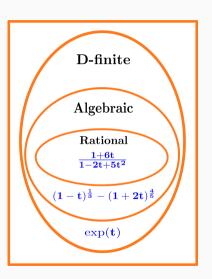
 $F(t,1) = \sum_{n=0}^{\infty} a_n t^n$





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)



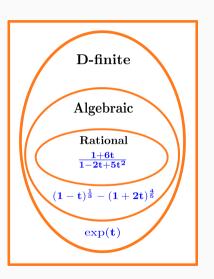
In this talk

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...

$$\begin{split} F(t,1) &= 1 + 2t + 9t^2 + 54t^3 + 378t^4 + \cdots \\ &= \mathbb{Q}[[t]] \\ &\text{annihilated by } R = 27t^2z^2 + (1-18t)z + 16t - 1 \in \mathbb{Q}[z,t] \end{split}$$



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

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 → Solving a problem previously out of reach.

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 → Solving a problem previously out of reach.

Plan

I Perform the above points for DDEs

[Bostan, N., Safey El Din $^\prime$ 23]

II Perform the above points for systems of DDEs

[N., Yurkevich '23]

Objects of interest: Discrete Differential Equations

Definition

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

$$F = f + t \cdot Q(F, \Delta F, \dots, \Delta^k F, t, u)$$
 (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 $\ell > 1$ 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 $Q \in \mathbb{Q}[y_0, \dots, y_k, t, u]$,

$$F = f + t \cdot Q(F, \Delta F, \dots, \Delta^k F, t, u)$$
 (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 $\Delta^{\ell+1} = \Delta^{\ell} \circ \Delta$.

Going back to our 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 $Q \in \mathbb{Q}[y_0, \dots, y_k, t, u]$,

$$F = f + t \cdot Q(F, \Delta F, \dots, \Delta^k F, t, u)$$
 (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 $\ell > 1$ we define $\Delta^{\ell+1} = \Delta^{\ell} \circ \Delta$.

Going back to our 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 $\mathbb{Q}(t, u)$.

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

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

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

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

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. $\partial_x P(F(t, U_i), U_i, F(t, 1), \partial_u F(t, 1)) = 0$,

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

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

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

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

Elimination theory

• Eliminate all series but F(t, 1)

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

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

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

Elimination theory

- Eliminate all series but F(t,1)
- \rightarrow Resultants

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
$$1 \le i \le 2$$
,
$$\begin{cases} P(F(t, U_i), U_i, F(t, 1), \partial_u F(t, 1)) = 0, \\ \frac{\partial_x P(F(t, U_i), U_i, F(t, 1), \partial_u F(t, 1))}{\partial_u P(F(t, U_i), U_i, F(t, 1), \partial_u F(t, 1))} = 0, \\ \frac{\partial_u P(F(t, U_i), U_i, F(t, 1), \partial_u F(t, 1))}{\partial_u P(t, U_i)} = 0. \end{cases}$$

Elimination theory

- Eliminate all series but F(t, 1)
- $\rightarrow \, \text{Resultants}$
- ightarrow Gröbner bases

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

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

Assumptions

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

Useful properties

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

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

Assumptions

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

Useful properties

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

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

Under the above assumptions:

$$\delta := \deg(P)$$

- 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)

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

Monomial orders

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

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

Monomial orders

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

Leading terms for some order \succ

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

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

Monomial orders

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

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 $\langle \mathsf{LT}_{\succ}(g_1), \ldots, \mathsf{LT}_{\succ}(g_t) \rangle = \langle \mathsf{LT}_{\succ}(\mathcal{I}) \rangle$.

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

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

Monomial orders

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

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 $\langle \mathsf{LT}_{\succ}(g_1), \ldots, \mathsf{LT}_{\succ}(g_t) \rangle = \langle \mathsf{LT}_{\succ}(\mathcal{I}) \rangle$.

Leading terms for some order \succ For $Q \in \mathcal{A}$, the leading term $\mathsf{LT}_{\succ}(Q)$ of Q is the monomial of highest weight for \succ .

Properties

- Such bases always exist and generate 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

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

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 **u**-coordinates to

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

$$\begin{split} &\pi_{\scriptscriptstyle X}: (x, \mathbf{u}, z_0, z_1) \in \overline{\mathbb{Q}(t)}^4 \mapsto (\mathbf{u}, z_0, z_1) \in \overline{\mathbb{Q}(t)}^3, \\ &\mathbf{W}:= \pi_{\scriptscriptstyle X}(V(\mathbf{P}, \partial_{\scriptscriptstyle X}\mathbf{P}, \partial_{\scriptscriptstyle \mathbf{u}}\mathbf{P}) \setminus V(\mathbf{u})) \\ &\pi_{\scriptscriptstyle \mathcal{U}}: (\mathbf{u}, z_0, z_1) \in \overline{\mathbb{Q}(t)}^3 \mapsto (z_0, z_1) \in \overline{\mathbb{Q}(t)}^2, \end{split}$$

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

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

$$\pi_{x}: (x, \mathbf{u}, z_{0}, z_{1}) \in \overline{\mathbb{Q}(t)}^{4} \mapsto (\mathbf{u}, z_{0}, z_{1}) \in \overline{\mathbb{Q}(t)}^{3},$$

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

$$\pi_{u}: (\mathbf{u}, z_{0}, z_{1}) \in \overline{\mathbb{Q}(t)}^{3} \mapsto (z_{0}, z_{1}) \in \overline{\mathbb{Q}(t)}^{2},$$

Characterize with polynomial constraints

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

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

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

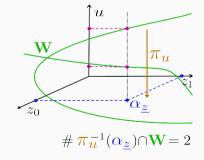
$$\pi_{\mathsf{x}}: (\mathsf{x}, \mathbf{u}, \mathsf{z}_0, \mathsf{z}_1) \in \overline{\mathbb{Q}(t)}^4 \mapsto (\mathbf{u}, \mathsf{z}_0, \mathsf{z}_1) \in \overline{\mathbb{Q}(t)}^3,$$

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

$$\pi_u: \left(\textbf{u}, \textbf{z}_0, \textbf{z}_1\right) \in \overline{\mathbb{Q}(\textbf{t})}^3 \mapsto \left(\textbf{z}_0, \textbf{z}_1\right) \in \overline{\mathbb{Q}(\textbf{t})}^2,$$

Characterize with polynomial constraints

$$\mathcal{F}_2 := \{ \underline{\alpha_z} \in \overline{\mathbb{Q}(t)}^2 | \# \pi_u^{-1}(\underline{\alpha_z}) \cap \mathbf{W} \ge 2 \}$$



Input:
$$F(t, u) = 1 + t \left(uF(t, u) + \frac{F(t, u) - F(t, 0) - u\partial_u F(t, 0)}{u^2} \right),$$
Output: $t^3 F(t, 0)^3 - F(t, 0) + 1 = 0.$

k = 2

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

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

k = 2

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

Input:
$$F(t, u) = 1 + t \left(uF(t, u) + \frac{F(t, u) - F(t, 0) - u\partial_u F(t, 0)}{u^2} \right)$$
,
Output: $t^3 F(t, 0)^3 - F(t, 0) + 1 = 0$.

- Compute $P \in \mathbb{Q}(t)[x, u, \mathbf{z}_0, z_1]$ 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:
$$F(t, u) = 1 + t \left(uF(t, u) + \frac{F(t, u) - F(t, 0) - u\partial_u F(t, 0)}{u^2} \right)$$
,
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 $\{u\} \succ_{lex} \{z_0, z_1\}$:

$$\mathsf{B}_0: \qquad \qquad \gamma_0 \\ \mathsf{B}_1: \left\{ \begin{array}{c} \beta_1 \cdot u + \gamma_1 \\ \vdots \\ \beta_r \cdot u + \gamma_r \end{array} \right. \qquad \text{``At } \alpha \in \pi_u(V(G_u)) \subset \overline{\mathbb{Q}(t)}^2, \\ \mathsf{B}_2: \quad \mathsf{g}_2:= u^2 + \beta_{r+1} \cdot u + \gamma_{r+1} \end{array} \right.$$

there exist two distinct solutions in u''

k = 2

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

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 $\{u\} \succ_{lex} \{z_0, z_1\}$:

$$egin{aligned} \mathsf{B}_0: & \gamma_0 \ & egin{aligned} eta_1 \cdot u + \gamma_1 \ & dots \ & \ddots \ & \gamma_i, eta_j \in \mathbb{Q}(t)[z_0, z_1] \end{aligned} \ & \mathsf{B}_2: & \mathsf{g}_2:= u^2 + eta_{r+1} \cdot u + \gamma_{r+1} \end{aligned}$$

"At $\alpha \in \pi_{u}(V(G_{u})) \subset \overline{\mathbb{Q}(t)}^{2}$. there exist two distinct solutions in μ''

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

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

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 $\{u\} \succ_{lex} \{z_0, z_1\}$:

$$egin{aligned} \mathsf{B}_0: & \gamma_0 \ & egin{aligned} eta_1 \cdot u + \gamma_1 \ & dots \ & \ddots \ & \gamma_i, eta_j \in \mathbb{Q}(t)[z_0, z_1] \end{aligned} \ & \mathsf{B}_2: & \mathsf{g}_2:= u^2 + eta_{r+1} \cdot u + \gamma_{r+1} \end{aligned}$$

"At $\alpha \in \pi_{u}(V(G_{u})) \subset \overline{\mathbb{Q}(t)}^{2}$. there exist two distinct solutions in μ''

k = 2

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

[Extension theorem]

 $\alpha \in \pi_u(V(G_u)) \implies \text{LeadingCoeff}_u(\mathbf{g_2}) \neq 0$ Distinct solutions in $u \implies \operatorname{disc}_{\mathbf{u}}(\mathbf{g}_2) \neq 0$ (inequations)

(**ISSAC**′23)

 $\begin{array}{ccc} \textbf{Projecting} & \implies & \textbf{Elimination theorem} \\ \textbf{Lifting points of the projections} & \implies & \textbf{Extension theorem} \end{array}$

ISSAC′23)

 $\begin{array}{ccc} \textbf{Projecting} & \Longrightarrow & \textbf{Elimination theorem} \\ \textbf{Lifting points of the projections} & \Longrightarrow & \textbf{Extension theorem} \end{array}$

[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 .

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

(ISSAC'23)

Projecting ⇒ Elimination theorem

Lifting points of the projections ⇒ 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 .

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



(**ISSAC**′23)

David A. Cox John Little Donal O'Shea

Projecting ⇒ Elimination theorem

Lifting points of the projections ⇒ 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 .

Varieties, and Algorithms
An Introduction to Computational Algebraic Geometry and Commutative Algebra.
Fourth Edition

 \leadsto 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**)

ISSAC'23)

 $\textbf{Projecting} \hspace{1cm} \Longrightarrow \hspace{1cm} \textbf{Elimination theorem}$

Lifting points of the projections \implies 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 .



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

[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)

Systems of Discrete Differential Equations

What could be extended to systems?

Systems of Discrete Differential Equations

What could be extended to systems?

Modelling special Eulerian planar orientations:

$$\begin{cases} F(t,u) = 1 + t \cdot \left(u + 2uF(t,u)^2 + 2uG(t,1) + u\frac{F(t,u) - uF(t,1)}{u-1} \right), \\ G(t,u) = t \cdot \left(2uF(t,u)G(t,u) + uF(t,u) + uG(t,1) + u\frac{G(t,u) - uG(t,1)}{u-1} \right). \end{cases}$$

[Bonichon, Bousquet-Mélou, Dorbec, Pennarun '17]

Systems of Discrete Differential Equations

What could be extended to systems?

Modelling special Eulerian planar orientations:

$$\begin{cases} F(t,u) = 1 + t \cdot \left(u + 2uF(t,u)^2 + 2uG(t,1) + u\frac{F(t,u) - uF(t,1)}{u-1} \right), \\ G(t,u) = t \cdot \left(2uF(t,u)G(t,u) + uF(t,u) + uG(t,1) + u\frac{G(t,u) - uG(t,1)}{u-1} \right). \end{cases}$$

[Bonichon, Bousquet-Mélou, Dorbec, Pennarun '17]

Modelling hard particles on planar maps:

$$\begin{cases} F(t, u) = x - y + G(t, u) + tu \left(uF(t, u)^2 + \frac{uF(t, u) - F(t, 1)}{u - 1} \right) \\ G(t, u) = y + tsu \left(F(t, u)G(t, u) + \frac{G(t, u) - G(t, 1)}{u - 1} \right) \end{cases}$$

[Bousquet-Mélou, Jehanne '06]

[Popescu '86, Swan '98]

(1.4) THEOREM. Let k be a field, $k\langle X \rangle$ the algebraic power series ring in $X = (X_1, \dots, X_r)$ over k, f a finite system of polynomial equations over $k\langle X \rangle$ and $\hat{y} = (\hat{y}_1, \dots, \hat{y}_n) \in k[\![X]\!]^n$ a formal solution of f such that $\hat{y}_i \in k[\![X]\!]$, $\dots, X_{s_i}[\!]$, $1 \leq i \leq n$ for some positive integers $s_i \leq r$. Then there exists a solution $y = (y_1, \dots, y_n)$ of f in $k\langle X \rangle$ such that $y_i \in k\langle X_1, \dots, X_{s_i} \rangle$, $1 \leq i \leq n$.

[Popescu '86, Swan '98]

(1.4) THEOREM. Let k be a field, $k\langle X \rangle$ the algebraic power series ring in $X = (X_1, \dots, X_r)$ over k, f a finite system of polynomial equations over $k\langle X \rangle$ and $\hat{y} = (\hat{y}_1, \dots, \hat{y}_n) \in k[\![X]\!]^n$ a formal solution of f such that $\hat{y}_i \in k[\![X]\!]_i$, $\dots, X_{s_i}[\!]_i$, $1 \leq i \leq n$ for some positive integers $s_i \leq r$. Then there exists a solution $y = (y_1, \dots, y_n)$ of f in $k\langle X \rangle$ such that $y_i \in k\langle X_1, \dots, X_{s_i} \rangle$, $1 \leq i \leq n$.

• Solutions of systems of DDEs are unique with components in $\mathbb{Q}[u][[t]] \implies$ they are algebraic!

[Popescu '86, Swan '98]

(1.4) THEOREM. Let k be a field, $k\langle X \rangle$ the algebraic power series ring in $X=(X_1,\cdots,X_r)$ over k, f a finite system of polynomial equations over $k\langle X \rangle$ and $\hat{y}=(\hat{y}_1,\cdots,\hat{y}_n)\in k[\![X]\!]^n$ a formal solution of f such that $\hat{y}_i\in k[\![X_1,\cdots,X_{s_i}]\!]$, $1\leqslant i\leqslant n$ for some positive integers $s_i\leqslant r$. Then there exists a solution $y=(y_1,\cdots,y_n)$ of f in $k\langle X \rangle$ such that $y_i\in k\langle X_1,\cdots,X_{s_i}\rangle$, $1\leqslant i\leqslant n$.

• Solutions of systems of DDEs are unique with components in $\mathbb{Q}[u][[t]] \implies$ they are algebraic!

[planar maps]
$$H(t,u) = 1 + t \left(u^2 H(t,u)^2 + u \frac{u H(t,u) - G(t,u)}{u-1} \right)$$

- There exists a solution (H,G)=(F,F(t,1)), where $F\in \mathbb{Q}[u][[t]]$,
- The involved series are F(t,1) and F(t,u), and $\{t\} \subset \{t,u\}$.

[Popescu '86, Swan '98]

(1.4) Theorem. Let k be a field, $k\langle X \rangle$ the algebraic power series ring in $X=(X_1,\cdots,X_r)$ over k, f a finite system of polynomial equations over $k\langle X \rangle$ and $\hat{y}=(\hat{y}_1,\cdots,\hat{y}_n)\in k[\![X]\!]^n$ a formal solution of f such that $\hat{y}_i\in k[\![X]\!],\cdots,X_{s_i}$, $1\leqslant i\leqslant n$ for some positive integers $s_i\leqslant r$. Then there exists a solution $y=(y_1,\cdots,y_n)$ of f in $k\langle X \rangle$ such that $y_i\in k\langle X_1,\cdots,X_{s_i}\rangle$, $1\leqslant i\leqslant n$.

• Solutions of systems of DDEs are unique with components in $\mathbb{Q}[u][[t]] \implies$ they are algebraic!

[planar maps]
$$H(t,u) = 1 + t \left(u^2 H(t,u)^2 + u \frac{u H(t,u) - G(t,u)}{u-1} \right)$$

- There exists a solution (H,G)=(F,F(t,1)), where $F\in \mathbb{Q}[u][[t]]$,
- ullet The involved series are F(t,1) and F(t,u), and $\{t\}\subset\{t,u\}$.

The proof is **highly not constructive**... How to compute witnesses?



Constructive algebraicity theorem for solutions of systems of DDEs (FPSAC'23)

[N., Yurkevich '23]

Let $n, k \geq 1$ be integers and $f_1, \ldots, f_n \in \mathbb{Q}[u], Q_1, \ldots, Q_n \in \mathbb{Q}[y_1, \ldots, y_{n(k+1)}, t, u]$ be polynomials. Denote $\nabla^k F := F, \Delta F, \ldots, \Delta^k F$. Then the system of DDEs

$$\begin{cases} (\mathbf{E}_{\mathbf{F}_{1}}) \colon & F_{1} = f_{1}(u) + t \cdot Q_{1}(\nabla^{k}F_{1}, \dots, \nabla^{k}F_{n}, t, u), \\ \vdots & & \vdots \\ (\mathbf{E}_{\mathbf{F}_{n}}) \colon & F_{n} = f_{n}(u) + t \cdot Q_{n}(\nabla^{k}F_{1}, \dots, \nabla^{k}F_{n}, t, u). \end{cases}$$
(SDDEs)

admits a unique vector of solutions $(F_1, \ldots, F_n) \in \mathbb{Q}[u][[t]]^n$, and all its components are algebraic over $\mathbb{Q}(t, u)$.

Constructive algebraicity theorem for solutions of systems of DDEs (FPSAC'23)

[N., Yurkevich '23]

Let $n, k \geq 1$ be integers and $f_1, \ldots, f_n \in \mathbb{Q}[u], Q_1, \ldots, Q_n \in \mathbb{Q}[y_1, \ldots, y_{n(k+1)}, t, u]$ be polynomials. Denote $\nabla^k F := F, \Delta F, \ldots, \Delta^k F$. Then the system of DDEs

$$\begin{cases} (\mathbf{E}_{\mathbf{F}_{1}}): & F_{1} = f_{1}(u) + t \cdot Q_{1}(\nabla^{k}F_{1}, \dots, \nabla^{k}F_{n}, t, u), \\ \vdots & & \vdots \\ (\mathbf{E}_{\mathbf{F}_{n}}): & F_{n} = f_{n}(u) + t \cdot Q_{n}(\nabla^{k}F_{1}, \dots, \nabla^{k}F_{n}, t, u). \end{cases}$$
(SDDEs)

admits a unique vector of solutions $(F_1, \ldots, F_n) \in \mathbb{Q}[u][[t]]^n$, and all its components are algebraic over $\mathbb{Q}(t, u)$.

[Proof sketch]

- There exists a **polynomial system** S defined over $\mathbb{Q}(t)$ in nk(n+2) equations and unknowns, that admits a solution P with $F_1(t,1)$ as one of its coordinates,
- The Jacobian of S is invertible at $\mathcal{P} \implies F_1(t,1)$ is algebraic over $\mathbb{Q}(t)$.

Identifying more polynomial equations

Consider

$$\leadsto F_1, F_2 \equiv F_1(t, u), F_2(t, u) \in \mathbb{Q}[u][[t]]$$

$$\begin{cases} 0 = (1 - F_1) \cdot (\mathbf{u} - 1) + t\mathbf{u} \cdot (2\mathbf{u}F_1^2 - \mathbf{u}F_1(t, 1) + 2\mathbf{u}F_2(t, 1) - 2F_1^2 + \mathbf{u} + F_1 - 2F_2(t, 1) - 1), \\ 0 = F_2 \cdot (1 - \mathbf{u}) + t\mathbf{u} \cdot (2\mathbf{u}F_1F_2 + \mathbf{u}F_1 - 2F_1F_2 - F_1 + F_2 - F_2(t, 1)). \end{cases}$$

Denote by $E_1, E_2 \in \mathbb{Q}(t)[x_1, x_2, \mathbf{u}, \mathbf{z}_0, \mathbf{z}_1]$ polynomials such that

for
$$i \in \{1,2\}, E_i(F_1(t,\mathbf{u}),F_2(t,\mathbf{u}),\mathbf{u},F_1(t,1),F_2(t,1)) = 0.$$
 $(\equiv E_i(\mathbf{u}))$

Identifying more polynomial equations

Consider

$$\rightsquigarrow F_1, F_2 \equiv F_1(t, u), F_2(t, u) \in \mathbb{Q}[u][[t]]$$

$$\begin{cases} 0 = (1 - F_1) \cdot (\mathbf{u} - 1) + t\mathbf{u} \cdot (2\mathbf{u}F_1^2 - \mathbf{u}F_1(t, 1) + 2\mathbf{u}F_2(t, 1) - 2F_1^2 + \mathbf{u} + F_1 - 2F_2(t, 1) - 1), \\ 0 = F_2 \cdot (1 - \mathbf{u}) + t\mathbf{u} \cdot (2\mathbf{u}F_1F_2 + \mathbf{u}F_1 - 2F_1F_2 - F_1 + F_2 - F_2(t, 1)). \end{cases}$$

Denote by $E_1, E_2 \in \mathbb{Q}(t)[x_1, x_2, \mathbf{u}, \mathbf{z_0}, \mathbf{z_1}]$ polynomials such that

for
$$i \in \{1,2\}, E_i(F_1(t,\mathbf{u}), F_2(t,\mathbf{u}), \mathbf{u}, F_1(t,1), F_2(t,1)) = 0.$$
 $(\equiv E_i(\mathbf{u}))$

Differentiating with respect to u yields

$$\begin{pmatrix} (\partial_{x_1}E_1)(u) & (\partial_{x_2}E_1)(u) \\ (\partial_{x_1}E_2)(u) & (\partial_{x_2}E_2)(u) \end{pmatrix} \cdot \begin{pmatrix} \partial_uF_1 \\ \partial_uF_2 \end{pmatrix} + \begin{pmatrix} (\partial_uE_1)(u) \\ (\partial_uE_2)(u) \end{pmatrix} = 0.$$

$$\text{For } U(t) \in \bigcup_{d \geq 1} \overline{\mathbb{Q}}[[t^{\frac{1}{d}}]], \begin{cases} \text{if} & (\partial_{x_1} E_1 \cdot \partial_{x_2} E_2 - \partial_{x_1} E_2 \cdot \partial_{x_2} E_1)(U(t)) = 0, \\ \text{then } & (\partial_{x_1} E_1 \cdot \partial_u E_2 \ - \partial_{x_1} E_2 \cdot \partial_u E_1) \ (U(t)) = 0. \end{cases}$$

Identifying more polynomial equations

Consider

$$\leadsto F_1, F_2 \equiv F_1(t, u), F_2(t, u) \in \mathbb{Q}[u][[t]]$$

$$\begin{cases} 0 = (1 - F_1) \cdot (\mathbf{u} - 1) + t\mathbf{u} \cdot (2\mathbf{u}F_1^2 - \mathbf{u}F_1(t, 1) + 2\mathbf{u}F_2(t, 1) - 2F_1^2 + \mathbf{u} + F_1 - 2F_2(t, 1) - 1), \\ 0 = F_2 \cdot (1 - \mathbf{u}) + t\mathbf{u} \cdot (2\mathbf{u}F_1F_2 + \mathbf{u}F_1 - 2F_1F_2 - F_1 + F_2 - F_2(t, 1)). \end{cases}$$

Denote by $E_1, E_2 \in \mathbb{Q}(t)[x_1, x_2, \mathbf{u}, \mathbf{z_0}, \mathbf{z_1}]$ polynomials such that

for
$$i \in \{1, 2\}, E_i(F_1(t, \mathbf{u}), F_2(t, \mathbf{u}), \mathbf{u}, F_1(t, 1), F_2(t, 1)) = 0.$$
 $(\equiv E_i(\mathbf{u}))$

Differentiating with respect to u yields

$$\begin{pmatrix} (\partial_{x_1}E_1)(u) & (\partial_{x_2}E_1)(u) \\ (\partial_{x_1}E_2)(u) & (\partial_{x_2}E_2)(u) \end{pmatrix} \cdot \begin{pmatrix} \partial_uF_1 \\ \partial_uF_2 \end{pmatrix} + \begin{pmatrix} (\partial_uE_1)(u) \\ (\partial_uE_2)(u) \end{pmatrix} = 0.$$

$$\text{For } U(t) \in \bigcup_{d \geq 1} \overline{\mathbb{Q}}[[t^{\frac{1}{d}}]], \begin{cases} \text{if} & (\partial_{x_1} E_1 \cdot \partial_{x_2} E_2 - \partial_{x_1} E_2 \cdot \partial_{x_2} E_1)(U(t)) = 0, \\ \text{then } & (\partial_{x_1} E_1 \cdot \partial_u E_2 \ - \partial_{x_1} E_2 \cdot \partial_u E_1) \ (U(t)) = 0. \end{cases}$$

Does this yield an elimination procedure?

A polynomial system for systems of 2 DDEs of order 1

$$\begin{cases} F_1 = f_1(u) + t \cdot Q_1(F_1, \Delta F_1, F_2, \Delta F_2, t, u), \\ F_2 = f_2(u) + t \cdot Q_2(F_1, \Delta F_1, F_2, \Delta F_2, t, u). \end{cases}$$
(SDDEs)

A polynomial system for systems of 2 DDEs of order 1

$$\begin{cases} F_{1} = f_{1}(u) + t \cdot Q_{1}(F_{1}, \Delta F_{1}, F_{2}, \Delta F_{2}, t, u), \\ F_{2} = f_{2}(u) + t \cdot Q_{2}(F_{1}, \Delta F_{1}, F_{2}, \Delta F_{2}, t, u). \end{cases}$$
(SDDEs)

Define the "numerators" E_1 , E_2 and the polynomials

$$\mathsf{Det} := \mathsf{det} \begin{pmatrix} \partial_{\mathsf{x}_1} E_1 & \partial_{\mathsf{x}_2} E_1 \\ \partial_{\mathsf{x}_1} E_2 & \partial_{\mathsf{x}_2} E_2 \end{pmatrix} \quad \mathsf{and} \quad P := \mathsf{det} \begin{pmatrix} \partial_{\mathsf{x}_1} E_1 & \partial_{\mathsf{u}} E_1 \\ \partial_{\mathsf{x}_1} E_2 & \partial_{\mathsf{u}} E_2 \end{pmatrix}.$$

Set up the duplicated polynomial system S, consisting in the 2 duplications of the polynomials $(E_1, E_2, \text{Det}, P)$: it has 8 equations and unknowns.

Moreover, one of its solutions in $\overline{\mathbb{Q}(t)}^8$ is

$$\mathcal{P} := (F_1(t, U_1), F_2(t, U_1), F_1(t, U_2), F_2(t, U_2), U_1, U_2, F_1(t, 1), F_2(t, 1)).$$

Compute an element of $\langle \mathcal{S}, m \cdot (U_1 - U_2) - 1 \rangle \cap \mathbb{Q}[z_0, t]$.

A polynomial system for systems of 2 DDEs of order 1

$$\begin{cases} F_{1} = f_{1}(u) + t \cdot Q_{1}(F_{1}, \Delta F_{1}, F_{2}, \Delta F_{2}, t, u), \\ F_{2} = f_{2}(u) + t \cdot Q_{2}(F_{1}, \Delta F_{1}, F_{2}, \Delta F_{2}, t, u). \end{cases}$$
(SDDEs)

Define the "numerators" E_1, E_2 and the polynomials

$$\mathsf{Det} := \mathsf{det} \begin{pmatrix} \partial_{\mathsf{x}_1} \mathsf{E}_1 & \partial_{\mathsf{x}_2} \mathsf{E}_1 \\ \partial_{\mathsf{x}_1} \mathsf{E}_2 & \partial_{\mathsf{x}_2} \mathsf{E}_2 \end{pmatrix} \quad \mathsf{and} \quad P := \mathsf{det} \begin{pmatrix} \partial_{\mathsf{x}_1} \mathsf{E}_1 & \partial_{\mathsf{u}} \mathsf{E}_1 \\ \partial_{\mathsf{x}_1} \mathsf{E}_2 & \partial_{\mathsf{u}} \mathsf{E}_2 \end{pmatrix}.$$

Set up the duplicated polynomial system S, consisting in the 2 duplications of the polynomials (E_1, E_2, Det, P) : it has 8 equations and unknowns.

Moreover, one of its solutions in $\overline{\mathbb{Q}(t)}^8$ is

$$\mathcal{P} := (F_1(t, U_1), F_2(t, U_1), F_1(t, U_2), F_2(t, U_2), U_1, U_2, F_1(t, 1), F_2(t, 1)).$$

Compute an element of $\langle \mathcal{S}, m \cdot (U_1 - U_2) - 1 \rangle \cap \mathbb{Q}[z_0, t]$.

The geometric strategy previously described for solving one DDE can be extended here!

Conclusion and perspectives

- Decidability: geometry-driven algorithm computing $R \in \mathbb{Q}[z,t] \setminus \{0\}$ s.t. $R(F_1(t,1),t) = 0$,
- Resolution of the DDE of 5-constellations in an automatic fashion,
- Constructive proof of algebraicity of solutions of SDDEs.

Conclusion and perspectives

- Decidability: geometry-driven algorithm computing $R \in \mathbb{Q}[z,t] \setminus \{0\}$ s.t. $R(F_1(t,1),t) = 0$,
- Resolution of the DDE of 5-constellations in an automatic fashion,
- Constructive proof of algebraicity of solutions of SDDEs.

- Implementing the algorithm in a Maple package? (Work in progress)
- Expanded algorithmic comparison in the system case?
 (Work in progress with S. Yurkevich)
- More nested catalytic variables in the direction of Popescu's theorem?
 (Work in progress with M. Bousquet-Mélou)

RTCA: Computer Algebra for Functional Equations in Combinatorics & Physics

September 18 to December 11, 2023

Organizers:

Alin Bostan (Inria, Saday), Mark Giesbrecht (University of Waterloo) Christoph Koutschan (RICAM, Linz), Marni Mishna GFU, Burnabyi Mohab Safey El Din (Sorbonne Université), Bruno Salvy (Inria, Lyon) Gilles Villard (CNRS, Lyon)



Recent Trends in Computer Algebra

Thematic program with courses, workshops and topical days

CIRM Preparatory School March 6-10, 2023

Fundamental Algorithms and Algorithmic Complexity Special week: September 18-22 Workshop: September 25-29

Geometry of Polynomial System Solving, Optimization and Topology Special week: October 9-13 Workshop: October 16-20 Topical days: October 23-24

Computer Algebra for Functional Equations in Combinatorics & Physics Special week Nov. 27-Dec.1 Workshop: December 4-8 Topical day: December 11



Program coordinated by the Centre Emile Borel (CEB) at IHP (Paris) and also accessible onlin Participation of postdocs and PhD students is strongly encouraged Resistration is free bowever mandatory.

Scientific program and registration on: https://indico.math.cnrs.fr/category/588 Deadling for financial manner: March 157, 2023

Contact: RTCA2023-Panis@in

CEB organization assistant: Sofia Minasia CEB manager: Sylvie Lhermitte



November 27th → December 11th

Special week:

November 27th \rightarrow December 1st,

• Workshop:

December 4th → December 8th,

• Topical day:

December 11th.

Thank you for your attention!

```
Input: (The rather big DDE associated with the enumeration of 5-constellations) 
Output: 15625t^2F(t,1)^5 - 31250t^2F(t,1)^4 + (25000t^2 - 1000t)F(t,1)^3 - (10000t^2 - 8700t)F(t,1)^2 + (2000t^2 - 15855t + 16)F(t,1) - 160t^2 + 8139t - 16 = 0
```

```
Input: (The rather big DDE associated with the enumeration of 5-constellations) 
Output: 15625t^2F(t,1)^5 - 31250t^2F(t,1)^4 + (25000t^2 - 1000t)F(t,1)^3 - (10000t^2 - 8700t)F(t,1)^2 + (2000t^2 - 15855t + 16)F(t,1) - 160t^2 + 8139t - 16 = 0
```

- ullet Draw at random a prime number p and some $c\in \mathbb{F}_p$,
- Compute upper bounds (9,3) on the bidegree of $M \in \mathbb{F}_p[z,t]$ annihilating F(t,1) modulo p,
- Expand the truncated series $F(t, 1) \mod t^{55}$, $55 = 2 \cdot 9 \cdot 3 + 1$
- Guess $R \in \mathbb{Q}[z, t]$ such that $R(F(t, 1), t) = O(t^{(9+1)\cdot(3+1)-1})$,
- Check that $R(t, F(t, 1)) = O(t^{55})$. (\implies R is satisfied)

Input: (The rather big DDE associated with the enumeration of 5-constellations) **Output:** $15625t^2F(t,1)^5 - 31250t^2F(t,1)^4 + (25000t^2 - 1000t)F(t,1)^3 - (10000t^2 - 8700t)F(t,1)^2 + (2000t^2 - 15855t + 16)F(t,1) - 160t^2 + 8139t - 16 = 0$

- Draw at random a prime number p and some $c \in \mathbb{F}_p$,
- **Compute** upper bounds (9,3) on the bidegree of $M \in \mathbb{F}_p[z,t]$ annihilating F(t,1) modulo p,
- Expand the truncated series $F(t, 1) \mod t^{55}$, $55 = 2 \cdot 9 \cdot 3 + 1$
- **Guess** $R \in \mathbb{Q}[z, t]$ such that $R(F(t, 1), t) = O(t^{(9+1)\cdot(3+1)-1})$,
- Check that $R(t, F(t, 1)) = O(t^{55})$. (\Longrightarrow R is satisfied)

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

- \leadsto elimination strategy,
- → Newton iteration,
- → Hermite Padé approximants,
- $\rightsquigarrow \textbf{multiplicity lemma}.$

Input: (The rather big DDE associated with the enumeration of 5-constellations)

Output:
$$15625t^2F(t,1)^5 - 31250t^2F(t,1)^4 + (25000t^2 - 1000t)F(t,1)^3 - (10000t^2 - 8700t)F(t,1)^2 + (2000t^2 - 15855t + 16)F(t,1) - 160t^2 + 8139t - 16 = 0$$

- ullet Draw at random a prime number p and some $c\in\mathbb{F}_p$,
- Compute upper bounds (9,3) on the bidegree of $M \in \mathbb{F}_p[z,t]$ annihilating F(t,1) modulo p,
- Expand the truncated series $F(t, 1) \mod t^{55}$, $55 = 2 \cdot 9 \cdot 3 + 1$
- Guess $R \in \mathbb{Q}[z,t]$ such that $R(F(t,1),t) = O(t^{(9+1)\cdot(3+1)-1})$,
- Check that $R(t, F(t, 1)) = O(t^{55})$. (\implies R is satisfied)

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

→ elimination strategy,

→ Newton iteration,

 $\rightsquigarrow \textbf{Hermite Pad\'e approximants},$

→ multiplicity lemma.

Strategy	Timing	(d_z, d_t)
Elimination	2d21h	(9,3)
Hybrid G-P	2h40min	(5, 2)

Consider

$$\begin{cases} \mathbf{F_1} = f_1(u) + t \cdot Q_1(\nabla^k F_1, \dots, \nabla^k F_n, t, u), \\ \vdots & \vdots \\ \mathbf{F_n} = f_n(u) + t \cdot Q_n(\nabla^k F_1, \dots, \nabla^k F_n, t, u). \end{cases}$$
(SDDEs)

Consider

$$\begin{cases} F_{1} = f_{1}(u) + t \cdot Q_{1}(\nabla^{k}F_{1}, \dots, \nabla^{k}F_{n}, t, u), \\ \vdots & \vdots \\ F_{n} = f_{n}(u) + t \cdot Q_{n}(\nabla^{k}F_{1}, \dots, \nabla^{k}F_{n}, t, u). \end{cases}$$
(SDDEs)

Perturbe (SDDEs) and define the "numerators" E_1, \ldots, E_n and the polynomials

$$\mathsf{Det} := \mathsf{det} \begin{pmatrix} \partial_{x_1} E_1 & \dots & \partial_{x_n} E_1 \\ \vdots & \ddots & \vdots \\ \partial_{x_1} E_n & \dots & \partial_{x_n} E_n \end{pmatrix} \quad \mathsf{and} \quad P := \mathsf{det} \begin{pmatrix} \partial_{x_1} E_1 & \dots & \partial_{x_{n-1}} E_1 & \partial_u E_1 \\ \vdots & \ddots & \vdots & \vdots \\ \partial_{x_1} E_{n-1} & \dots & \partial_{x_{n-1}} E_{n-1} & \partial_u E_{n-1} \\ \partial_{x_1} E_n & \dots & \partial_{x_{n-1}} E_n & \partial_u E_n \end{pmatrix},$$

Consider

$$\begin{cases} \mathbf{F_1} = f_1(u) + t \cdot Q_1(\nabla^k F_1, \dots, \nabla^k F_n, t, u), \\ \vdots & \vdots \\ \mathbf{F_n} = f_n(u) + t \cdot Q_n(\nabla^k F_1, \dots, \nabla^k F_n, t, u). \end{cases}$$
(SDDEs)

Perturbe (SDDEs) and define the "numerators" E_1, \ldots, E_n and the polynomials

$$\mathsf{Det} := \mathsf{det} \begin{pmatrix} \partial_{\mathsf{x}_1} E_1 & \dots & \partial_{\mathsf{x}_n} E_1 \\ \vdots & \ddots & \vdots \\ \partial_{\mathsf{x}_1} E_n & \dots & \partial_{\mathsf{x}_n} E_n \end{pmatrix} \quad \mathsf{and} \quad P := \mathsf{det} \begin{pmatrix} \partial_{\mathsf{x}_1} E_1 & \dots & \partial_{\mathsf{x}_{n-1}} E_1 & \partial_u E_1 \\ \vdots & \ddots & \vdots & \vdots \\ \partial_{\mathsf{x}_1} E_{n-1} & \dots & \partial_{\mathsf{x}_{n-1}} E_{n-1} & \partial_u E_{n-1} \\ \partial_{\mathsf{x}_1} E_n & \dots & \partial_{\mathsf{x}_{n-1}} E_n & \partial_u E_n \end{pmatrix},$$

Set up the duplicated polynomial system (S_{dup}), consisting in the nk duplications of the polynomials E_1, \ldots, E_n , Det, P. It has nk(n+2) variables and equations.

Consider

$$\begin{cases} F_{1} = f_{1}(u) + t \cdot Q_{1}(\nabla^{k}F_{1}, \dots, \nabla^{k}F_{n}, t, u), \\ \vdots & \vdots \\ F_{n} = f_{n}(u) + t \cdot Q_{n}(\nabla^{k}F_{1}, \dots, \nabla^{k}F_{n}, t, u). \end{cases}$$
(SDDEs)

Perturbe (SDDEs) and **define** the "numerators" E_1, \ldots, E_n and the polynomials

$$\mathsf{Det} := \mathsf{det} \begin{pmatrix} \partial_{\mathsf{x}_1} E_1 & \dots & \partial_{\mathsf{x}_n} E_1 \\ \vdots & \ddots & \vdots \\ \partial_{\mathsf{x}_1} E_n & \dots & \partial_{\mathsf{x}_n} E_n \end{pmatrix} \quad \mathsf{and} \quad P := \mathsf{det} \begin{pmatrix} \partial_{\mathsf{x}_1} E_1 & \dots & \partial_{\mathsf{x}_{n-1}} E_1 & \partial_{\mathsf{u}} E_1 \\ \vdots & \ddots & \vdots & \vdots \\ \partial_{\mathsf{x}_1} E_{n-1} & \dots & \partial_{\mathsf{x}_{n-1}} E_{n-1} & \partial_{\mathsf{u}} E_{n-1} \\ \partial_{\mathsf{x}_1} E_n & \dots & \partial_{\mathsf{x}_{n-1}} E_n & \partial_{\mathsf{u}} E_n \end{pmatrix},$$

Set up the duplicated polynomial system (S_{dup}), consisting in the nk duplications of the polynomials E_1, \ldots, E_n , Det, P. It has nk(n+2) variables and equations.

Compute a non-trivial element of $(\langle \mathcal{S}_{dup} \rangle : det(Jac_{\mathcal{S}_{dup}})^{\infty}) \cap \mathbb{K}[t, z_0, \epsilon]$, then set ϵ to 0.