## 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:

## Which type of equations are we looking at?

## rooted planar maps



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

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

## Which type of equations are we looking at?

## rooted planar maps



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

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


$$
\begin{aligned}
F(t, u)=1+t u\left(F(t, u)^{3}\right. & +(2 F(t, u)+F(t, 1)) \frac{F(t, u)-F(t, 1)}{u-1} \\
& \left.+\frac{F(t, u)-F(t, 1)-(u-1) \partial_{u} F(t, 1)}{(u-1)^{2}}\right)
\end{aligned}
$$

## Which type of equations are we looking at?

## rooted planar maps



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

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


$$
\begin{aligned}
F(t, u)=1+t u\left(F(t, u)^{3}\right. & +(2 F(t, u)+F(t, 1)) \frac{F(t, u)-F(t, 1)}{u-1} \\
& \left.+\frac{F(t, u)-F(t, 1)-(u-1) \partial_{u} F(t, 1)}{(u-1)^{2}}\right)
\end{aligned}
$$

## hard particles on planar maps

$$
\left\{\begin{array}{l}
F(t, u)=x-y+G(t, u)+t u\left(u F(t, u)^{2}+\frac{u F(t, u)-F(t, 1)}{u-1}\right) \\
G(t, u)=y+t s u\left(F(t, u) G(t, u)+\frac{G(t, u)-G(t, 1)}{u-1}\right)
\end{array}\right.
$$

## How to relate these combinatorial objects to such equations?

## rooted planar maps



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

## How to relate these combinatorial objects to such equations?

## rooted planar maps



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

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

$$
\begin{array}{cc}
\sum_{n=0}^{\infty} a_{n} t^{n} & \text { generating function } \\
F(t, u):=\sum_{n=0}^{\infty} \sum_{d=0}^{n} a_{n, d} u^{d} t^{n} \quad \text { refinement }
\end{array}
$$

## How to relate these combinatorial objects to such equations?

## rooted planar maps



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

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

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

generating function $\downarrow$ refinement

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


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

$$
-\quad-\quad-1
$$

$$
t u^{2} F(t, u)^{2}
$$

## How to relate these combinatorial objects to such equations?

## rooted planar maps



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

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

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

generating function $\downarrow$ refinement

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



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

$$
t u^{2} F(t, u)^{2}
$$

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

## 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...

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

## 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...

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

From R:

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


## 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.


## 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.


## Plan

I Perform the above points for DDEs
II Perform the above points for systems of DDEs
[Bostan, N., Safey El Din '23] [N., Yurkevich '23]

## Objects of interest: Discrete Differential Equations

## Definition

Given $f \in \mathbb{Q}[u], k \geq 1$, and $Q \in \mathbb{Q}\left[y_{0}, \ldots, y_{k}, t, u\right]$,

$$
\begin{equation*}
F=f+t \cdot Q\left(F, \Delta F, \ldots, \Delta^{k} F, t, u\right) \tag{DDE}
\end{equation*}
$$

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 $Q \in \mathbb{Q}\left[y_{0}, \ldots, y_{k}, t, u\right]$,

$$
\begin{equation*}
F=f+t \cdot Q\left(F, \Delta F, \ldots, \Delta^{k} F, t, u\right) \tag{DDE}
\end{equation*}
$$

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...

$$
\begin{aligned}
F(t, u)=1+t u\left(F(t, u)^{3}\right. & +(2 F(t, u)+F(t, 1)) \frac{F(t, u)-F(t, 1)}{u-1} \\
& \left.+\frac{F(t, u)-F(t, 1)-(u-1) \partial_{u} F(t, 1)}{(u-1)^{2}}\right)
\end{aligned}
$$

## Objects of interest: Discrete Differential Equations

## Definition

Given $f \in \mathbb{Q}[u], k \geq 1$, and $Q \in \mathbb{Q}\left[y_{0}, \ldots, y_{k}, t, u\right]$,

$$
\begin{equation*}
F=f+t \cdot Q\left(F, \Delta F, \ldots, \Delta^{k} F, t, u\right) \tag{DDE}
\end{equation*}
$$

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...

$$
\begin{aligned}
F(t, u)=1+t u\left(F(t, u)^{3}\right. & +(2 F(t, u)+F(t, 1)) \frac{F(t, u)-F(t, 1)}{u-1} \\
& \left.+\frac{F(t, u)-F(t, 1)-(u-1) \partial_{u} F(t, 1)}{(u-1)^{2}}\right)
\end{aligned}
$$

## Theorem

[Bousquet-Mélou, Jehanne '06]
The unique solution in $\mathbb{Q}[u][[t]]$ of (DDE) is algebraic over $\mathbb{Q}(t, u)$.
$\leadsto$ Constructive proof $\Longrightarrow$ algorithm

Input: $F(t, u)=1+t u\left(F(t, u)^{3}+(2 F(t, u)+F(t, 1)) \frac{F(t, u)-F(t, 1)}{u-1}+\frac{F(t, u)-F(t, 1)-(u-1) \partial_{u} F(t, 1)}{(u-1)^{2}}\right)$,
Output: $81 t^{2} F(t, 1)^{3}-9 t(9 t-2) F(t, 1)^{2}+\left(27 t^{2}-66 t+1\right) F(t, 1)-3 t^{2}+47 t-1=0$.

Input: $F(t, u)=1+t u\left(F(t, u)^{3}+(2 F(t, u)+F(t, 1)) \frac{F(t, u)-F(t, 1)}{u-1}+\frac{F(t, u)-F(t, 1)-(u-1) \partial_{u} F(t, 1)}{(u-1)^{2}}\right)$,
Output: $81 t^{2} F(t, 1)^{3}-9 t(9 t-2) F(t, 1)^{2}+\left(27 t^{2}-66 t+1\right) F(t, 1)-3 t^{2}+47 t-1=0$.

- Compute $P \in \mathbb{Q}(t)\left[x, u, z_{0}, z_{1}\right]$ such that $P\left(F(t, u), u, F(t, 1), \partial_{u} F(t, 1)\right)=0$,

Input: $F(t, u)=1+t u\left(F(t, u)^{3}+(2 F(t, u)+F(t, 1)) \frac{F(t, u)-F(t, 1)}{u-1}+\frac{F(t, u)-F(t, 1)-(u-1) \partial_{u} F(t, 1)}{(u-1)^{2}}\right)$,
Output: $81 t^{2} F(t, 1)^{3}-9 t(9 t-2) F(t, 1)^{2}+\left(27 t^{2}-66 t+1\right) F(t, 1)-3 t^{2}+47 t-1=0$.

- Compute $P \in \mathbb{Q}(t)\left[x, u, z_{0}, z_{1}\right]$ such that $P\left(F(t, u), u, F(t, 1), \partial_{u} F(t, 1)\right)=0$,
- Consider

$$
\partial_{u} F(t, u) \cdot \partial_{x} P\left(F(t, u), u, F(t, 1), \partial_{u} F(t, 1)\right)+\partial_{u} P\left(F(t, u), u, F(t, 1), \partial_{u} F(t, 1)\right)=0
$$

Input: $F(t, u)=1+t u\left(F(t, u)^{3}+(2 F(t, u)+F(t, 1)) \frac{F(t, u)-F(t, 1)}{u-1}+\frac{F(t, u)-F(t, 1)-(u-1) \partial_{u} F(t, 1)}{(u-1)^{2}}\right)$,
Output: $81 t^{2} F(t, 1)^{3}-9 t(9 t-2) F(t, 1)^{2}+\left(27 t^{2}-66 t+1\right) F(t, 1)-3 t^{2}+47 t-1=0$.

- Compute $P \in \mathbb{Q}(t)\left[x, u, z_{0}, z_{1}\right]$ such that $P\left(F(t, u), u, F(t, 1), \partial_{u} F(t, 1)\right)=0$,
- Consider

$$
\partial_{u} F(t, u) \cdot \partial_{x} P\left(F(t, u), u, F(t, 1), \partial_{u} F(t, 1)\right)+\partial_{u} P\left(F(t, u), u, F(t, 1), \partial_{u} F(t, 1)\right)=0
$$

- Show that there exist distinct $U_{1}, U_{2} \in \bigcup_{d \geq 1} \overline{\mathbb{Q}}\left[\left[t^{\frac{1}{d}}\right]\right]$ s.t. $\partial_{x} P\left(F\left(t, U_{i}\right), U_{i}, F(t, 1), \partial_{u} F(t, 1)\right)=0$,

Input: $F(t, u)=1+t u\left(F(t, u)^{3}+(2 F(t, u)+F(t, 1)) \frac{F(t, u)-F(t, 1)}{u-1}+\frac{F(t, u)-F(t, 1)-(u-1) \partial_{u} F(t, 1)}{(u-1)^{2}}\right)$,
Output: $81 t^{2} F(t, 1)^{3}-9 t(9 t-2) F(t, 1)^{2}+\left(27 t^{2}-66 t+1\right) F(t, 1)-3 t^{2}+47 t-1=0$.

- Compute $P \in \mathbb{Q}(t)\left[x, u, z_{0}, z_{1}\right]$ such that $P\left(F(t, u), u, F(t, 1), \partial_{u} F(t, 1)\right)=0$,
- Consider

$$
\partial_{u} F(t, u) \cdot \partial_{x} P\left(F(t, u), u, F(t, 1), \partial_{u} F(t, 1)\right)+\partial_{u} P\left(F(t, u), u, F(t, 1), \partial_{u} F(t, 1)\right)=0
$$

- Show that there exist distinct $U_{1}, U_{2} \in \bigcup_{d \geq 1} \overline{\mathbb{Q}}\left[\left[t^{\frac{1}{d}}\right]\right]$ s.t. $\partial_{x} P\left(F\left(t, U_{i}\right), U_{i}, F(t, 1), \partial_{u} F(t, 1)\right)=0$,
- Set up

For $1 \leq i \leq 2,\left\{\begin{array}{c}P\left(F\left(t, U_{i}\right), U_{i}, F(t, 1), \partial_{u} F(t, 1)\right)=0, \\ \partial_{x} P\left(F\left(t, U_{i}\right), U_{i}, F(t, 1), \partial_{u} F(t, 1)\right)=0, \\ \partial_{u} P\left(F\left(t, U_{i}\right), U_{i}, F(t, 1), \partial_{u} F(t, 1)\right)=0, \\ m \cdot\left(U_{1}-U_{2}\right)-1=0 .\end{array}\right.$

Input: $F(t, u)=1+t u\left(F(t, u)^{3}+(2 F(t, u)+F(t, 1)) \frac{F(t, u)-F(t, 1)}{u-1}+\frac{F(t, u)-F(t, 1)-(u-1) \partial_{u} F(t, 1)}{(u-1)^{2}}\right)$,
Output: $81 t^{2} F(t, 1)^{3}-9 t(9 t-2) F(t, 1)^{2}+\left(27 t^{2}-66 t+1\right) F(t, 1)-3 t^{2}+47 t-1=0$.

- Compute $P \in \mathbb{Q}(t)\left[x, u, z_{0}, z_{1}\right]$ such that $P\left(F(t, u), u, F(t, 1), \partial_{u} F(t, 1)\right)=0$,
- Consider

$$
\partial_{u} F(t, u) \cdot \partial_{x} P\left(F(t, u), u, F(t, 1), \partial_{u} F(t, 1)\right)+\partial_{u} P\left(F(t, u), u, F(t, 1), \partial_{u} F(t, 1)\right)=0
$$

- Show that there exist distinct $U_{1}, U_{2} \in \bigcup_{d \geq 1} \overline{\mathbb{Q}}\left[\left[t^{\frac{1}{d}}\right]\right]$ s.t. $\partial_{x} P\left(F\left(t, U_{i}\right), U_{i}, F(t, 1), \partial_{u} F(t, 1)\right)=0$,
- Set up

For $1 \leq i \leq 2,\left\{\begin{array}{r}P\left(F\left(t, U_{i}\right), U_{i}, F(t, 1), \partial_{u} F(t, 1)\right)=0, \\ \partial_{x} P\left(F\left(t, U_{i}\right), U_{i}, F(t, 1), \partial_{u} F(t, 1)\right)=0, \\ \partial_{u} P\left(F\left(t, U_{i}\right), U_{i}, F(t, 1), \partial_{u} F(t, 1)\right)=0, \\ m \cdot\left(U_{1}-U_{2}\right)-1=0 .\end{array}\right.$

## Elimination theory

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

Input: $F(t, u)=1+t u\left(F(t, u)^{3}+(2 F(t, u)+F(t, 1)) \frac{F(t, u)-F(t, 1)}{u-1}+\frac{F(t, u)-F(t, 1)-(u-1) \partial_{u} F(t, 1)}{(u-1)^{2}}\right)$,
Output: $81 t^{2} F(t, 1)^{3}-9 t(9 t-2) F(t, 1)^{2}+\left(27 t^{2}-66 t+1\right) F(t, 1)-3 t^{2}+47 t-1=0$.

- Compute $P \in \mathbb{Q}(t)\left[x, u, z_{0}, z_{1}\right]$ such that $P\left(F(t, u), u, F(t, 1), \partial_{u} F(t, 1)\right)=0$,
- Consider

$$
\partial_{u} F(t, u) \cdot \partial_{x} P\left(F(t, u), u, F(t, 1), \partial_{u} F(t, 1)\right)+\partial_{u} P\left(F(t, u), u, F(t, 1), \partial_{u} F(t, 1)\right)=0
$$

- Show that there exist distinct $U_{1}, U_{2} \in \bigcup_{d \geq 1} \overline{\mathbb{Q}}\left[\left[t^{\frac{1}{d}}\right]\right]$ s.t. $\partial_{x} P\left(F\left(t, U_{i}\right), U_{i}, F(t, 1), \partial_{u} F(t, 1)\right)=0$,
- Set up

For $1 \leq i \leq 2,\left\{\begin{array}{r}P\left(F\left(t, U_{i}\right), U_{i}, F(t, 1), \partial_{u} F(t, 1)\right)=0, \\ \partial_{x} P\left(F\left(t, U_{i}\right), U_{i}, F(t, 1), \partial_{u} F(t, 1)\right)=0, \\ \partial_{u} P\left(F\left(t, U_{i}\right), U_{i}, F(t, 1), \partial_{u} F(t, 1)\right)=0, \\ m \cdot\left(U_{1}-U_{2}\right)-1=0 .\end{array}\right.$

## Elimination theory

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

Input: $F(t, u)=1+t u\left(F(t, u)^{3}+(2 F(t, u)+F(t, 1)) \frac{F(t, u)-F(t, 1)}{u-1}+\frac{F(t, u)-F(t, 1)-(u-1) \partial_{u} F(t, 1)}{(u-1)^{2}}\right)$,
Output: $81 t^{2} F(t, 1)^{3}-9 t(9 t-2) F(t, 1)^{2}+\left(27 t^{2}-66 t+1\right) F(t, 1)-3 t^{2}+47 t-1=0$.

- Compute $P \in \mathbb{Q}(t)\left[x, u, z_{0}, z_{1}\right]$ such that $P\left(F(t, u), u, F(t, 1), \partial_{u} F(t, 1)\right)=0$,
- Consider

$$
\partial_{u} F(t, u) \cdot \partial_{x} P\left(F(t, u), u, F(t, 1), \partial_{u} F(t, 1)\right)+\partial_{u} P\left(F(t, u), u, F(t, 1), \partial_{u} F(t, 1)\right)=0
$$

- Show that there exist distinct $U_{1}, U_{2} \in \bigcup_{d \geq 1} \overline{\mathbb{Q}}\left[\left[t^{\frac{1}{d}}\right]\right]$ s.t. $\partial_{x} P\left(F\left(t, U_{i}\right), U_{i}, F(t, 1), \partial_{u} F(t, 1)\right)=0$,
- Set up

For $1 \leq i \leq 2,\left\{\begin{array}{c}P\left(F\left(t, U_{i}\right), U_{i}, F(t, 1), \partial_{u} F(t, 1)\right)=0, \\ \partial_{x} P\left(F\left(t, U_{i}\right), U_{i}, F(t, 1), \partial_{u} F(t, 1)\right)=0, \\ \partial_{u} P\left(F\left(t, U_{i}\right), U_{i}, F(t, 1), \partial_{u} F(t, 1)\right)=0, \\ m \cdot\left(U_{1}-U_{2}\right)-1=0 .\end{array}\right.$

## Elimination theory

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


## Quantitative estimates

$$
\mathcal{S}: \quad \text { For } 1 \leq i \leq 2,\left\{\begin{array}{r}
P\left(F\left(t, U_{i}\right), F(t, 1), \partial_{u} F(t, 1), t, U_{i}\right)=0, \\
\partial_{x} P\left(F\left(t, U_{i}\right), F(t, 1), \partial_{u} F(t, 1), t, U_{i}\right)=0, \\
\partial_{u} P\left(F\left(t, U_{i}\right), F(t, 1), \partial_{u} F(t, 1), t, U_{i}\right)=0,
\end{array} \quad U_{1}-U_{2} \neq 0 .\right.
$$

## Quantitative estimates

$$
\mathcal{S}: \quad \text { For } 1 \leq i \leq 2,\left\{\begin{array}{r}
P\left(F\left(t, U_{i}\right), F(t, 1), \partial_{u} F(t, 1), t, U_{i}\right)=0, \\
\partial_{x} P\left(F\left(t, U_{i}\right), F(t, 1), \partial_{u} F(t, 1), t, U_{i}\right)=0, \\
\partial_{u} P\left(F\left(t, U_{i}\right), F(t, 1), \partial_{u} F(t, 1), t, U_{i}\right)=0,
\end{array} \quad U_{1}-U_{2} \neq 0 .\right.
$$

## 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 $\mathbb{Q}(t)$.


## Quantitative estimates

$$
\mathcal{S}: \quad \text { For } 1 \leq i \leq 2,\left\{\begin{array}{r}
P\left(F\left(t, U_{i}\right), F(t, 1), \partial_{u} F(t, 1), t, U_{i}\right)=0, \\
\partial_{x} P\left(F\left(t, U_{i}\right), F(t, 1), \partial_{u} F(t, 1), t, U_{i}\right)=0, \\
\partial_{u} P\left(F\left(t, U_{i}\right), F(t, 1), \partial_{u} F(t, 1), t, U_{i}\right)=0,
\end{array} \quad U_{1}-U_{2} \neq 0 .\right.
$$

## 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.

$$
\mathcal{S}: \quad \text { For } 1 \leq i \leq 2,\left\{\begin{array}{r}
P\left(F\left(t, U_{i}\right), F(t, 1), \partial_{u} F(t, 1), t, U_{i}\right)=0, \\
\partial_{x} P\left(F\left(t, U_{i}\right), F(t, 1), \partial_{u} F(t, 1), t, U_{i}\right)=0, \\
\partial_{u} P\left(F\left(t, U_{i}\right), F(t, 1), \partial_{u} F(t, 1), t, U_{i}\right)=0,
\end{array} \quad U_{1}-U_{2} \neq 0 .\right.
$$

## 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.
[Bostan, N., Safey El Din '23]
Under the above assumptions:

$$
\delta:=\operatorname{deg}(P)
$$

- There exists some nonzero polynomial $R \in \mathbb{Q}\left[z_{0}, t\right]$ 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 $O_{\log }\left(\delta^{17}\right)$ ops. in $\mathbb{Q}$.


## Some preliminaries on Gröbner bases

$\mathcal{A}:=\mathbb{Q}[x, y]$ polynomial ring, where $\boldsymbol{y}=y_{1}, \ldots, y_{s}$.

## Monomial orders

- $x^{4} y_{1}^{3} y_{2}^{2} \succ_{\text {lex }} x^{3} y_{1}^{4} y_{2}^{2}$ for a lexicographic order, - $x^{4} y_{1}^{2} y_{2}^{3} \succ_{\text {bmon }} x^{4} y_{1}^{3} y_{2}$ 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

- $x^{4} y_{1}^{3} y_{2}^{2} \succ_{\text {lex }} x^{3} y_{1}^{4} y_{2}^{2}$ for a lexicographic order,
- $x^{4} y_{1}^{2} y_{2}^{3} \succ_{\text {bmon }} x^{4} y_{1}^{3} y_{2}$ 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

$\mathcal{A}:=\mathbb{Q}[x, y]$ polynomial ring, where $\boldsymbol{y}=y_{1}, \ldots, y_{s}$.

## Monomial orders

- $x^{4} y_{1}^{3} y_{2}^{2} \succ_{\text {lex }} x^{3} y_{1}^{4} y_{2}^{2}$ for a lexicographic order,
- $x^{4} y_{1}^{2} y_{2}^{3} \succ_{\text {bmon }} x^{4} y_{1}^{3} y_{2}$ 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 $\succ$.

Fix a monomial order $\succ$ on $\mathcal{A}$. A finite subset $G=\left\{g_{1}, \ldots, g_{t}\right\}$ of an ideal $\mathcal{I} \subset \mathcal{A}$ different from 0 is said to be a Gröbner basis if $\left\langle\mathrm{LT}_{\succ}\left(g_{1}\right), \ldots, \mathrm{LT}_{\succ}\left(g_{t}\right)\right\rangle=\left\langle\mathrm{LT}_{\succ}(\mathcal{I})\right\rangle$.

## Some preliminaries on Gröbner bases

$\mathcal{A}:=\mathbb{Q}[x, y]$ polynomial ring, where $\boldsymbol{y}=y_{1}, \ldots, y_{s}$.

## Monomial orders

- $x^{4} y_{1}^{3} y_{2}^{2} \succ_{\text {lex }} x^{3} y_{1}^{4} y_{2}^{2}$ for a lexicographic order,
- $x^{4} y_{1}^{2} y_{2}^{3} \succ_{\text {bmon }} x^{4} y_{1}^{3} y_{2}$ for a block monomial order.


## Definition

Fix a monomial order $\succ$ on $\mathcal{A}$. A finite subset $G=\left\{g_{1}, \ldots, g_{t}\right\}$ of an ideal $\mathcal{I} \subset \mathcal{A}$ different from 0 is said to be a Gröbner basis if $\left.\langle\mathrm{LT}]_{\succ}\left(g_{1}\right), \ldots, \mathrm{LT}_{\succ}\left(g_{t}\right)\right\rangle=\left\langle\mathrm{LT}_{\succ}(\mathcal{I})\right\rangle$.

## 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 $\succ$.
## 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

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

## 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

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

$$
\begin{aligned}
& \pi_{x}:\left(x, \mathbf{u}, z_{0}, z_{1}\right) \in \overline{\mathbb{Q}}(t)^{4} \mapsto\left(\mathbf{u}, z_{0}, z_{1}\right) \in{\overline{\mathbb{Q}}(t)^{3}}^{3} \\
& \mathbf{W}:=\pi_{x}\left(V\left(\mathbf{P}, \partial_{\mathbf{x}} \mathbf{P}, \partial_{\mathbf{u}} \mathbf{P}\right) \backslash V(\mathbf{u})\right) \\
& \pi_{u}:\left(\mathbf{u}, z_{0}, z_{1}\right) \in{\overline{\mathbb{Q}}(t)^{3}}{ }^{2}\left(z_{0}, z_{1}\right) \in{\overline{\mathbb{Q}}(t)^{2}}^{2}
\end{aligned}
$$

## 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

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

$$
\begin{aligned}
& \pi_{x}:\left(x, \mathbf{u}, z_{0}, z_{1}\right) \in \overline{\mathbb{Q}}(t)^{4} \mapsto\left(\mathbf{u}, z_{0}, z_{1}\right) \in{\overline{\mathbb{Q}}(t)^{3}}^{3} \\
& \mathbf{W}:=\pi_{x}\left(V\left(\mathbf{P}, \partial_{\mathbf{x}} \mathbf{P}, \partial_{\mathbf{u}} \mathbf{P}\right) \backslash V(\mathbf{u})\right) \\
& \pi_{u}:\left(\mathbf{u}, z_{0}, z_{1}\right) \in \overline{\mathbb{Q}}(t)^{3} \mapsto\left(z_{0}, z_{1}\right) \in \overline{\mathbb{Q}(t)}^{2}
\end{aligned}
$$

Characterize with polynomial constraints
$\mathcal{F}_{2}:=\left\{\alpha_{\underline{z}} \in \overline{\mathbb{Q}}(t)^{2} \mid \# \pi_{u}^{-1}\left(\alpha_{\underline{z}}\right) \cap \mathbf{W} \geq 2\right\}$

## 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

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

$\pi_{x}:\left(x, \mathbf{u}, z_{0}, z_{1}\right) \in \overline{\mathbb{Q}}(t)^{4} \mapsto\left(\mathbf{u}, z_{0}, z_{1}\right) \in \overline{\mathbb{Q}}(t)^{3}$,
$\mathbf{W}:=\pi_{x}\left(V\left(\mathbf{P}, \partial_{\mathbf{x}} \mathbf{P}, \partial_{\mathbf{u}} \mathbf{P}\right) \backslash V(\mathbf{u})\right)$
$\pi_{u}:\left(\mathbf{u}, z_{0}, z_{1}\right) \in \overline{\mathbb{Q}}(t)^{3} \mapsto\left(z_{0}, z_{1}\right) \in \overline{\mathbb{Q}}(t)^{2}$,

Characterize with polynomial constraints
$\mathcal{F}_{2}:=\left\{\alpha_{\underline{z}} \in \overline{\mathbb{Q}}(t)^{2} \mid \# \pi_{u}^{-1}\left(\alpha_{\underline{z}}\right) \cap \mathbf{W} \geq 2\right\}$


## Solving a toy example...

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

## Solving a toy example...

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

- Compute $P \in \mathbb{Q}(t)\left[x, u, z_{0}, z_{1}\right]$ such that $P\left(F(t, u), u, F(t, 0), \partial_{u} F(t, 0)\right)=0$,


## Solving a toy example...

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

- Compute $P \in \mathbb{Q}(t)\left[x, u, z_{0}, z_{1}\right]$ such that $P\left(F(t, u), u, F(t, 0), \partial_{u} F(t, 0)\right)=0$,
- Compute $G_{u}$ Gröbner basis of $\left\langle P, \partial_{1} P, \partial_{2} P, m \cdot u-1\right\rangle \cap \mathbb{Q}(t)\left[u, z_{0}, z_{1}\right]$ for $\{u\} \succ$ lex $\left\{z_{0}, z_{1}\right\}$ :


## Solving a toy example...

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

- Compute $P \in \mathbb{Q}(t)\left[x, u, z_{0}, z_{1}\right]$ such that $P\left(F(t, u), u, F(t, 0), \partial_{u} F(t, 0)\right)=0$,
- Compute $G_{u}$ Gröbner basis of $\left\langle P, \partial_{1} P, \partial_{2} P, m \cdot u-1\right\rangle \cap \mathbb{Q}(t)\left[u, z_{0}, z_{1}\right]$ for $\{u\} \succ$ lex $\left\{z_{0}, z_{1}\right\}$ :
$\mathrm{B}_{0}: \quad \gamma_{0}$
$\mathbf{B}_{1}:\left\{\begin{array}{c}\beta_{1} \cdot u+\gamma_{1} \\ \vdots \\ \beta_{r} \cdot u+\gamma_{r}\end{array}, \boldsymbol{\gamma}_{\boldsymbol{i}}, \boldsymbol{\beta}_{\boldsymbol{j}} \in \mathbb{Q}(t)\left[z_{0}, z_{1}\right]\right.$
$\mathbf{B}_{2}: \quad \mathbf{g}_{2}:=u^{2}+\boldsymbol{\beta}_{r+1} \cdot u+\gamma_{r+1}$
"At $\left.\boldsymbol{\alpha} \in \pi_{u}\left(V\left(G_{u}\right)\right) \subset \overline{\mathbb{Q}(t)}\right)^{2}$, there exist two distinct solutions in $u$ "

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

$$
k=2
$$

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

- Compute $P \in \mathbb{Q}(t)\left[x, u, z_{0}, z_{1}\right]$ such that $P\left(F(t, u), u, F(t, 0), \partial_{u} F(t, 0)\right)=0$,
- Compute $G_{u}$ Gröbner basis of $\left\langle P, \partial_{1} P, \partial_{2} P, m \cdot u-1\right\rangle \cap \mathbb{Q}(t)\left[u, z_{0}, z_{1}\right]$ for $\{u\} \succ_{\text {lex }}\left\{z_{0}, z_{1}\right\}$ :
$\mathrm{B}_{0}: \quad \gamma_{0}$
$\mathbf{B}_{1}:\left\{\begin{array}{c}\beta_{1} \cdot u+\gamma_{1} \\ \vdots \\ \beta_{r} \cdot u+\gamma_{r}\end{array}\right.$

$$
, \boldsymbol{\gamma}_{i}, \boldsymbol{\beta}_{j} \in \mathbb{Q}(t)\left[z_{0}, z_{1}\right]
$$

$$
\text { "At } \boldsymbol{\alpha} \in \pi_{u}\left(V\left(G_{u}\right)\right) \subset{\overline{\mathbb{Q}}(t)^{2}}^{2},
$$

At $\alpha \in V\left(G_{u} \cap \mathbb{K}\left[t, z_{0}, z_{1}\right]\right)$ fixed, there exist two solutions in $u$
$\Longrightarrow \beta_{i}, \gamma_{j}=0 \quad$ (equations)

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

- Compute $P \in \mathbb{Q}(t)\left[x, u, z_{0}, z_{1}\right]$ such that $P\left(F(t, u), u, F(t, 0), \partial_{u} F(t, 0)\right)=0$,
- Compute $G_{u}$ Gröbner basis of $\left\langle P, \partial_{1} P, \partial_{2} P, m \cdot u-1\right\rangle \cap \mathbb{Q}(t)\left[u, z_{0}, z_{1}\right]$ for $\{u\} \succ_{\text {lex }}\left\{z_{0}, z_{1}\right\}$ :
$B_{0}$ :
$\gamma_{0}$
$\mathrm{B}_{1}:\{$

$$
\begin{array}{cl}
\boldsymbol{\beta}_{1} \cdot u+\gamma_{1} & \\
\vdots & , \gamma_{i}, \boldsymbol{\beta}_{\boldsymbol{j}} \in \mathbb{Q}(t)\left[z_{0}, z_{1}\right]
\end{array}
$$

"At $\boldsymbol{\alpha} \in \pi_{u}\left(V\left(G_{u}\right)\right) \subset \overline{\mathbb{Q}}(t)^{2}$,

$$
\beta_{r} \cdot u+\gamma_{r}
$$ there exist two distinct solutions in $u$ "

$\mathbf{B}_{2}: \quad \mathbf{g}_{2}:=u^{2}+\boldsymbol{\beta}_{\boldsymbol{r}+\boldsymbol{1}} \cdot u+\gamma_{r+1}$

At $\boldsymbol{\alpha} \in V\left(G_{u} \cap \mathbb{K}\left[t, z_{0}, z_{1}\right]\right)$ fixed, there exist two solutions in $u$ $\Longrightarrow \beta_{i}, \gamma_{j}=0 \quad$ (equations)

## [Extension theorem]

$\boldsymbol{\alpha} \in \pi_{u}\left(V\left(G_{u}\right)\right) \quad \Longrightarrow$ LeadingCoeff $\left(g_{2}\right) \neq 0$
Distinct solutions in $u \Longrightarrow \operatorname{disc}_{\mathrm{u}}\left(\mathrm{g}_{2}\right) \neq 0 \quad$ (inequations)

Projecting<br>$\Longrightarrow$ Elimination theorem<br>Lifting points of the projections $\Longrightarrow$ Extension theorem

## ... yields an algorithm based on elimination theory

```
Projecting \Longrightarrow Elimination theorem
Lifting points of the projections }\Longrightarrow\mathrm{ Extension theorem
```

[Proposition] Let $g \in\left(\mathbb{Q}(t)\left[z_{0}, z_{1}\right]\right)[u]$. Then $g$ has at least $i$ distinct solutions at $\boldsymbol{\alpha} \in \overline{\mathbb{Q}}(t)^{2}$ if and only if the $(i \times i)$-minors of the Hermite quadratic form associated with $g$ do not vanish simultaneously at $\boldsymbol{\alpha}$.
$\leadsto$ Reduces to studying the multiplication maps $\left(M_{u^{\ell}}: q \mapsto q \cdot u^{\ell}\right)_{\ell \geq 1}$ in $\left(\mathbb{Q}\left[t, z_{0}, z_{1}\right]\right)[u] /\langle g\rangle$

## ... yields an algorithm based on elimination theory

## Projecting $\quad \Longrightarrow$ Elimination theorem <br> Lifting points of the projections $\Longrightarrow$ Extension theorem

[Proposition] Let $g \in\left(\mathbb{Q}(t)\left[z_{0}, z_{1}\right]\right)[u]$. Then $g$ has at least $i$ distinct solutions at $\boldsymbol{\alpha} \in \overline{\mathbb{Q}}(t)^{2}$ if and only if the $(i \times i)$-minors of the Hermite quadratic form associated with $g$ do not vanish simultaneously at $\boldsymbol{\alpha}$.

David A. Cox Donal O'Shea

Ideals, Varieties, and Algorithms
An Introduction to Computational Algebraic Geometry and Commutative Algebra

Fourth Edition
$\leadsto$ Reduces to studying the multiplication maps $\left(M_{u^{\ell}}: q \mapsto q \cdot u^{\ell}\right)_{\ell \geq 1}$ in $\left(\mathbb{Q}\left[t, z_{0}, z_{1}\right]\right)[u] /\langle g\rangle$

## Projecting <br> $\Longrightarrow$ Elimination theorem <br> Lifting points of the projections $\Longrightarrow$ Extension theorem

David A. Cox Donal O'Shea

Ideals, Varieties, and Algorithms
An Introduction to Computational Algebraic Geometry and Commutative Algebra

Fourth Edition
$\leadsto$ Reduces to studying the multiplication maps $\left(M_{u^{\ell}}: q \mapsto q \cdot u^{\ell}\right)_{\ell \geq 1}$ in $\left(\mathbb{Q}\left[t, z_{0}, z_{1}\right]\right)[u] /\langle g\rangle$
[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

## Projecting <br> $\Longrightarrow$ Elimination theorem <br> Lifting points of the projections $\Longrightarrow$ Extension theorem

David A. Cox Donal O'Shea
deals, Varieties, and Algorithms
An Introduction to Computational Algebraic Geometry and Commutative Algebra

Fourth Edition
$\leadsto$ Reduces to studying the multiplication maps $\left(M_{u^{\ell}}: q \mapsto q \cdot u^{\ell}\right)_{\ell \geq 1}$ in $\left(\mathbb{Q}\left[t, z_{0}, z_{1}\right]\right)[u] /\langle g\rangle$
[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 | $\left(d_{z_{0}}, \boldsymbol{d}_{\boldsymbol{t}}\right)$ |
| :---: | :---: | :---: |
| Duplication | $>5 \mathrm{~d}$ | $?$ |
| Elimination | 2 d 21 h | $(\mathbf{9}, \mathbf{3})$ |

## 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:

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

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

## Systems of Discrete Differential Equations

What could be extended to systems?

Modelling special Eulerian planar orientations:

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

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

Modelling hard particles on planar maps:

$$
\left\{\begin{array}{l}
F(t, u)=x-y+G(t, u)+t u\left(u F(t, u)^{2}+\frac{u F(t, u)-F(t, 1)}{u-1}\right) \\
G(t, u)=y+t s u\left(F(t, u) G(t, u)+\frac{G(t, u)-G(t, 1)}{u-1}\right)
\end{array}\right.
$$

## [Popescu '86, Swan '98]

(1.4) Theorem. Let $k$ be a field, $k\langle X\rangle$ the algebraic power series ring in $X=\left(X_{1}, \cdots, X_{r}\right)$ over $k, f$ a finite system of polynomial equations over $k\langle X\rangle$ and $\hat{y}=\left(\hat{y}_{1}, \cdots, \hat{y}_{n}\right) \in k \llbracket X \rrbracket^{n}$ a formal solution of $f$ such that $\hat{y}_{i} \in k \llbracket X_{1}$, $\cdots, X_{s_{i}} \rrbracket, 1 \leqslant i \leqslant n$ for some positive integers $s_{i} \leqslant r$. Then there exists a solution $y=\left(y_{1}, \cdots, y_{n}\right)$ of $f$ in $k\langle X\rangle$ such that $y_{i} \in k\left\langle X_{1}, \cdots, X_{s_{i}}\right\rangle, 1 \leqslant i \leqslant n$.

## [Popescu '86, Swan '98]

(1.4) Theorem. Let $k$ be a field, $k\langle X\rangle$ the algebraic power series ring in $X=\left(X_{1}, \cdots, X_{r}\right)$ over $k, f$ a finite system of polynomial equations over $k\langle X\rangle$ and $\hat{y}=\left(\hat{y}_{1}, \cdots, \hat{y}_{n}\right) \in k \llbracket X \rrbracket^{n}$ a formal solution of $f$ such that $\hat{y}_{i} \in k \llbracket X_{1}$, $\left.\cdots, X_{s_{i}}\right], 1 \leqslant i \leqslant n$ for some positive integers $s_{i} \leqslant r$. Then there exists a solution $y=\left(y_{1}, \cdots, y_{n}\right)$ of $f$ in $k\langle X\rangle$ such that $y_{i} \in k\left\langle X_{1}, \cdots, X_{s_{i}}\right\rangle, 1 \leqslant i \leqslant n$.

- Solutions of systems of DDEs are unique with components in $\mathbb{Q}[\boldsymbol{u}][[\boldsymbol{t}]] \Longrightarrow$ 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 $X=\left(X_{1}, \cdots, X_{r}\right)$ over $k, f$ a finite system of polynomial equations over $k\langle X\rangle$ and $\hat{y}=\left(\hat{y}_{1}, \cdots, \hat{y}_{n}\right) \in k \llbracket X \rrbracket^{n}$ a formal solution of $f$ such that $\hat{y}_{i} \in k \llbracket X_{1}$, $\cdots, X_{s_{i}} \rrbracket, 1 \leqslant i \leqslant n$ for some positive integers $s_{i} \leqslant r$. Then there exists a solution $y=\left(y_{1}, \cdots, y_{n}\right)$ of $f$ in $k\langle X\rangle$ such that $y_{i} \in k\left\langle X_{1}, \cdots, X_{s_{i}}\right\rangle, 1 \leqslant i \leqslant n$.

- Solutions of systems of DDEs are unique with components in $\mathbb{Q}[\boldsymbol{u}][[\boldsymbol{t}]] \Longrightarrow$ 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 $X=\left(X_{1}, \cdots, X_{r}\right)$ over $k, f$ a finite system of polynomial equations over $k\langle X\rangle$ and $\hat{y}=\left(\hat{y}_{1}, \cdots, \hat{y}_{n}\right) \in k \llbracket X \rrbracket^{n}$ a formal solution of $f$ such that $\hat{y}_{i} \in k \llbracket X_{1}$, $\cdots, X_{s_{i}} \rrbracket, 1 \leqslant i \leqslant n$ for some positive integers $s_{i} \leqslant r$. Then there exists a solution $y=\left(y_{1}, \cdots, y_{n}\right)$ of $f$ in $k\langle X\rangle$ such that $y_{i} \in k\left\langle X_{1}, \cdots, X_{s_{i}}\right\rangle, 1 \leqslant i \leqslant n$.

- Solutions of systems of DDEs are unique with components in $\mathbb{Q}[\boldsymbol{u}][[\boldsymbol{t}]] \Longrightarrow$ 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 $\{\boldsymbol{t}\} \subset\{\boldsymbol{t}, \boldsymbol{u}\}$.

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 $f_{1}, \ldots, f_{n} \in \mathbb{Q}[u], Q_{1}, \ldots, Q_{n} \in \mathbb{Q}\left[y_{1}, \ldots, y_{n(k+1)}, t, u\right]$ be polynomials. Denote $\nabla^{k} F:=F, \Delta F, \ldots, \Delta^{k} F$. Then the system of DDEs

$$
\left\{\begin{array}{cc}
\left(\mathrm{E}_{\mathrm{F}_{1}}\right): & F_{1}=f_{1}(u)+t \cdot Q_{1}\left(\nabla^{k} F_{1}, \ldots, \nabla^{k} F_{n}, t, u\right), \\
\vdots & \vdots \\
\left(\mathrm{E}_{\mathrm{F}_{\mathrm{n}}}\right): & F_{n}=f_{n}(u)+t \cdot Q_{n}\left(\nabla^{\star} F_{1}, \ldots, \nabla^{\star} F_{n}, t, u\right) .
\end{array}\right.
$$

(SDDEs)
admits a unique vector of solutions $\left(F_{1}, \ldots, F_{n}\right) \in \mathbb{Q}[u][[t]]^{n}$, and all its components are algebraic over $\mathbb{Q}(t, u)$.

## Constructive algebraicity theorem for solutions of systems of DDEs (FPSAC

[N., Yurkevich '23]

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

$$
\left\{\begin{array}{cc}
\left(\mathrm{E}_{\mathrm{F}_{1}}\right): & F_{1}=f_{1}(u)+t \cdot Q_{1}\left(\nabla^{k} F_{1}, \ldots, \nabla^{k} F_{n}, t, u\right), \\
\vdots & \vdots \\
\left(\mathrm{E}_{\mathrm{F}_{\mathrm{n}}}\right): & F_{n}=f_{n}(u)+t \cdot Q_{n}\left(\nabla^{\star} F_{1}, \ldots, \nabla^{\star} F_{n}, t, u\right) .
\end{array}\right.
$$

admits a unique vector of solutions $\left(F_{1}, \ldots, F_{n}\right) \in \mathbb{Q}[u][[t]]^{n}$, and all its components are algebraic over $\mathbb{Q}(t, u)$.

## [Proof sketch]

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


## Identifying more polynomial equations

## Consider

$\rightsquigarrow F_{1}, F_{2} \equiv F_{1}(t, u), F_{2}(t, u) \in \mathbb{Q}[u][[t]]$

$$
\left\{\begin{array}{l}
0=\left(1-F_{1}\right) \cdot(\mathbf{u}-1)+t \mathbf{u} \cdot\left(2 \mathbf{u} F_{1}^{2}-\mathbf{u} F_{1}(t, 1)+2 \mathbf{u} F_{2}(t, 1)-2 F_{1}^{2}+\mathbf{u}+F_{1}-2 F_{2}(t, 1)-1\right), \\
0=F_{2} \cdot(1-\mathbf{u})+t \mathbf{u} \cdot\left(2 \mathbf{u} F_{1} F_{2}+\mathbf{u} F_{1}-2 F_{1} F_{2}-F_{1}+F_{2}-F_{2}(t, 1)\right) .
\end{array}\right.
$$

Denote by $E_{1}, E_{2} \in \mathbb{Q}(t)\left[x_{1}, x_{2}, \mathbf{u}, z_{0}, z_{1}\right]$ polynomials such that

$$
\text { for } i \in\{1,2\}, \quad E_{i}\left(F_{1}(t, \mathbf{u}), F_{2}(t, \mathbf{u}), \mathbf{u}, F_{1}(t, 1), F_{2}(t, 1)\right)=0 . \quad\left(\equiv E_{i}(\mathbf{u})\right)
$$

## Identifying more polynomial equations

## Consider

$\rightsquigarrow F_{1}, F_{2} \equiv F_{1}(t, u), F_{2}(t, u) \in \mathbb{Q}[u][[t]]$

$$
\left\{\begin{array}{l}
0=\left(1-F_{1}\right) \cdot(\mathbf{u}-1)+t \mathbf{u} \cdot\left(2 \mathbf{u} F_{1}^{2}-\mathbf{u} F_{1}(t, 1)+2 \mathbf{u} F_{2}(t, 1)-2 F_{1}^{2}+\mathbf{u}+F_{1}-2 F_{2}(t, 1)-1\right), \\
0=F_{2} \cdot(1-\mathbf{u})+t \mathbf{u} \cdot\left(2 \mathbf{u} F_{1} F_{2}+\mathbf{u} F_{1}-2 F_{1} F_{2}-F_{1}+F_{2}-F_{2}(t, 1)\right) .
\end{array}\right.
$$

Denote by $E_{1}, E_{2} \in \mathbb{Q}(t)\left[x_{1}, x_{2}, \mathbf{u}, z_{0}, z_{1}\right]$ polynomials such that

$$
\text { for } i \in\{1,2\}, \quad E_{i}\left(F_{1}(t, \mathbf{u}), F_{2}(t, \mathbf{u}), \mathbf{u}, F_{1}(t, 1), F_{2}(t, 1)\right)=0 . \quad\left(\equiv E_{i}(\mathbf{u})\right)
$$

Differentiating with respect to $u$ yields

$$
\begin{aligned}
& \qquad\left(\begin{array}{ll}
\left(\partial_{x_{1}} E_{1}\right)(\mathrm{u}) & \left(\partial_{x_{2}} E_{1}\right)(\mathrm{u}) \\
\left(\partial_{x_{1}} E_{2}\right)(\mathrm{u}) & \left(\partial_{x_{2}} E_{2}\right)(\mathrm{u})
\end{array}\right) \cdot\binom{\partial_{\mathrm{u}} F_{1}}{\partial_{\mathrm{u}} F_{2}}+\binom{\left(\partial_{\mathrm{u}} E_{1}\right)(\mathrm{u})}{\left(\partial_{\mathrm{u}} E_{2}\right)(\mathrm{u})}=0 . \\
& \text { For } \mathbf{U}(\mathrm{t}) \in \bigcup_{d \geq 1} \overline{\mathbb{Q}}\left[[ t ^ { \frac { 1 } { d } ] ] } ] \left\{\begin{array}{ll}
\text { if } & \left(\partial_{x_{1}} E_{1} \cdot \partial_{\mathbf{x}_{2}} E_{2}-\partial_{x_{1}} E_{2} \cdot \partial_{x_{2}} E_{1}\right)(\mathrm{U}(\mathrm{t}))=0, \\
\text { then }\left(\partial_{x_{1}} E_{1} \cdot \partial_{\mathrm{u}} E_{2}-\partial_{x_{1}} E_{2} \cdot \partial_{\mathrm{u}} E_{1}\right)(\mathrm{U}(\mathrm{t}))=0 .
\end{array}\right.\right.
\end{aligned}
$$

## Identifying more polynomial equations

## Consider

$\leadsto F_{1}, F_{2} \equiv F_{1}(t, u), F_{2}(t, u) \in \mathbb{Q}[u][[t]]$

$$
\left\{\begin{array}{l}
0=\left(1-F_{1}\right) \cdot(\mathbf{u}-1)+t \mathbf{u} \cdot\left(2 \mathbf{u} F_{1}^{2}-\mathbf{u} F_{1}(t, 1)+2 \mathbf{u} F_{2}(t, 1)-2 F_{1}^{2}+\mathbf{u}+F_{1}-2 F_{2}(t, 1)-1\right), \\
0=F_{2} \cdot(1-\mathbf{u})+t \mathbf{u} \cdot\left(2 \mathbf{u} F_{1} F_{2}+\mathbf{u} F_{1}-2 F_{1} F_{2}-F_{1}+F_{2}-F_{2}(t, 1)\right) .
\end{array}\right.
$$

Denote by $E_{1}, E_{2} \in \mathbb{Q}(t)\left[x_{1}, x_{2}, \mathbf{u}, z_{0}, z_{1}\right]$ polynomials such that

$$
\text { for } i \in\{1,2\}, \quad E_{i}\left(F_{1}(t, \mathbf{u}), F_{2}(t, \mathbf{u}), \mathbf{u}, F_{1}(t, 1), F_{2}(t, 1)\right)=0 . \quad\left(\equiv E_{i}(\mathbf{u})\right)
$$

Differentiating with respect to $u$ yields

$$
\begin{aligned}
& \qquad\left(\begin{array}{ll}
\left(\partial_{x_{1}} E_{1}\right)(\mathrm{u}) & \left(\partial_{x_{2}} E_{1}\right)(\mathrm{u}) \\
\left(\partial_{x_{1}} E_{2}\right)(\mathrm{u}) & \left(\partial_{x_{2}} E_{2}\right)(\mathrm{u})
\end{array}\right) \cdot\binom{\partial_{\mathrm{u}} F_{1}}{\partial_{\mathrm{u}} F_{2}}+\binom{\left(\partial_{\mathrm{u}} E_{1}\right)(\mathrm{u})}{\left(\partial_{\mathrm{u}} E_{2}\right)(\mathrm{u})}=0 . \\
& \text { For } \mathbf{U}(\mathrm{t}) \in \bigcup_{d \geq 1} \overline{\mathbb{Q}}\left[[ t ^ { \frac { 1 } { d } ] ] } ] \left\{\begin{array}{ll}
\text { if } & \left(\partial_{x_{1}} E_{1} \cdot \partial_{\mathbf{x}_{2}} E_{2}-\partial_{x_{1}} E_{2} \cdot \partial_{x_{2}} E_{1}\right)(\mathrm{U}(\mathrm{t}))=0, \\
\text { then }\left(\partial_{x_{1}} E_{1} \cdot \partial_{\mathrm{u}} E_{2}-\partial_{x_{1}} E_{2} \cdot \partial_{\mathrm{u}} E_{1}\right)(\mathrm{U}(\mathrm{t}))=0 .
\end{array}\right.\right.
\end{aligned}
$$

## A polynomial system for systems of 2 DDEs of order 1

$$
\left\{\begin{array}{l}
F_{1}=f_{1}(u)+t \cdot Q_{1}\left(F_{1}, \Delta F_{1}, F_{2}, \Delta F_{2}, t, u\right),  \tag{SDDEs}\\
F_{2}=f_{2}(u)+t \cdot Q_{2}\left(F_{1}, \Delta F_{1}, F_{2}, \Delta F_{2}, t, u\right) .
\end{array}\right.
$$

## A polynomial system for systems of 2 DDEs of order 1

$$
\left\{\begin{array}{l}
F_{1}=f_{1}(u)+t \cdot Q_{1}\left(F_{1}, \Delta F_{1}, F_{2}, \Delta F_{2}, t, u\right)  \tag{SDDEs}\\
F_{2}=f_{2}(u)+t \cdot Q_{2}\left(F_{1}, \Delta F_{1}, F_{2}, \Delta F_{2}, t, u\right)
\end{array}\right.
$$

Define the "numerators" $E_{1}, E_{2}$ and the polynomials

$$
\text { Det }:=\operatorname{det}\left(\begin{array}{ll}
\partial_{\times_{1}} E_{1} & \partial_{\times_{x_{2}}} E_{1} \\
\partial_{\times_{1}} E_{2} & \partial_{\times_{2}} E_{2}
\end{array}\right) \quad \text { and } \quad P:=\operatorname{det}\left(\begin{array}{ll}
\partial_{x_{1}} E_{1} & \partial_{u} E_{1} \\
\partial_{\times_{1}} E_{2} & \partial_{u} E_{2}
\end{array}\right) .
$$

Set up the duplicated polynomial system $\mathcal{S}$, consisting in the 2 duplications of the polynomials $\left(E_{1}, E_{2}\right.$, Det, $\left.P\right)$ : it has 8 equations and unknowns.
Moreover, one of its solutions in $\overline{\mathbb{Q}}(t)^{8}$ is

$$
\mathcal{P}:=\left(F_{1}\left(t, U_{1}\right), F_{2}\left(t, U_{1}\right), F_{1}\left(t, U_{2}\right), F_{2}\left(t, U_{2}\right), U_{1}, U_{2}, F_{1}(t, 1), F_{2}(t, 1)\right)
$$

Compute an element of $\left\langle\mathcal{S}, m \cdot\left(U_{1}-U_{2}\right)-1\right\rangle \cap \mathbb{Q}\left[z_{0}, t\right]$.

## A polynomial system for systems of 2 DDEs of order 1

$$
\left\{\begin{array}{l}
F_{1}=f_{1}(u)+t \cdot Q_{1}\left(F_{1}, \Delta F_{1}, F_{2}, \Delta F_{2}, t, u\right)  \tag{SDDEs}\\
F_{2}=f_{2}(u)+t \cdot Q_{2}\left(F_{1}, \Delta F_{1}, F_{2}, \Delta F_{2}, t, u\right)
\end{array}\right.
$$

Define the "numerators" $E_{1}, E_{2}$ and the polynomials

$$
\text { Det }:=\operatorname{det}\left(\begin{array}{ll}
\partial_{\times_{1}} E_{1} & \partial_{\times_{2}} E_{1} \\
\partial_{\times_{1}} E_{2} & \partial_{\times_{2}} E_{2}
\end{array}\right) \quad \text { and } \quad P:=\operatorname{det}\left(\begin{array}{ll}
\partial_{x_{1}} E_{1} & \partial_{u} E_{1} \\
\partial_{\times_{1}} E_{2} & \partial_{u} E_{2}
\end{array}\right)
$$

Set up the duplicated polynomial system $\mathcal{S}$, consisting in the 2 duplications of the polynomials $\left(E_{1}, E_{2}\right.$, Det, $\left.P\right)$ : it has 8 equations and unknowns.
Moreover, one of its solutions in $\overline{\mathbb{Q}}(t)^{8}$ is

$$
\mathcal{P}:=\left(F_{1}\left(t, U_{1}\right), F_{2}\left(t, U_{1}\right), F_{1}\left(t, U_{2}\right), F_{2}\left(t, U_{2}\right), U_{1}, U_{2}, F_{1}(t, 1), F_{2}(t, 1)\right)
$$

Compute an element of $\left\langle\mathcal{S}, m \cdot\left(U_{1}-U_{2}\right)-1\right\rangle \cap \mathbb{Q}\left[z_{0}, t\right]$.

## Conclusion and perspectives

- Decidability: geometry-driven algorithm computing $R \in \mathbb{Q}[z, t] \backslash\{0\}$ s.t. $R\left(F_{1}(t, 1), t\right)=0$,
- 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 $R \in \mathbb{Q}[z, t] \backslash\{0\}$ s.t. $R\left(F_{1}(t, 1), t\right)=0$,
- 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)

November 27th $\rightarrow$ December 11th
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
Aggorithmic Complexity 
Workshop: September 25-29
Geometry of Polynomial System
Solving, Optimization and Topology
Special week: October 9-13
Topical days: October 23-24
Computer Algebra for Functional
Equations in Combinatorics & Physics
Workshop: Docember 4-8
Topical dyy: December 11
```



Frogar coordnated by the Centre Emile Borel (CEB) at HP (Paris) and aso accessbie onilim
Progam coord noted by the Centre Emile Borel (CBB) at HP (Paris)a
Partipation of postdocs and Pho sudents isstrongy ercouraged
Rogistration is thee how ever mandatary
 Deadine for financil support March 15", 2023

CEB orgarization assistart Sofia Minasian
CEB manager SMMe Lhernite
uwwip.f.

November 27th $\rightarrow$ December 1st,

- Workshop:

December 4th $\rightarrow$ December 8th,

- Topical day:

December 11th.

## Solving 5-constellations using a Hybrid Guess-and-Prove strategy

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

## Solving 5-constellations using a Hybrid Guess-and-Prove strategy

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

- 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 $F(t, 1) \bmod t^{55}, \quad 55=2 \cdot 9 \cdot 3+1$
- Guess $R \in \mathbb{Q}[z, t]$ such that $R(F(t, 1), t)=O\left(t^{(9+1) \cdot(3+1)-1}\right)$,
- Check that $R(t, F(t, 1))=O\left(t^{55}\right) . \quad(\Longrightarrow \mathrm{R}$ is satisfied $)$


## Solving 5-constellations using a Hybrid Guess-and-Prove strategy

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

- 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 $F(t, 1) \bmod t^{55}, \quad 55=2 \cdot 9 \cdot 3+1$
- Guess $R \in \mathbb{Q}[z, t]$ such that $R(F(t, 1), t)=O\left(t^{(9+1) \cdot(3+1)-1}\right)$,
- Check that $R(t, F(t, 1))=O\left(t^{55}\right) . \quad(\Longrightarrow \mathrm{R}$ is satisfied $)$
[Bostan, N., Safey El Din '23]
$\rightsquigarrow$ elimination strategy,
$\rightsquigarrow$ Newton iteration,
$\rightsquigarrow$ Hermite Padé approximants,
$\rightsquigarrow$ multiplicity lemma.


## Solving 5-constellations using a Hybrid Guess-and-Prove strategy

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

- 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 $F(t, 1) \bmod t^{55}, \quad 55=2 \cdot 9 \cdot 3+1$
- Guess $R \in \mathbb{Q}[z, t]$ such that $R(F(t, 1), t)=O\left(t^{(9+1) \cdot(3+1)-1}\right)$,
- Check that $R(t, F(t, 1))=O\left(t^{55}\right)$. $\quad(\Longrightarrow \mathrm{R}$ is satisfied $)$
[Bostan, N., Safey El Din '23]
$\rightsquigarrow$ elimination strategy,
$\rightsquigarrow$ Newton iteration,
$\rightsquigarrow$ Hermite Padé approximants,
$\rightsquigarrow$ multiplicity lemma.

| Strategy | Timing | $\left(\boldsymbol{d}_{\boldsymbol{z}}, \boldsymbol{d}_{\boldsymbol{t}}\right)$ |
| :---: | :---: | :---: |
| Elimination | 2 d 21 h | $(\mathbf{9}, \mathbf{3})$ |
| Hybrid G-P | $2 \mathrm{~h} 40 \min$ | $(5,2)$ |

## A polynomial system for systems of DDEs

## Consider

$$
\left\{\begin{array}{c}
F_{1}=f_{1}(u)+t \cdot Q_{1}\left(\nabla^{k} F_{1}, \ldots, \nabla^{k} F_{n}, t, u\right) \\
\vdots \\
F_{n}=f_{n}(u)+t \cdot Q_{n}\left(\nabla^{k} F_{1}, \ldots, \nabla^{k} F_{n}, t, u\right)
\end{array}\right.
$$

(SDDEs)

## A polynomial system for systems of DDEs

## Consider

$$
\left\{\begin{array}{c}
F_{1}=f_{1}(u)+t \cdot Q_{1}\left(\nabla^{k} F_{1}, \ldots, \nabla^{k} F_{n}, t, u\right) \\
\vdots \\
F_{n}= \\
\vdots
\end{array}\right.
$$

(SDDEs)

Perturbe (SDDEs) and define the "numerators" $E_{1}, \ldots, E_{n}$ and the polynomials
$\operatorname{Det}:=\operatorname{det}\left(\begin{array}{ccc}\partial_{x_{1}} E_{1} & \ldots & \partial_{x_{n}} E_{1} \\ \vdots & \ddots & \vdots \\ \partial_{x_{1}} E_{n} & \ldots & \partial_{x_{n}} E_{n}\end{array}\right)$

$$
\text { and } \quad P:=\operatorname{det}\left(\begin{array}{cccc}
\partial_{x_{1}} E_{1} & \ldots & \partial_{x_{n-1}} E_{1} & \partial_{u} E_{1} \\
\vdots & \ddots & \vdots & \vdots \\
\partial_{x_{1}} E_{n-1} & \ldots & \partial_{x_{n-1}} E_{n-1} & \partial_{u} E_{n-1} \\
\partial_{x_{1}} E_{n} & \ldots & \partial_{x_{n-1}} E_{n} & \partial_{u} E_{n}
\end{array}\right)
$$

## A polynomial system for systems of DDEs

## Consider

$$
\left\{\begin{array}{c}
F_{1}=f_{1}(u)+t \cdot Q_{1}\left(\nabla^{k} F_{1}, \ldots, \nabla^{k} F_{n}, t, u\right) \\
\vdots \\
F_{n}=f_{n}(u)+t \cdot Q_{n}\left(\nabla^{k} F_{1}, \ldots, \nabla^{k} F_{n}, t, u\right)
\end{array}\right.
$$

(SDDEs)

Perturbe (SDDEs) and define the "numerators" $E_{1}, \ldots, E_{n}$ and the polynomials
$\operatorname{Det}:=\operatorname{det}\left(\begin{array}{ccc}\partial_{x_{1}} E_{1} & \ldots & \partial_{x_{n}} E_{1} \\ \vdots & \ddots & \vdots \\ \partial_{x_{1}} E_{n} & \ldots & \partial_{x_{n}} E_{n}\end{array}\right) \quad$ and $\quad P:=\operatorname{det}\left(\begin{array}{cccc}\partial_{x_{1}} E_{1} & \ldots & \partial_{x_{n-1}} E_{1} & \partial_{u} E_{1} \\ \vdots & \ddots & \vdots & \vdots \\ \partial_{x_{1}} E_{n-1} & \ldots & \partial_{x_{n-1}} E_{n-1} & \partial_{u} E_{n-1} \\ \partial_{x_{1}} E_{n} & \ldots & \partial_{x_{n-1}} E_{n} & \partial_{u} E_{n}\end{array}\right)$,
Set up the duplicated polynomial system $\left(\mathcal{S}_{\text {dup }}\right)$, consisting in the $n k$ duplications of the polynomials $E_{1}, \ldots, E_{n}$, Det, $P$. It has $n k(n+2)$ variables and equations.

## A polynomial system for systems of DDEs

## Consider

$$
\left\{\begin{array}{c}
F_{1}=f_{1}(u)+t \cdot Q_{1}\left(\nabla^{k} F_{1}, \ldots, \nabla^{k} F_{n}, t, u\right) \\
\vdots \\
F_{n}=f_{n}(u)+t \cdot Q_{n}\left(\nabla^{k} F_{1}, \ldots, \nabla^{k} F_{n}, t, u\right)
\end{array}\right.
$$

(SDDEs)

Perturbe (SDDEs) and define the "numerators" $E_{1}, \ldots, E_{n}$ and the polynomials
$\operatorname{Det}:=\operatorname{det}\left(\begin{array}{ccc}\partial_{x_{1}} E_{1} & \ldots & \partial_{x_{n}} E_{1} \\ \vdots & \ddots & \vdots \\ \partial_{x_{1}} E_{n} & \ldots & \partial_{x_{n}} E_{n}\end{array}\right) \quad$ and $\quad P:=\operatorname{det}\left(\begin{array}{cccc}\partial_{x_{1}} E_{1} & \ldots & \partial_{x_{n-1}} E_{1} & \partial_{u} E_{1} \\ \vdots & \ddots & \vdots & \vdots \\ \partial_{x_{1}} E_{n-1} & \ldots & \partial_{x_{n-1}} E_{n-1} & \partial_{u} E_{n-1} \\ \partial_{x_{1}} E_{n} & \ldots & \partial_{x_{n-1}} E_{n} & \partial_{u} E_{n}\end{array}\right)$,
Set up the duplicated polynomial system $\left(\mathcal{S}_{\text {dup }}\right)$, consisting in the $n k$ duplications of the polynomials $E_{1}, \ldots, E_{n}$, Det, $P$. It has $n k(n+2)$ variables and equations.

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

