Thomas Decomposition and its Applications

Thomas Bächler, Vladimir Gerdt, Markus Lange-Hegermann, Wilhelm Plesken, Daniel Robertz
Lehrstuhl B für Mathematik, RWTH Aachen; Joint Institute for Nuclear Research, Dubna

Algebraic Simple Systems

- K field of characteristic 0, $R := K[x_1, \ldots, x_n]$ with ranking $x_1 < \ldots < x_n$.
- A system S of **equations** and **inequations** in R is **simple**, if $\forall x$

① S contains at most one $S_x \in R$ with highest variable x (**triangularity**).

② If $\mathbf{s}$ solves $\{S_y \mid y < x\}$ then $S_x(\mathbf{s}, x)$ has $\deg_x(S_x)$ **distinct zeroes** in $\overline{K}$.

Thomas Algorithm for Disjoint Decomposition

- Denote the set of solutions of a system T in $\overline{K}$ by $\mathcal{L}(T)$. A family of systems $(S_i)_{i=1}^m$ is called **disjoint decomposition** of T if $\mathcal{L}(T) = \biguplus_{i=1}^m \mathcal{L}(S_i)$.
- The Thomas **algorithm** uses **pseudo remainders** and **subresultants** to compute a **disjoint** (Thomas) **decomposition into simple systems**.

Strict Treatment of Inequations

All zeroes of **inequations** have to be removed from the solution set. This requires them to be treated *similarly to the equations*. For example, consider the system $S := \{p = 0, q \neq 0\} = \{x^2 - x + 1 = 0, x + a \neq 0\}$. For almost all values $\widetilde{a}$, $S_{|a=\widetilde{a}}$ has two distinct zeroes, exceptions determined by $r(\widetilde{a}) = 0$, where $r = \mathrm{res}(p, q, x) = a^2 + a + 1$. Use r to decompose S into the simple systems $\{p = 0, r \neq 0\}$ and $\{x - a - 1 = 0, r = 0\}$.

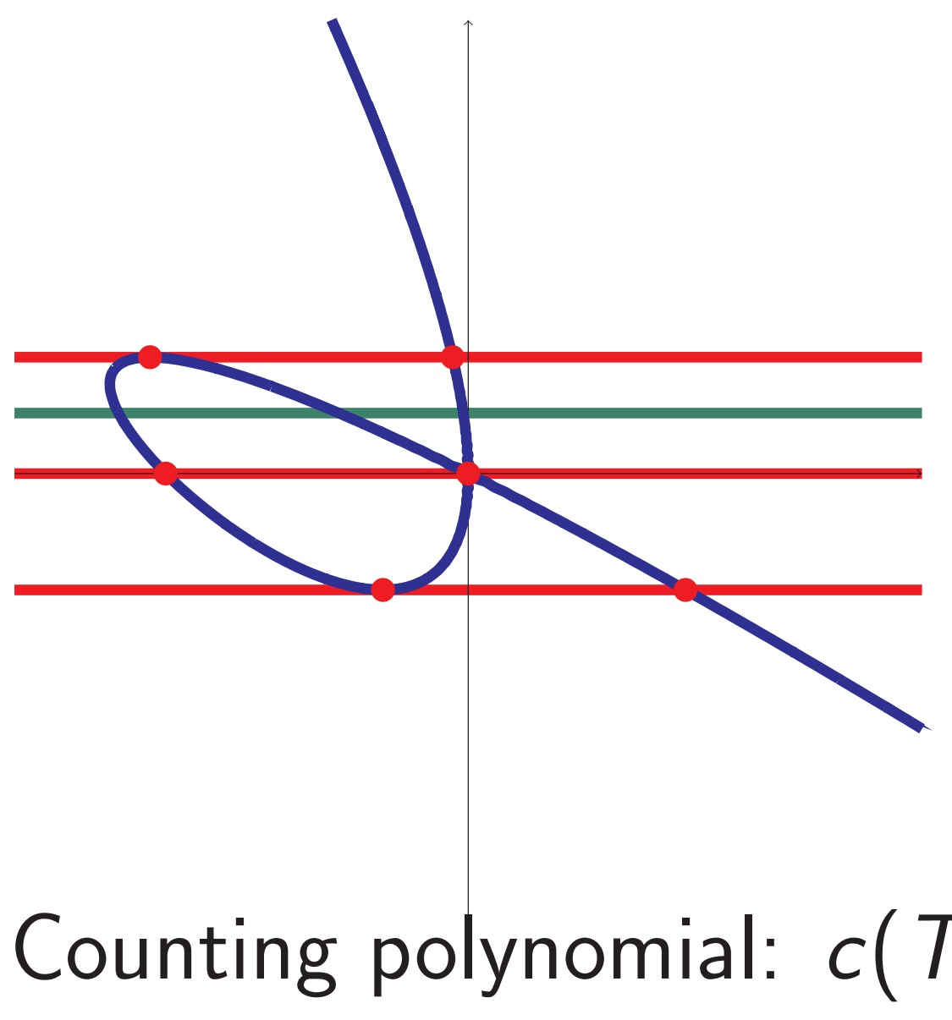
Counting Solutions

A simple system S has **type** $(\tau(S_{x_1}), \ldots, \tau(S_{x_n}))$ with

$$\tau(S_x) := \begin{cases} \deg_x(S_x) & \text{if } S_x \text{ is an equation} \\ \infty - \deg_x(S_x) & \text{if } S_x \text{ is an inequation} \\ \infty & \text{if } S_x \text{ is empty} \end{cases}$$

and **counting polynomial** $c(S) := \prod_{i=1}^n \tau(S_{x_i}) \in \mathbb{Z}[\infty]$. For a system T, $c(T) := \sum_{i=1}^m c(S_i)$ for *any* Thomas decomposition $(S_i)_{i=1}^m$ of T.

Example: Thomas Decomposition and Counting Polynomial

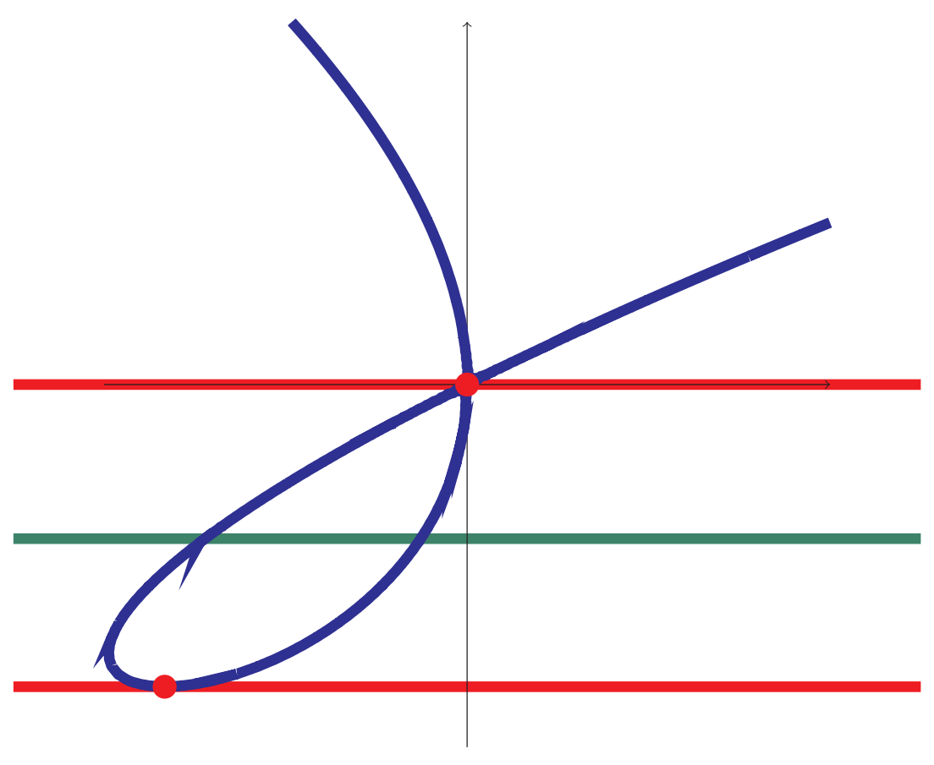


1) Consider $p := x^3 + 3x^2y + 3xy^2 + y^3 + x^2 + 2xy$.
Decompose T:=$\{p = 0\}$ into

$$S_1 := \{p = x^3 + \ldots = 0, \mathrm{disc}_x(p) = y^3 + \ldots \neq 0\}$$
$$S_2 := \{x^2 + \ldots = 0, \mathrm{disc}_x(p) = y^3 + \ldots = 0\}$$

The **fibres** of $\pi : \mathcal{L}(\{p = 0\}) \to \overline{K} : (x, y) \mapsto y$ satisfy $|\pi^{-1}(y)| = 3$ on S_1 and $|\pi^{-1}(y)| = 2$ on S_2.

Counting polynomial: $c(T) = c(S_1) + c(S_2) = 3(\infty - 3) + 2 \cdot 3 = 3\infty - 3$.



2) The polynomial $q = y^3 - x^2 + 2xy$ yields the decomposition $(\{q = x^2 + \ldots = 0, y^2 + \ldots \neq 0\}, \{x^2 + \ldots = 0, y^2 + \ldots = 0\})$ and thus the counting polynomial $2\infty - 2$.

3) A coordinate transformation of p yields q. Thus the counting polynomial is coordinate-dependent. However, in almost all coordinates it equals $c(T)$: the **generic counting polynomial**.

Counting over Finite Fields

- Under certain conditions, a Thomas decomposition over extensions of $\mathbb{Q}$ can be used to count solutions over an arbitrary finite field F.
- **Example**: A Thomas decomposition of $X^T \omega X = \omega$ for the symplectic form ω over $\mathbb{Q}[X_{ij} | 1 \leq i, j \leq 4]$ yields $|Sp(4, F)| = |F|^{10} - |F|^8 - |F|^6 + |F|^4$.

Implementation

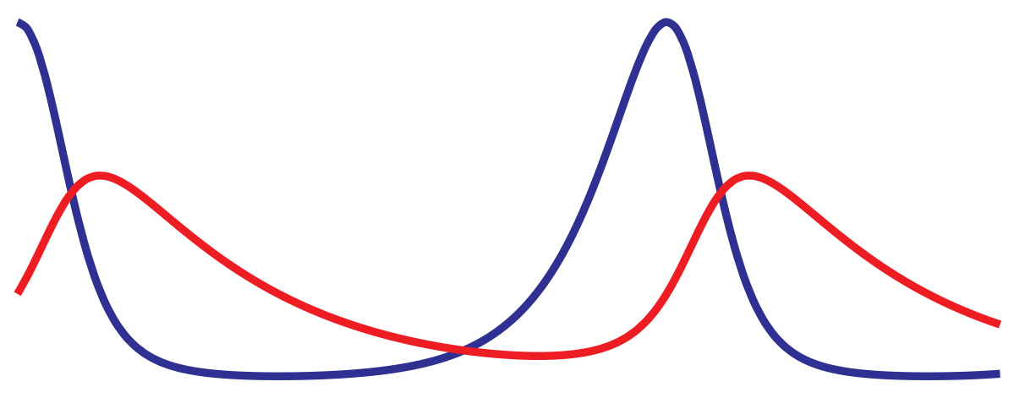
The Thomas decomposition is implemented in the Maple packages `AlgebraicThomas` and `DifferentialThomas`, available at

`http://wwwb.math.rwth-aachen.de/thomasdecomposition/`

Differential Thomas Decomposition

- Treat **differential-algebraic systems** as *algebraic systems* for the **jets**.
- The Thomas ∂-**decomposition** makes systems algebraically **simple** and **involutive** in the sense of Janet.

Parameter Identification



The numbers $y(t)$ of **predator** and $x(t)$ of **prey** interacting in a closed biological system are modelled by the Lotka-Volterra-equations

$$\dot{x}(t) = x(t)\,(\alpha - \beta y(t))\,,\ \dot{y}(t) = -y(t)\,(\gamma - \delta x(t))\,,$$

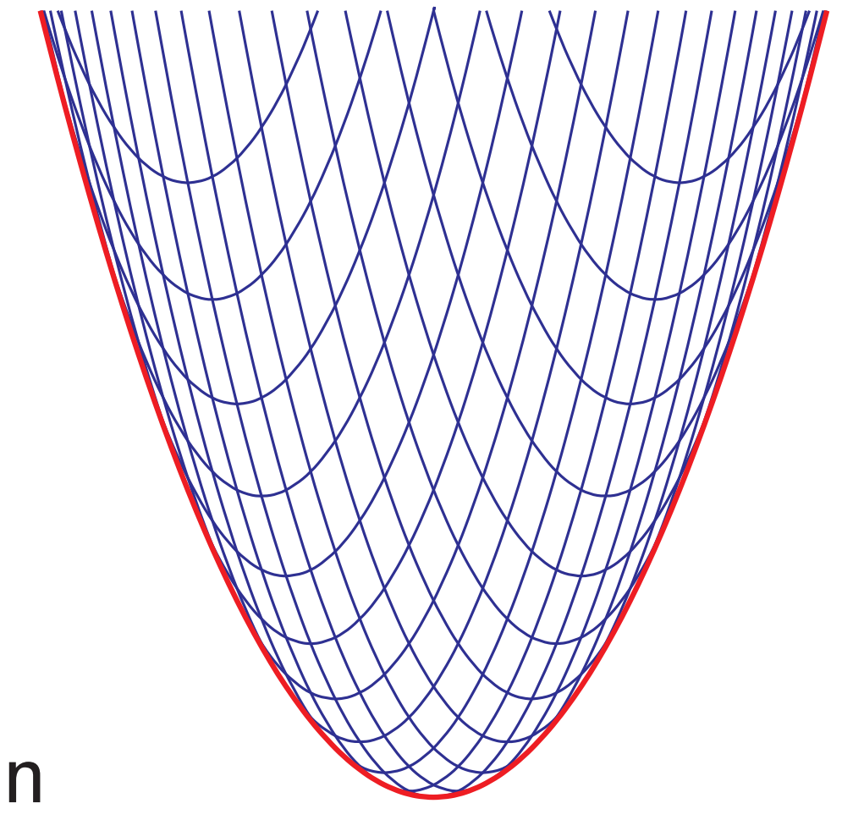
where $\alpha, \beta, \gamma, \delta \in \mathbb{R}$ represent real parameters. By using an **elimination ranking** $\alpha, \beta, \gamma, \delta \gg x, y$, express α, β, γ and δ in $x(t)$ and $y(t)$ to compute them from *empirical data*. In addition to the **generic result**

$$\alpha = \ldots,\ \beta = -\frac{x(t)\ddot{x}(t) - \dot{x}(t)^2}{x(t)^2\dot{y}(t)}, \gamma = \ldots,\ \text{and } \delta = \frac{y(t)\ddot{y}(t) - \dot{y}(t)^2}{y(t)^2\dot{x}(t)}$$

the Thomas ∂-decomposition also computes **degenerate** cases.

Counting Solutions of Differential Systems

- ∂-**counting polynomial** as a generalization of (i) Hilbert series for linear PDEs, (ii) ∂-dimension polynomial, & (iii) the algebraic counting polynomial.
- **Example:** Count $T := \{y(t) = \sum_{i=0}^\infty a_i t^i \mid \dot{y}^2 - 4t\dot{y} + 8t^2 - 4y = 0\}$.
  The ∂-decomposition splits the system into $\{y \mid \dot{y}^2 - 4t\dot{y} + 8t^2 - 4y, y \neq t^2\}$ and $\{y \mid y = t^2\}$ with counting polynomial $2(\infty - 1) + 1$ corresponding to each possible 0th Taylor coefficient a_0, which leads to two functions except one singular choice.

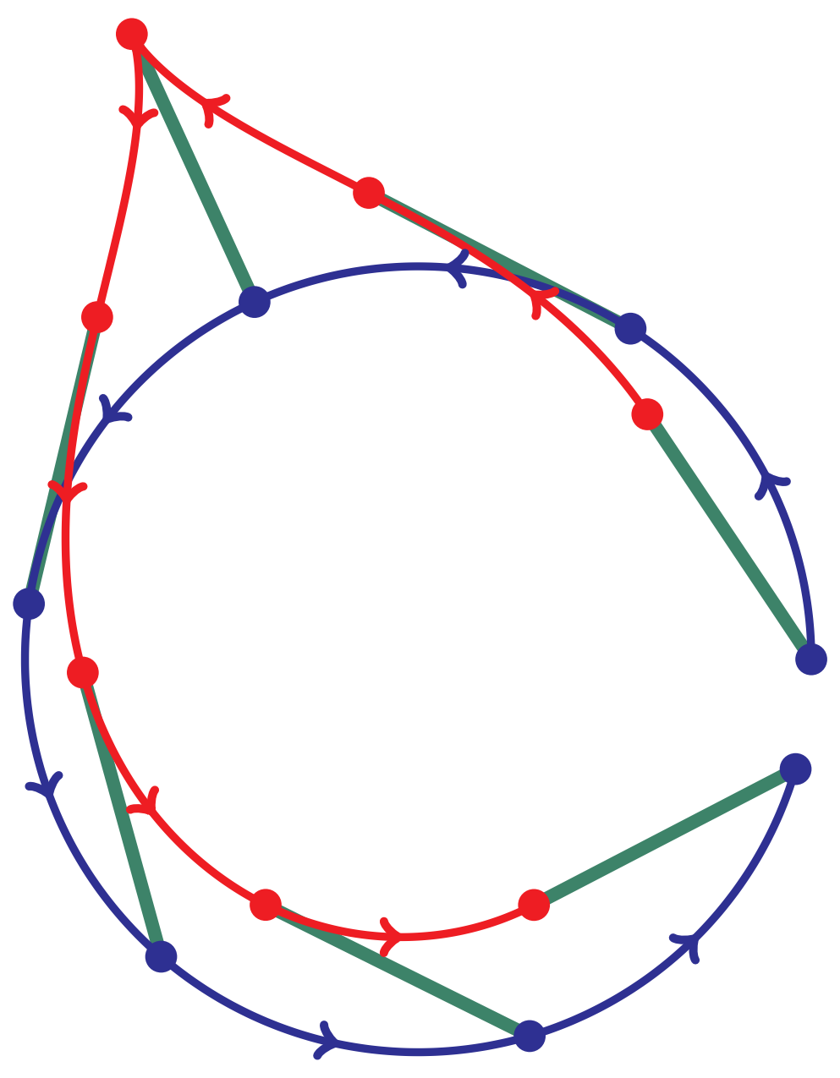


- Plan: Make it *algorithmic* via extended ∂-decomposition by translating inequations for functions to ones for Taylor coefficients.
  Example: $S = \{\ddot{y} = 0,\ y \neq 0\}$ is solved by $\{a \cdot t + b \mid (a,b) \neq (0,0)\}$. The leaders suggest $c(S) = \infty \cdot (\infty - 1)$ instead of the correct $c(S) = \infty^2 - 1$.
  Application: Check generality of results of a PDE solver.

Solutions of PDE-Systems of Special Form

- Use ∂-decomposition to **check completeness of the solution returned by symbolic PDE-solvers** via splitting and counting.
- **Example**: Consider $F(u) := \left(\frac{\partial^2 u}{\partial x^2}\right)^2 + \frac{\partial^2 u}{\partial y^2} + \frac{\partial u}{\partial x} + \frac{\partial u}{\partial y} = 0$ for $u = u(x, y)$.
  Maple (`pdsolve`) gives the solutions $f(x) + g(y)$ with some constraints.
  The ∂-decomposition of $\{F(u)\}$ gives a solution $\tilde{u}(x, y) := (x + y + 1)e^{-y}$.
  The PDE $p(v) := \frac{\partial^2 v}{\partial x \partial y} = 0$ characterizes analytic functions of the form $f(x) + g(y)$. The solution $\tilde{u}$ is not found by `pdsolve`, since $p(\tilde{u}) \neq 0$.

Automatic Theorem Proving



Theorem: Let $(X(t), Y(t))$ be the **template curve** with **tractrix** $(x(t), y(t))$ for distance $d > 0$ and nondegeneracy condition $\dot{x}\dot{Y} - \dot{X}\dot{y} \neq 0$. The **evolute** of the tractrix is given by the intersection points of the normals of $(X(t), Y(t))$ and $(x(t), y(t))$.

Proof: Compute the Thomas ∂-decomposition of

$$(X(t) - x(t))^2 + (Y(t) - y(t))^2 - d^2 = 0$$
$$\dot{y}(t)(X(t) - x(t)) + \dot{x}(t)(Y(t) - y(t)) = 0$$

and the **inequation** $\dot{x}\dot{Y} - \dot{X}\dot{y} \neq 0$ describing the connection of template and tractrix. Symbolically compute the intersection a of the normals of template and tractrix and compute the evolute b from the definition as envelope of the normals. The difference $a(t) - b(t)$ of these curves **reduces to zero** w.r.t. *all* systems of the above decomposition. □

Lehrstuhl B für Mathematik - RWTH Aachen University - Aachen, Germany; Joint Institute for Nuclear Research - Dubna, Russia