# Algorithms for Computing Triangular Decompositions of Polynomial Systems

Changbo Chen and Marc Moreno Maza

ORCCA, University of Western Ontario, Canada

ISSAC 2011
June 11, 2011

# Gauss elimination and Gröbner basis

Variable order : $z > y > x$.

## Linear

$$\begin{cases} 2x + y + z - 1 = 0 \\ x + 2y + z - 1 = 0 \\ x + y + 2z - 1 = 0 \end{cases} \Rightarrow \begin{cases} 4z - 1 = 0 \\ 4y - 1 = 0 \\ 4x - 1 = 0 \end{cases}$$

## Nonlinear

$$\begin{cases} x^2 + y + z - 1 = 0 \\ x + y^2 + z - 1 = 0 \\ x + y + z^2 - 1 = 0 \end{cases} \Rightarrow \begin{cases} z + y + x^2 - 1 & = & 0 \\ y^2 - y - x^2 + x & = & 0 \\ 2x^2y + x^4 - x^2 & = & 0 \\ x^6 - 4x^4 + 4x^3 - x^2 & = & 0 \end{cases}$$

# Triangular decomposition

## Input system

$$\begin{aligned} x^2 + y + z - 1 &= 0 \\ x + y^2 + z - 1 &= 0 \\ x + y + z^2 - 1 &= 0 \end{aligned}$$

## A triangular decomposition

$$\left\{ \begin{array}{r} z - x = 0 \\ y - x = 0 \\ x^2 + 2x - 1 = 0 \end{array} \right. \quad \left\{ \begin{array}{r} z = 0 \\ y = 0 \\ x - 1 = 0 \end{array} \right. \quad \left\{ \begin{array}{r} z = 0 \\ y - 1 = 0 \\ x = 0 \end{array} \right. \quad \left\{ \begin{array}{r} z - 1 = 0 \\ y = 0 \\ x = 0 \end{array} \right.$$

# A breif historical review

## Theory

- Characteristic set of a prime ideal (J.F. Ritt, 1930s).
- Characteristic set of a polynomial system (W.T. Wu, 1970s)
- Regular chain (M. Kalkbrener) (L. Yang and J.Z. Zhang), 1990s
- Unification of different concepts (P. Aubry, D. Lazard and M. Moreno Maza, 1999).

## Algorithm

(J.F. Ritt 1930s, W.T. Wu, 1970s, M. Kalkbrener 1991, D. Lazard 1991-1992, D.M. Wang 1993-1998-2000, Triade algorithm, M. Moreno Maza 2000)

## Software

Epsilon (D.M. Wang), Wsolve (D.K. Wang), RegularChains (initialized by F. Lemaire, M. Moreno Maza and Y. Xie) library in Maple.

# Application of triangular decomposition

- Differential systems (F. Boulier, D. Lazard, F. Ollivier, and M. Petitot 1995, É. Hubert 2000)
- Difference systems (X.S. Gao, J. Van der Hoeven, Y. Luo, and C. Yuan 2009)
- Real parametric systems (L. Yang, X.R. Hou and B. Xia 2001)
- Primary decomposition (T. Shimoyama and K. Yokoyama 1996)
- Cylindrical algebraic decomposition (C. Chen, M. Moreno Maza, B. Xia and L. Yang 2009)
- Semi-algebraic systems (C. Chen, J.H. Davenport, J.P. May , M. Moreno Maza, B. Xia, and R. Xiao 2010)

# Classification of existing algorithms

**By specification**

- encode all the zeros of $F$

$$V(F) = \cup_{i=1}^{e} W(T_i)$$

- represent only the "generic zeros"

$$V(F) = \cup_{i=1}^{e} \overline{W(T_i)}$$

**By algorithmic principle**

- variable elimination

$$\mathrm{Solve}_n(F \subset \mathbf{k}[x_1, \ldots, x_{n-1}, x_n]) \to \mathrm{Solve}_{n-1}(F' \subset \mathbf{k}[x_1, \ldots, x_{n-1}])$$

- equation elimination (incremental solving)

$$\mathrm{Solve}_m(\{f_1, \ldots, f_{m-1}, f_m\}) \to \mathrm{Solve}_{m-1}(\{f_1, \ldots, f_{m-1}\})$$

# Contribution of this paper

## Avoid unnecessary computations

- Weakened notion of regular GCD
- Less regularity test

## Recycle necessary computations

- recycling subresultant chains

# Contribution of this paper

## Avoid unnecessary computations

- Weakened notion of regular GCD
- Less regularity test

## Recycle necessary computations

- recycling subresultant chains

## Contribution of this paper

# Avoid unnecessary computations

- Weakened notion of regular GCD
- Less regularity test

# Recycle necessary computations

- recycling subresultant chains

# Contribution of this paper

## Avoid unnecessary computations

- Weakened notion of regular GCD
- Less regularity test

## Recycle necessary computations

- recycling subresultant chains

# Contribution of this paper

## Avoid unnecessary computations

- Weakened notion of regular GCD
- Less regularity test

## Recycle necessary computations

- recycling subresultant chains

# Plan

# Plan

# Set up

- polynomial ring $R = \mathbf{k}[x_1 < \cdots < x_n]$
- polynomial $p \in R$
- $\mathrm{mvar}(p)$ : largest variable appearing in $p$
- $\mathrm{init}(p)$ : leading coefficient of $p$ w.r.t. $\mathrm{mvar}(p)$

- a polynomial set $T \subset R$
- $T$ is a triangular set if $\mathrm{mvar}(p) \neq \mathrm{mvar}(q)$ for all $p \neq q \in T$
- $\mathrm{init}(T)$: the product of the initials of polynomials in $T$
- $\mathrm{sat}(T) := \langle T \rangle : \mathrm{init}(T)^{\infty}$

- an element $p \neq 0$ of a ring $\mathbb{A}$ is regular if $p$ is not a zerodivisor in $\mathbb{A}$
- a triangular set $T$ is a regular chain if $\mathrm{init}(T)$ is regular in $R/\mathrm{sat}(T)$

# Set up

- polynomial ring $R = \mathbf{k}[x_1 < \cdots < x_n]$
- polynomial $p \in R$
- $\mathrm{mvar}(p)$ : largest variable appearing in $p$
- $\mathrm{init}(p)$ : leading coefficient of $p$ w.r.t. $\mathrm{mvar}(p)$

- a polynomial set $T \subset R$
- $T$ is a triangular set if $\mathrm{mvar}(p) \neq \mathrm{mvar}(q)$ for all $p \neq q \in T$
- $\mathrm{init}(T)$: the product of the initials of polynomials in $T$
- $\mathrm{sat}(T) := \langle T \rangle : \mathrm{init}(T)^{\infty}$

- an element $p \neq 0$ of a ring $\mathbb{A}$ is regular if $p$ is not a zerodivisor in $\mathbb{A}$
- a triangular set $T$ is a regular chain if $\mathrm{init}(T)$ is regular in $R/\mathrm{sat}(T)$

# Set up

- polynomial ring $R = \mathbf{k}[x_1 < \cdots < x_n]$
- polynomial $p \in R$
- $\mathrm{mvar}(p)$ : largest variable appearing in $p$
- $\mathrm{init}(p)$ : leading coefficient of $p$ w.r.t. $\mathrm{mvar}(p)$

- a polynomial set $T \subset R$
- $T$ is a triangular set if $\mathrm{mvar}(p) \neq \mathrm{mvar}(q)$ for all $p \neq q \in T$
- $\mathrm{init}(T)$: the product of the initials of polynomials in $T$
- $\mathrm{sat}(T) := \langle T \rangle : \mathrm{init}(T)^{\infty}$

- an element $p \neq 0$ of a ring $\mathbb{A}$ is regular if $p$ is not a zerodivisor in $\mathbb{A}$
- a triangular set $T$ is a regular chain if $\mathrm{init}(T)$ is regular in $R/\mathrm{sat}(T)$

# Set up

- polynomial ring $R = \mathbf{k}[x_1 < \cdots < x_n]$
- polynomial $p \in R$
- $\mathrm{mvar}(p)$ : largest variable appearing in $p$
- $\mathrm{init}(p)$ : leading coefficient of $p$ w.r.t. $\mathrm{mvar}(p)$

- a polynomial set $T \subset R$
- $T$ is a triangular set if $\mathrm{mvar}(p) \neq \mathrm{mvar}(q)$ for all $p \neq q \in T$
- $\mathrm{init}(T)$: the product of the initials of polynomials in $T$
- $\mathrm{sat}(T) := \langle T \rangle : \mathrm{init}(T)^{\infty}$

- an element $p \neq 0$ of a ring $\mathbb{A}$ is regular if $p$ is not a zerodivisor in $\mathbb{A}$
- a triangular set $T$ is a regular chain if $\mathrm{init}(T)$ is regular in $R/\mathrm{sat}(T)$

# Set up

- polynomial ring $R = \mathbf{k}[x_1 < \cdots < x_n]$
- polynomial $p \in R$
- $\mathrm{mvar}(p)$ : largest variable appearing in $p$
- $\mathrm{init}(p)$ : leading coefficient of $p$ w.r.t. $\mathrm{mvar}(p)$

- a polynomial set $T \subset R$
- $T$ is a triangular set if $\mathrm{mvar}(p) \neq \mathrm{mvar}(q)$ for all $p \neq q \in T$
- $\mathrm{init}(T)$: the product of the initials of polynomials in $T$
- $\mathrm{sat}(T) := \langle T \rangle : \mathrm{init}(T)^\infty$

- an element $p \neq 0$ of a ring $\mathbb{A}$ is regular if $p$ is not a zerodivisor in $\mathbb{A}$
- a triangular set $T$ is a regular chain if $\mathrm{init}(T)$ is regular in $R/\mathrm{sat}(T)$

# Set up

- polynomial ring $R = \mathbf{k}[x_1 < \cdots < x_n]$
- polynomial $p \in R$
- $\mathrm{mvar}(p)$ : largest variable appearing in $p$
- $\mathrm{init}(p)$ : leading coefficient of $p$ w.r.t. $\mathrm{mvar}(p)$

- a polynomial set $T \subset R$
- $T$ is a triangular set if $\mathrm{mvar}(p) \neq \mathrm{mvar}(q)$ for all $p \neq q \in T$
- $\mathrm{init}(T)$: the product of the initials of polynomials in $T$
- $\mathrm{sat}(T) := \langle T \rangle : \mathrm{init}(T)^{\infty}$

- an element $p \neq 0$ of a ring $\mathbb{A}$ is regular if $p$ is not a zerodivisor in $\mathbb{A}$
- a triangular set $T$ is a regular chain if $\mathrm{init}(T)$ is regular in $R/\mathrm{sat}(T)$

# Set up

- polynomial ring $R = \mathbf{k}[x_1 < \cdots < x_n]$
- polynomial $p \in R$
- $\mathrm{mvar}(p)$ : largest variable appearing in $p$
- $\mathrm{init}(p)$ : leading coefficient of $p$ w.r.t. $\mathrm{mvar}(p)$

- a polynomial set $T \subset R$
- $T$ is a triangular set if $\mathrm{mvar}(p) \neq \mathrm{mvar}(q)$ for all $p \neq q \in T$
- $\mathrm{init}(T)$: the product of the initials of polynomials in $T$
- $\mathrm{sat}(T) := \langle T \rangle : \mathrm{init}(T)^{\infty}$

- an element $p \neq 0$ of a ring $\mathbb{A}$ is regular if $p$ is not a zerodivisor in $\mathbb{A}$
- a triangular set $T$ is a regular chain if $\mathrm{init}(T)$ is regular in $R/\mathrm{sat}(T)$

# Set up

- polynomial ring $R = \mathbf{k}[x_1 < \cdots < x_n]$
- polynomial $p \in R$
- $\mathrm{mvar}(p)$ : largest variable appearing in $p$
- $\mathrm{init}(p)$ : leading coefficient of $p$ w.r.t. $\mathrm{mvar}(p)$

- a polynomial set $T \subset R$
- $T$ is a triangular set if $\mathrm{mvar}(p) \neq \mathrm{mvar}(q)$ for all $p \neq q \in T$
- $\mathrm{init}(T)$: the product of the initials of polynomials in $T$
- $\mathrm{sat}(T) := \langle T \rangle : \mathrm{init}(T)^{\infty}$

- an element $p \neq 0$ of a ring $\mathbb{A}$ is regular if $p$ is not a zerodivisor in $\mathbb{A}$
- a triangular set $T$ is a regular chain if $\mathrm{init}(T)$ is regular in $R/\mathrm{sat}(T)$

# Set up

- polynomial ring $R = \mathbf{k}[x_1 < \cdots < x_n]$
- polynomial $p \in R$
- $\mathrm{mvar}(p)$ : largest variable appearing in $p$
- $\mathrm{init}(p)$ : leading coefficient of $p$ w.r.t. $\mathrm{mvar}(p)$

- a polynomial set $T \subset R$
- $T$ is a triangular set if $\mathrm{mvar}(p) \neq \mathrm{mvar}(q)$ for all $p \neq q \in T$
- $\mathrm{init}(T)$: the product of the initials of polynomials in $T$
- $\mathrm{sat}(T) := \langle T \rangle : \mathrm{init}(T)^{\infty}$

- an element $p \neq 0$ of a ring $\mathbb{A}$ is regular if $p$ is not a zerodivisor in $\mathbb{A}$
- a triangular set $T$ is a regular chain if $\mathrm{init}(T)$ is regular in $R/\mathrm{sat}(T)$

# Set up

- polynomial ring $R = \mathbf{k}[x_1 < \cdots < x_n]$
- polynomial $p \in R$
- $\mathrm{mvar}(p)$ : largest variable appearing in $p$
- $\mathrm{init}(p)$ : leading coefficient of $p$ w.r.t. $\mathrm{mvar}(p)$

- a polynomial set $T \subset R$
- $T$ is a triangular set if $\mathrm{mvar}(p) \neq \mathrm{mvar}(q)$ for all $p \neq q \in T$
- $\mathrm{init}(T)$: the product of the initials of polynomials in $T$
- $\mathrm{sat}(T) := \langle T \rangle : \mathrm{init}(T)^{\infty}$

- an element $p \neq 0$ of a ring $\mathbb{A}$ is regular if $p$ is not a zerodivisor in $\mathbb{A}$
- a triangular set $T$ is a regular chain if $\mathrm{init}(T)$ is regular in $R/\mathrm{sat}(T)$

# Set up

- polynomial ring $R = \mathbf{k}[x_1 < \cdots < x_n]$
- polynomial $p \in R$
- $\mathrm{mvar}(p)$ : largest variable appearing in $p$
- $\mathrm{init}(p)$ : leading coefficient of $p$ w.r.t. $\mathrm{mvar}(p)$

- a polynomial set $T \subset R$
- $T$ is a triangular set if $\mathrm{mvar}(p) \neq \mathrm{mvar}(q)$ for all $p \neq q \in T$
- $\mathrm{init}(T)$: the product of the initials of polynomials in $T$
- $\mathrm{sat}(T) := \langle T \rangle : \mathrm{init}(T)^{\infty}$

- an element $p \neq 0$ of a ring $\mathbb{A}$ is regular if $p$ is not a zerodivisor in $\mathbb{A}$
- a triangular set $T$ is a regular chain if $\mathrm{init}(T)$ is regular in $R/\mathrm{sat}(T)$

# Regular chain

**Example**

$$T := \begin{cases} t_2 = (x_1 + x_2){x_3}^2 + x_3 + 1 \\ t_1 = {x_1}^2 - 2. \end{cases}$$

Under the order $x_3 > x_2 > x_1$,

- $\mathrm{mvar}(t_2) = x_3$ and $\mathrm{init}(t_2) = x_1 + x_2$
- $\mathrm{init}(t_2)$ is regular modulo $\langle t_1 \rangle : 1^\infty$
- $T$ is a regular chain
- quasi-component of $T$: $W(T) = V(T) \setminus V(\mathrm{init}(t_2)\mathrm{init}(t_1))$.

**Proposition**

*Let $T$ be a regular chain. Then $\mathrm{sat}(T)$ is a proper equi-dimensional ideal. Moreover, $V(\mathrm{sat}(T)) = \overline{W(T)}$.*

# Triangular decomposition of an algebraic variety

### Kalkbrener triangular decomposition

Let $F \subset \mathbf{k}[\mathbf{x}]$. A family of regular chains $T_1, \ldots, T_e$ of $\mathbf{k}[\mathbf{x}]$ is called a Kalkbrener triangular decomposition of $V(F)$ if

$$V(F) = \cup_{i=1}^{e} V(\mathrm{sat}(T_i)).$$

### Lazard-Wu triangular decomposition

Let $F \subset \mathbf{k}[\mathbf{x}]$. A family of regular chains $T_1, \ldots, T_e$ of $\mathbf{k}[\mathbf{x}]$ is called a Lazard-Wu triangular decomposition of $V(F)$ if

$$V(F) = \cup_{i=1}^{e} W(T_i).$$

# Plan

# Regular GCD

## Definition (M. Moreno Maza, 2000)

- $\mathbb{A}$: be a commutative ring with unity.
- $p, t \in \mathbb{A}[y] \setminus \mathbb{A}$.

We say that $g \in \mathbb{A}[y]$ is a *regular GCD* of $p, t$ if:

($R_1$) $\mathrm{lc}(g, y)$ is a regular element in $\mathbb{A}$;

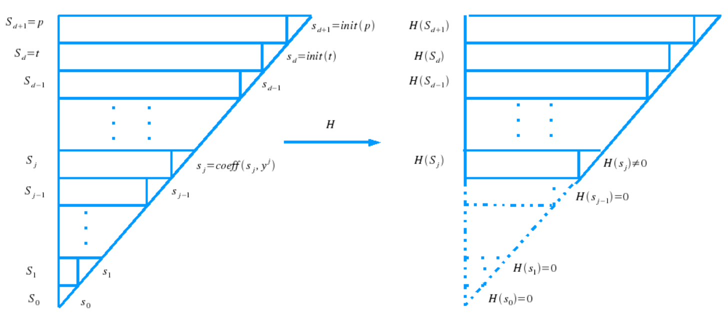
($R_2$) $g \in \langle p, t \rangle$ in $\mathbb{A}[y]$;

($R_3$) if $\deg(g, y) > 0$, then $\mathrm{prem}(p, g) = \mathrm{prem}(t, g) = 0$.

## Remark

- If $\mathbb{A}$ is a field, the definition coincides with the usual notion of a GCD.
- Let $R = \mathbf{k}[x_1, \ldots, x_{k-1}]$ and let $T$ be a regular chain of $R$.
- In (M. Moreno Maza, 2000), $\mathbb{A} = R/\mathrm{sat}(T)$.
- In this study, $\mathbb{A} = R/\sqrt{\mathrm{sat}(T)}$.

# Specialization properties of subresultants




## Theorem

Let $H$ be a homomorphism from a ring $R$ to a field $\mathbb{L}$. Let $p, t \in R[y]$. Let $j$ be the smallest integer s.t. $H(s_j) \neq 0$. Then $H(S_j) = \gcd(H(p), H(t))$.

# Computing regular GCD via subresultants

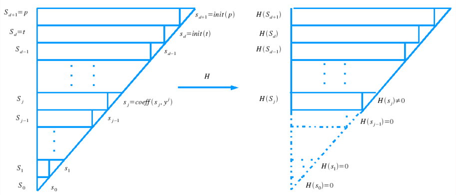
- Let $T$ be a regular chain of a polynomial ring $R$.
- Let $p, t \in R[y]$ with positive degrees in $y$.
- Let $\mathbb{A} = R/\sqrt{\mathrm{sat}(T)}$.

## Theorem

Let $j$ be an integer such that $s_j$ is regular in $\mathbb{A}$ and $s_i = 0$ in $\mathbb{A}$ for any $0 \le i < j$, then $S_j$ is a regular GCD of $p$ and $t$ in $\mathbb{A}[x_k]$.

## Proof

- Let $\mathfrak{p} \in \mathrm{Ass}(\mathrm{sat}(T))$.
- Let $\mathbb{L} := \mathrm{fr}(\mathrm{R}/\mathfrak{p})$
- $R \xrightarrow{H} \mathbb{L}$.
- $H(S_j) = \gcd(H(p), H(t)$ in $\mathbb{L}[x_k]$.



# Properties of Regular GCD

- Let $R := \mathbf{k}[x_1, \ldots, x_{k-1}]$, where $1 \leq k \leq n$.
- Let $T \subset \mathbf{k}[x_1, \ldots, x_{k-1}]$ be a regular chain.
- Let $p, t, g \in R[x_k]$ be polynomials with main variable $x_k$.

## Proposition

*Assume* $T \cup \{t\}$ *is a regular chain and* $g$ *is a regular GCD of* $p$ *and* $t$ *in* $R[x_k]/\sqrt{\mathrm{sat}(T)}$. *We have:*

$$\begin{array}{rcl} V(p) \cap W(T \cup t) & \subseteq & W(T \cup g) \cup V(\{p, h_g\}) \cap W(T \cup t) \\ & \subseteq & V(p) \cap \overline{W(T \cup t)}. \end{array}$$

Generally, $V(p) \cap W(T \cup t) \subseteq \cup_{i=1}^{e} W(T_i \cup g_i) \subseteq V(p) \cap \overline{W(T \cup t)}$, where $g_i$ is a regular GCD of $p$ and $t$ in $R[x_k]/\sqrt{\mathrm{sat}(T_i)}$.

# Plan

# Incremental algorithm and intersect operation

## Intersect operation

- Let $R = \mathbf{k}[x_1 < \cdots < x_n]$.
- Let $p \in R$ and $T$ be a regular chain of $R$.
- Intersect$(p, T, R)$ returns regular chains $T_1, \ldots, T_e \subset R$ such that

$$V(p) \cap W(T) \subseteq W(T_1) \cup \cdots \cup W(T_e) \subseteq V(p) \cap \overline{W(T)}.$$

## Triangularize$(F, R)$

- **if** $F = \{\ \}$ **then** return $\{\varnothing\}$
- Choose a polynomial $p \in F$ with maximal rank
- **for** $T \in$ Triangularize$(F \setminus \{p\}, R)$ **do**
  output Intersect$(p, T, R)$
  **end**

# Incremental algorithm and intersect operation

## Intersect operation

- Let $R = \mathbf{k}[x_1 < \cdots < x_n]$.
- Let $p \in R$ and $T$ be a regular chain of $R$.
- Intersect$(p, T, R)$ returns regular chains $T_1, \ldots, T_e \subset R$ such that

$$V(p) \cap W(T) \subseteq W(T_1) \cup \cdots \cup W(T_e) \subseteq V(p) \cap \overline{W(T)}.$$

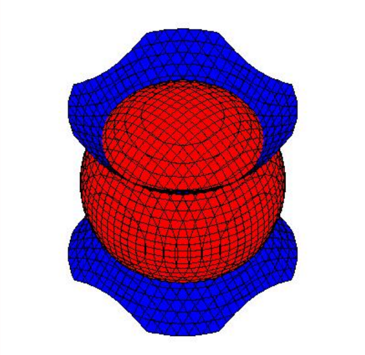
## Triangularize$(F, R)$

- **if** $F = \{ \}$ **then** return $\{\varnothing\}$
- Choose a polynomial $p \in F$ with maximal rank
- **for** $T \in$ Triangularize$(F \setminus \{p\}, R)$ **do**
  output Intersect$(p, T, R)$
  **end**

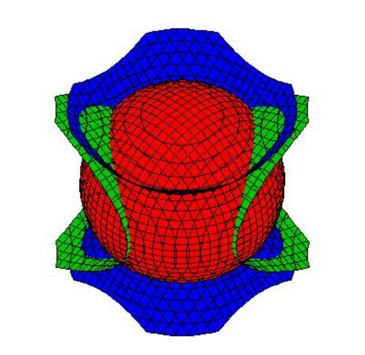
# An example

- $p_1 := x^2 + y^2 + z^2 - 4$
- $p_2 := x^2 + y^2 - z^2 - 1$
- $p_3 := z^3 + xy - 1$

$W(T) := V(p_1) \cap V(p_2)$



$V(p_3) \cap W(T)$



# Computing intersect: trivariate case

Input:

- a ring $R = \mathbf{k}[x < y < z]$
- a polynomial $p_3(x, y, z)$ of $R$
- a regular chain $T = \{t_3(x, y, z), t_2(x, y)\}$
- let $h_2 := \mathrm{init}(t_2)$ and $h_3 := \mathrm{init}(t_3)$
- assume that $\mathrm{res}(p, T) \in \mathbf{k}[x_1] \setminus \mathbf{k}$

Example

- a polynomial $p_3 := z^3 + xy - 1$
- a regular chain

$$T := \begin{cases} t_3 := 2z^2 - 3 \\ t_2 := 2y^2 + 2x^2 - 5 \end{cases}$$

# Computing intersect: trivariate case

Algorithm:

- $r_2 := \text{res}(p_3, t_3)$
- $r_1 := \text{res}(r_2, t_2)$
- **(Hypothesis)**: $h_2$ is invertible modulo $\langle r_1 \rangle$
- $g_2 := \text{RegularGcd}(r_2, t_2, \{r_1\})$
- **(Hypothesis)**: $h_3$ is invertible modulo $\langle r_1, g_2 \rangle$
- $g_3 := \text{RegularGcd}(p_3, t_3, \{r_1, g_2\})$

Output: $V(p_3) \cap W(T) = W(r_1, g_2, g_3)$

Example

$$\begin{cases} p_3 = z^3 + xy - 1 = 0 \\ t_3 = 2z^2 - 3 = 0 \\ t_2 = 2y^2 + 2x^2 - 5 = 0 \end{cases} \Rightarrow \begin{cases} g_3 = 3z + 2xy - 2 = 0 \\ g_2 = 16xy + 8x^4 - 20x^2 + 19 = 0 \\ r_1 = 64x^8 - 320x^6 + 960x^4 - 1400x^2 + 361 = 0 \end{cases}$$

# Computing intersect: projection phase

$$\begin{array}{ccc} p_3 & & t_3 \\ \downarrow & & \swarrow \\ r_2 := \mathrm{res}(p_3, t_3, z) & & t_2 \\ \downarrow & & \swarrow \\ r_1 := \mathrm{res}(r_2, t_2, y) & & \end{array}$$

Example

$$src(p_3, t_3) = \begin{cases} p_3 & := & z^3 + xy - 1 \\ t_3 & := & 2z^2 - 3 \\ S_1(p_3, t_3) & := & 6z + 4xy - 4 \\ S_0(p_3, t_3) & := & 8x^2y^2 - 16xy - 19 \end{cases}$$

$$src(r_2, t_2) = \begin{cases} r_2 & := & 8x^2y^2 - 16xy - 19 \\ t_2 & := & 2y^2 + 2x^2 - 5 \\ S_1(r_2, t_2) & := & 32xy + 38 - 40x^2 + 16x^4 \\ S_0(r_2, t_2) & := & 256x^8 - 1280x^6 + 3840x^4 - 5600x^2 + 1444 \end{cases}$$

# Computing intersect: extension phase

$$
\begin{array}{ccc}
p_3 & & t_3 \\
\downarrow & & \swarrow \\
r_2 := \mathrm{res}(p_3, t_3, z) & & t_2 \\
\downarrow & & \swarrow \\
r_1 := \mathrm{res}(r_2, t_2, y) & &
\end{array}
$$

**Theorem**

$V(p_3) \cap W(t_2, t_3) = W(r_1'', g_2', g_3)$.

$$
\begin{array}{c}
\boxed{g_3 := \mathrm{RegularGcd}(p_3, t_3, \{r_1'', g_2'\})} \\
\uparrow \\
\boxed{\{r_1'', g_2'\} := \mathrm{CleanChain}(\{r_1', g_2\}, h_3)} \\
\uparrow \\
\boxed{g_2 := \mathrm{RegularGcd}(r_2, t_2, \{r_1'\})} \\
\uparrow \\
\boxed{\{r_1'\} := \mathrm{CleanChain}(\{r_1\}, h_2)} \\
\uparrow \\
r_1
\end{array}
$$

**Example**

$$
\begin{cases}
g_3 = S_1(p_3, t_3) = 3z + 2xy - 2 \\
g_2' = g_2 = S_1(r_2, t_2) = 16xy + 8x^4 - 20x^2 + 19 \\
r_1'' = r_1 = S_0(r_2, t_2) = 64x^8 - 320x^6 + 960x^4 - 1400x^2 + 361
\end{cases}
$$

# Computing intersect: the actual algorithm

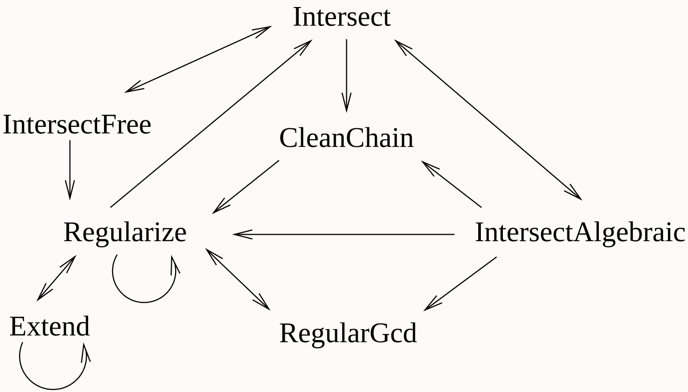



Figure: Flow graph of the Algorithms

# Computing Kalkbrener decomposition

### Krull's principle ideal theorem

Let $F \subset \mathbf{k}[\mathbf{x}]$ be finite. Let $\mathfrak{p}$ be a minimal prime ideal associated with $\langle F \rangle$. Then the height of $\mathfrak{p}$ is less than or equal to $\#(F)$.

### Corollary

Let $\mathcal{L}$ be a Kalkbrener triangular decomposition of $V(F)$. Let $T$ be a regular chain of $\mathcal{L}$, the height of which is greater than $\#(F)$. Then $\mathcal{L} \setminus \{T\}$ is also a Kalkbrener triangular decomposition of $V(F)$.

### The strategy

- prune the decomposition tree generated in computing a Lazard-Wu triangular decomposition
- remove the computation branches where the height of every generated regular chain is greater than $\#(F)$.

# Plan

# Benchmark I: input size

| | sys | #variables | #equations | total degree | dimension |
|---|---|---|---|---|---|
| 1 | 4corps-1parameter-homog | 4 | 3 | 8 | 1 |
| 2 | 8-3-config-Li | 12 | 7 | 2 | 7 |
| 3 | Alonso-Li | 7 | 4 | 4 | 3 |
| 4 | Bezier | 5 | 3 | 6 | 2 |
| 5 | Cheaters-homotopy-1 | 7 | 3 | 7 | 4 |
| 7 | childDraw-2 | 10 | 10 | 2 | 0 |
| 8 | Cinquin-Demongeot-3-3 | 4 | 3 | 4 | 1 |
| 9 | Cinquin-Demongeot-3-4 | 4 | 3 | 5 | 1 |
| 10 | collins-jsc02 | 5 | 4 | 3 | 1 |
| 11 | f-744 | 12 | 12 | 3 | 1 |
| 12 | Haas5 | 4 | 2 | 10 | 2 |
| 14 | Lichtblau | 3 | 2 | 11 | 1 |
| 16 | Liu-Lorenz | 5 | 4 | 2 | 1 |
| 17 | Mehta2 | 11 | 8 | 3 | 3 |
| 18 | Mehta3 | 13 | 10 | 3 | 3 |
| 19 | Mehta4 | 15 | 12 | 3 | 3 |
| 21 | p3p-isosceles | 7 | 3 | 3 | 4 |
| 22 | p3p | 8 | 3 | 3 | 5 |
| 23 | Pavelle | 8 | 4 | 2 | 4 |
| 24 | Solotareff-4b | 5 | 4 | 3 | 1 |
| 25 | Wang93 | 5 | 4 | 3 | 1 |

# Benchmark II: versus old versions

| | sys | TK13 | TK | TL13 | TL | STK | STL |
|---|---|---|---|---|---|---|---|
| 1 | 4corps-1parameter-homog | - | 36.9 | - | - | 62.8 | - |
| 2 | 8-3-config-Li | 8.7 | 5.9 | 29.7 | 25.8 | 6.0 | 26.6 |
| 3 | Alonso-Li | 0.3 | 0.4 | 14.0 | 2.1 | 0.4 | 2.2 |
| 4 | Bezier | - | 88.2 | - | - | - | - |
| 5 | Cheaters-homotopy-1 | 0.4 | 0.7 | - | - | 451.8 | - |
| 7 | childDraw-2 | - | - | - | - | 1326.8 | 1437.1 |
| 8 | Cinquin-Demongeot-3-3 | 3.2 | 0.6 | - | 7.1 | 0.7 | 8.8 |
| 9 | Cinquin-Demongeot-3-4 | 166.1 | 3.1 | - | - | 3.3 | - |
| 10 | collins-jsc02 | 5.8 | 0.4 | - | 1.5 | 0.4 | 1.5 |
| 11 | f-744 | - | 12.7 | - | 14.8 | 12.9 | 15.1 |
| 12 | Haas5 | 452.3 | 0.3 | - | - | 0.3 | - |
| 14 | Lichtblau | 0.7 | 0.3 | 801.7 | 143.5 | 0.3 | 531.3 |
| 16 | Liu-Lorenz | 0.4 | 0.4 | 4.7 | 2.3 | 0.4 | 4.4 |
| 17 | Mehta2 | - | 2.2 | - | 4.5 | 2.2 | 6.2 |
| 18 | Mehta3 | - | 14.4 | - | 51.1 | 14.5 | 63.1 |
| 19 | Mehta4 | - | 859.4 | - | 1756.3 | 859.2 | 1761.8 |
| 21 | p3p-isosceles | 1.2 | 0.3 | - | 352.5 | 0.3 | - |
| 22 | p3p | 168.8 | 0.3 | - | - | 0.3 | - |
| 23 | Pavelle | 0.8 | 0.5 | - | 7.0 | 0.4 | 12.6 |
| 24 | Solotareff-4b | 1.5 | 0.8 | - | 1.9 | 0.9 | 2.0 |
| 25 | Wang93 | 0.5 | 0.7 | 0.6 | 0.8 | 0.8 | 0.9 |

# Benchmark III: versus other solvers

| | sys | GL | GS | WS | TL | TK |
|---|---|---|---|---|---|---|
| 1 | 4corps-1parameter-homog | - | - | - | - | 36.9 |
| 2 | 8-3-config-Li | 108.7 | - | 27.8 | 25.8 | 5.9 |
| 3 | Alonso-Li | 3.4 | - | 7.9 | 2.1 | 0.4 |
| 4 | Bezier | - | - | - | - | 88.2 |
| 5 | Cheaters-homotopy-1 | 2609.5 | - | - | - | 0.7 |
| 7 | childDraw-2 | 19.3 | - | - | - | - |
| 8 | Cinquin-Demongeot-3-3 | 63.6 | - | - | 7.1 | 0.6 |
| 9 | Cinquin-Demongeot-3-4 | - | - | - | - | 3.1 |
| 10 | collins-jsc02 | - | - | 0.8 | 1.5 | 0.4 |
| 11 | f-744 | 30.8 | - | - | 14.8 | 12.7 |
| 12 | Haas5 | - | - | - | - | 0.3 |
| 14 | Lichtblau | 125.9 | - | - | 143.5 | 0.3 |
| 16 | Liu-Lorenz | 3.2 | 2160.1 | 40.2 | 2.3 | 0.4 |
| 17 | Mehta2 | - | - | 5.7 | 4.5 | 2.2 |
| 18 | Mehta3 | - | - | - | 51.1 | 14.4 |
| 19 | Mehta4 | - | - | - | 1756.3 | 859.4 |
| 21 | p3p-isosceles | 6.2 | - | 792.8 | 352.5 | 0.3 |
| 22 | p3p | 33.6 | - | - | - | 0.3 |
| 23 | Pavelle | 1.8 | - | - | 7.0 | 0.5 |
| 24 | Solotareff-4b | 35.2 | - | 9.1 | 1.9 | 0.8 |
| 25 | Wang93 | 0.2 | 1580.0 | 0.8 | 0.8 | 0.7 |

# Benchmark IV: output size of different solvers

| | sys | GL | GS | GD | TL | TK |
|---|---|---|---|---|---|---|
| 1 | 4corps-1parameter-homog | - | - | 21863 | - | 30738 |
| 2 | 8-3-config-Li | 67965 | - | 72698 | 7538 | 1384 |
| 3 | Alonso-Li | 1270 | - | 614 | 2050 | 374 |
| 4 | Bezier | - | - | 32054 | - | 114109 |
| 5 | Cheaters-homotopy-1 | 26387452 | - | 17297 | - | 285 |
| 7 | childDraw-2 | 938846 | - | 157765 | - | - |
| 8 | Cinquin-Demongeot-3-3 | 1652062 | - | 680 | 2065 | 895 |
| 9 | Cinquin-Demongeot-3-4 | - | - | 690 | - | 2322 |
| 10 | collins-jsc02 | - | - | 28720 | 2770 | 1290 |
| 11 | f-744 | 102082 | - | 83559 | 4509 | 4510 |
| 12 | Haas5 | - | - | 28 | - | 548 |
| 14 | Lichtblau | 6600095 | - | 224647 | 110332 | 5243 |
| 16 | Liu-Lorenz | 47688 | 123965 | 712 | 2339 | 938 |
| 17 | Mehta2 | - | - | 1374931 | 5347 | 5097 |
| 18 | Mehta3 | - | - | - | 25951 | 25537 |
| 19 | Mehta4 | - | - | - | 71675 | 71239 |
| 21 | p3p-isosceles | 56701 | - | 1453 | 9253 | 840 |
| 22 | p3p | 160567 | - | 1768 | - | 1712 |
| 23 | Pavelle | 17990 | - | 1552 | 3351 | 1086 |
| 24 | Solotareff-4b | 2903124 | - | 14810 | 2438 | 872 |
| 25 | Wang93 | 2772 | 56383 | 1377 | 1016 | 391 |

# Conclusion

- We present a new algorithm for computing triangular decompositions of polynomial systems incrementally.
- We propose a weakened notion of a polynomial GCD modulo a regular chain
- Extracting common work from similar expensive computations is also a key feature of our algorithms.
- Our implementation outperforms solvers with similar specifications by several orders of magnitude on sufficiently difficult problems.

Thank you!