Irredundant Triangular Decomposition

Gleb Pogudin[1], Agnes Szanto[2]

[1]New York University and City University of New York

[2]North Carolina State University

Big picture

Question

How can one represent the set

$$W = \{\mathbf{z} \in \mathbb{C}^n \mid f_1(\mathbf{z}) = \ldots = f_m(\mathbf{z}) = 0\},$$

where $f_1, \ldots, f_m \in \mathbb{C}[z_1, \ldots, z_n]$?

Big picture

Question

How can one represent the set

$$W = \{\mathbf{z} \in \mathbb{C}^n \mid f_1(\mathbf{z}) = \ldots = f_m(\mathbf{z}) = 0\},$$

where $f_1, \ldots, f_m \in \mathbb{C}[z_1, \ldots, z_n]$?

Possible approaches

- Gröbner bases
- Geometric resolution
- Triangular decomposition
- Witness sets

Big picture

Question

How can one represent the set

$$W = \{\mathbf{z} \in \mathbb{C}^n \mid f_1(\mathbf{z}) = \ldots = f_m(\mathbf{z}) = 0\},$$

where $f_1, \ldots, f_m \in \mathbb{C}[z_1, \ldots, z_n]$?

Possible approaches

- Gröbner bases
- Geometric resolution
- Triangular decomposition ← this talk
- Witness sets

What is a triangular set?

What is a triangular set?

Example (row echelon form)

$$p_1 = x_1 - 2x_2 + x_3 \quad \in \mathbb{C}[x_1, x_2, x_3]$$
$$p_2 = 5x_1 - x_2 \quad \in \mathbb{C}[x_1, x_2]$$
$$p_3 = x_1 - 1 \quad \in \mathbb{C}[x_1]$$

What is a triangular set?

Example (row echelon form)

$$\begin{aligned} p_1 &= x_1 - 2x_2 + x_3 && \in \mathbb{C}[x_1, x_2, x_3] \\ p_2 &= 5x_1 - x_2 && \in \mathbb{C}[x_1, x_2] \\ p_3 &= x_1 - 1 && \in \mathbb{C}[x_1] \end{aligned}$$

Example (nonlinear case)

$$\begin{aligned} p_1 &= x_1 x_3 - x_2^2 && \in \mathbb{C}[x_1, x_2, x_3] \\ p_2 &= x_2^3 - x_1^2 && \in \mathbb{C}[x_1, x_2] \end{aligned}$$

x_2 and x_3 are *leading variables* and x_1 is a *free variable*.

What is a triangular set?

Example (row echelon form)

$$\begin{aligned} p_1 &= x_1 - 2x_2 + x_3 && \in \mathbb{C}[x_1, x_2, x_3] \\ p_2 &= 5x_1 - x_2 && \in \mathbb{C}[x_1, x_2] \\ p_3 &= x_1 - 1 && \in \mathbb{C}[x_1] \end{aligned}$$

Example (nonlinear case)

$$\begin{aligned} p_1 &= x_1 x_3 - x_2^2 && \in \mathbb{C}[x_1, x_2, x_3] \\ p_2 &= x_2^3 - x_1^2 && \in \mathbb{C}[x_1, x_2] \end{aligned}$$

x_2 and x_3 are *leading variables* and x_1 is a *free variable*.

Remark

$$\textit{regular chain} = \text{triangular set} + \begin{pmatrix} \text{extra assumption} \\ \text{(“leading coefficient} \neq 0\text{”)} \end{pmatrix}$$

How do we use regular chains? Pseudo-reduction!

Input

- regular chain $\{x_1 x_3 - x_2^2, x_2^3 - x_1^2\} \subset \mathbb{C}[x_1, x_2, x_3]$
- polynomial $x_3^2 - x_2 \in \mathbb{C}[x_1, x_2, x_3]$

How do we use regular chains? Pseudo-reduction!

Input

- regular chain $\{x_1 x_3 - x_2^2, x_2^3 - x_1^2\} \subset \mathbb{C}[x_1, x_2, x_3]$
  vanish on the curve $t \to (t^3, t^2, t)$;
- polynomial $x_3^2 - x_2 \in \mathbb{C}[x_1, x_2, x_3]$
  also vanishes on $t \to (t^3, t^2, t)$.

How do we use regular chains? Pseudo-reduction!

Input

- regular chain $\{x_1 x_3 - x_2^2, x_2^3 - x_1^2\} \subset \mathbb{C}[x_1, x_2, x_3]$
  vanish on the curve $t \to (t^3, t^2, t)$;
- polynomial $x_3^2 - x_2 \in \mathbb{C}[x_1, x_2, x_3]$
  also vanishes on $t \to (t^3, t^2, t)$.

Pseudo-reduction

How do we use regular chains? Pseudo-reduction!

Input

- regular chain $\{x_1x_3 - x_2^2, x_2^3 - x_1^2\} \subset \mathbb{C}[x_1, x_2, x_3]$
  vanish on the curve $t \to (t^3, t^2, t)$;
- polynomial $x_3^2 - x_2 \in \mathbb{C}[x_1, x_2, x_3]$
  also vanishes on $t \to (t^3, t^2, t)$.

Pseudo-reduction

$$x_1(\underline{x_3^2} - x_2) - x_3(\underline{x_1x_3} - x_2^2) = r_1 \qquad \to \quad r_1 := -x_1x_2 + x_2^2x_3,$$

How do we use regular chains? Pseudo-reduction!

Input

- regular chain $\{x_1x_3 - x_2^2, x_2^3 - x_1^2\} \subset \mathbb{C}[x_1, x_2, x_3]$
  vanish on the curve $t \to (t^3, t^2, t)$*;*
- polynomial $x_3^2 - x_2 \in \mathbb{C}[x_1, x_2, x_3]$
  also vanishes on $t \to (t^3, t^2, t)$*.*

Pseudo-reduction

$$x_1(\underline{x_3^2} - x_2) - x_3(\underline{x_1x_3} - x_2^2) = r_1 \quad \to \quad r_1 := -x_1x_2 + x_2^2x_3,$$
$$x_1(\underline{x_2^2x_3} - x_1x_2) - x_2^2(\underline{x_1x_3} - x_2^2) = r_2 \quad \to \quad r_2 := -x_1^2x_2 + x_2^4,$$

How do we use regular chains? Pseudo-reduction!

Input

- regular chain $\{x_1x_3 - x_2^2, x_2^3 - x_1^2\} \subset \mathbb{C}[x_1, x_2, x_3]$
  vanish on the curve $t \to (t^3, t^2, t)$*;*
- polynomial $x_3^2 - x_2 \in \mathbb{C}[x_1, x_2, x_3]$
  also vanishes on $t \to (t^3, t^2, t)$*.*

Pseudo-reduction

$$
\begin{aligned}
x_1(\underline{x_3^2} - x_2) - x_3(\underline{x_1x_3} - x_2^2) = r_1 \quad &\to \quad r_1 := -x_1x_2 + x_2^2x_3, \\
x_1(\underline{x_2^2x_3} - x_1x_2) - x_2^2(\underline{x_1x_3} - x_2^2) = r_2 \quad &\to \quad r_2 := -x_1^2x_2 + x_2^4, \\
(\underline{x_2^4} - x_1^2x_2) - x_2(\underline{x_2^3} - x_1^2) = r_3 \quad &\to \quad r_3 := 0
\end{aligned}
$$

What is a triangular decomposition?

The ideal and variety defined by a regular chain

Let $\Delta \subset \mathbb{C}[\mathbf{x}]$ be a regular chain, then

$$\mathcal{I}(\Delta) := \{f \in \mathbb{C}[\mathbf{x}] \mid f \text{ pseudo-reduces to zero w.r.t. } \Delta\}.$$

What is a triangular decomposition?

The ideal and variety defined by a regular chain

Let $\Delta \subset \mathbb{C}[\mathbf{x}]$ be a regular chain, then

$$\mathcal{I}(\Delta) := \{f \in \mathbb{C}[\mathbf{x}] \mid f \text{ pseudo-reduces to zero w.r.t. } \Delta\}.$$

For example, $\mathcal{I}(\{x_1x_3 - x_2^2,\ x_2^3 - x_1^2\}) = (x_1x_3 - x_2^2,\ x_2x_3 - x_1,\ x_3^2 - x_2)$.

What is a triangular decomposition?

The ideal and variety defined by a regular chain

Let $\Delta \subset \mathbb{C}[\mathbf{x}]$ be a regular chain, then

$$\mathcal{I}(\Delta) := \{f \in \mathbb{C}[\mathbf{x}] \mid f \text{ pseudo-reduces to zero w.r.t. } \Delta\}.$$

For example, $\mathcal{I}(\{x_1x_3 - x_2^2,\ x_2^3 - x_1^2\}) = (x_1x_3 - x_2^2,\ x_2x_3 - x_1,\ x_3^2 - x_2)$.

Then $\mathcal{V}(\Delta) \subset \mathbb{C}^n$ is the set of common zeros of $\mathcal{I}(\Delta)$.

What is a triangular decomposition?

The ideal and variety defined by a regular chain

Let $\Delta \subset \mathbb{C}[\mathbf{x}]$ be a regular chain, then

$$\mathcal{I}(\Delta) := \{f \in \mathbb{C}[\mathbf{x}] \mid f \text{ pseudo-reduces to zero w.r.t. } \Delta\}.$$

For example, $\mathcal{I}(\{x_1x_3 - x_2^2,\ x_2^3 - x_1^2\}) = (x_1x_3 - x_2^2,\ x_2x_3 - x_1,\ x_3^2 - x_2)$.

Then $\mathcal{V}(\Delta) \subset \mathbb{C}^n$ is the set of common zeros of $\mathcal{I}(\Delta)$.

Caveat: In general, $\mathcal{I}(\Delta)$ is larger than the ideal generated by Δ.

What is a triangular decomposition?

The ideal and variety defined by a regular chain

Let $\Delta \subset \mathbb{C}[\mathbf{x}]$ be a regular chain, then

$$\mathcal{I}(\Delta) := \{f \in \mathbb{C}[\mathbf{x}] \mid f \text{ pseudo-reduces to zero w.r.t. } \Delta\}.$$

For example, $\mathcal{I}(\{x_1x_3 - x_2^2,\ x_2^3 - x_1^2\}) = (x_1x_3 - x_2^2,\ x_2x_3 - x_1,\ x_3^2 - x_2)$.

Then $\mathcal{V}(\Delta) \subset \mathbb{C}^n$ is the set of common zeros of $\mathcal{I}(\Delta)$.

Triangular decomposition

Let $X \subset \mathbb{C}^n$ be an algebraic variety. Then a representation

$$X = \mathcal{V}(\Delta_1) \cup \ldots \cup \mathcal{V}(\Delta_m),$$

where $\Delta_1, \ldots, \Delta_m$ are regular chains, is called a *triangular decomposition of* X.

What is a triangular decomposition?

The ideal and variety defined by a regular chain

Let $\Delta \subset \mathbb{C}[\mathbf{x}]$ be a regular chain, then

$$\mathcal{I}(\Delta) := \{f \in \mathbb{C}[\mathbf{x}] \mid f \text{ pseudo-reduces to zero w.r.t. } \Delta\}.$$

For example, $\mathcal{I}(\{x_1x_3 - x_2^2,\ x_2^3 - x_1^2\}) = (x_1x_3 - x_2^2,\ x_2x_3 - x_1,\ x_3^2 - x_2)$.

Then $\mathcal{V}(\Delta) \subset \mathbb{C}^n$ is the set of common zeros of $\mathcal{I}(\Delta)$.

Triangular decomposition

Let $X \subset \mathbb{C}^n$ be an algebraic variety. Then a representation

$$X = \mathcal{V}(\Delta_1) \cup \ldots \cup \mathcal{V}(\Delta_m),$$

where $\Delta_1, \ldots, \Delta_m$ are regular chains, is called a *triangular decomposition of* X.

Important remark: $m = 1$ is not enough for an arbitrary variety.

Irredundant triangular decomposition

Definition

A triangular decomposition

$$X = \mathcal{V}(\Delta_1) \cup \ldots \cup \mathcal{V}(\Delta_m)$$

is called *irredundant* if

$$\forall (i \neq j)\ \ \forall (C = \text{an irreducible component of } \mathcal{V}(\Delta_i)) \quad C \not\subset \mathcal{V}(\Delta_j).$$

Irredundant triangular decomposition

Definition

A triangular decomposition

$$X = \mathcal{V}(\Delta_1) \cup \ldots \cup \mathcal{V}(\Delta_m)$$

is called *irredundant* if

$$\forall (i \neq j)\ \ \forall (C = \text{an irreducible component of } \mathcal{V}(\Delta_i)) \quad C \not\subset \mathcal{V}(\Delta_j).$$

Main problem

The main problem is to design a good algorithm such that

Input An algebraic variety defined by a system of polynomial equations $f_1 = \ldots = f_s = 0$

Output Irredundant triangular decomposition of X

Motivation

- Reduce the size of the output

Motivation

- Reduce the size of the output
- Get correct information about the geometry of a variety

Motivation

- Reduce the size of the output
- Get correct information about the geometry of a variety

  Example

  System of equations

$$x_1x_3 - x_2^2 = x_2x_3 - x_1 = x_3^2 - x_2 = 0.$$

Motivation

- Reduce the size of the output
- Get correct information about the geometry of a variety

  Example

  System of equations

$$x_1x_3 - x_2^2 = x_2x_3 - x_1 = x_3^2 - x_2 = 0.$$

  Irredundant decomposition

$$X = \mathcal{V}(\{x_1x_3 - x_2^2,\ x_2^3 - x_1^2\})$$

Motivation

- Reduce the size of the output
- Get correct information about the geometry of a variety

  Example

  System of equations

$$x_1x_3 - x_2^2 = x_2x_3 - x_1 = x_3^2 - x_2 = 0.$$

  Irredundant decomposition

$$X = \mathcal{V}(\{x_1x_3 - x_2^2,\ x_2^3 - x_1^2\})$$

  Decomposition by RegularChains (Maple)

$$X = \mathcal{V}(\{x_1x_3 - x_2^2,\ x_2^3 - x_1^2\}) \cup \mathcal{V}(\{x_3, x_2, x_1\})$$

Motivation

- Reduce the size of the output
- Get correct information about the geometry of a variety

  Example

  System of equations

$$x_1x_3 - x_2^2 = x_2x_3 - x_1 = x_3^2 - x_2 = 0.$$

  Irredundant decomposition

$$X = \mathcal{V}(\{x_1x_3 - x_2^2,\ x_2^3 - x_1^2\})$$

  Decomposition by RegularChains (Maple)

$$X = \mathcal{V}(\{x_1x_3 - x_2^2,\ x_2^3 - x_1^2\}) \cup \mathcal{V}(\{x_3, x_2, x_1\})$$

- Design better Hensel lifting-based algorithms (later in the talk)

State of the art

State of the art

Theoretical grounds and first algorithms due to

Ritt, *Wu*, *Lazard*, *Aubry*, *Kalkbrenner*, and other researchers

State of the art

Theoretical grounds and first algorithms due to

Ritt, *Wu*, *Lazard*, *Aubry*, *Kalkbrenner*, and other researchers

General algorithms without irredundancy guarantees

- General theoretical algorithm (**1999**)
  Szanto
- Maple package RegularChains (**2005**)
  Alvandi, *Chen*, *Lemaire*, *Moreno Maza*, *Xie*, ...

State of the art

Theoretical grounds and first algorithms due to

Ritt, *Wu*, *Lazard*, *Aubry*, *Kalkbrenner*, and other researchers

General algorithms without irredundancy guarantees

- General theoretical algorithm (**1999**)
  Szanto
- Maple package RegularChains (**2005**)
  Alvandi, *Chen*, *Lemaire*, *Moreno Maza*, *Xie*, ...

Irredundant decomposition for special cases

- Irreducible varieties (**2003**)
  Schost
- Zero-dimensional varieties (**2005**)
  Dahan, *Moreno Maza*, *Schost*, *Wu*, *Xie*

Brute-force solution

Algorithm for computing an irredundant triangular decomposition

1. Compute prime decomposition of the radical of the ideal (e.g., Gröbner bases)
2. Apply Schost's algorithm to every prime component

Brute-force solution

Algorithm for computing an irredundant triangular decomposition

1. Compute prime decomposition of the radical of the ideal (e.g., Gröbner bases)
2. Apply Schost's algorithm to every prime component

Not the end of the story

- double-exponential theoretical complexity
- triangular decomposition is often used as *an alternative* to Gröbner bases
- not factorization-free

Main result

We design a Monte Carlo algorithm:

Input: algebraic variety $X \subset \mathbb{C}^n$
defined by $f_1 = \ldots = f_m = 0$, where $\deg f_i \leqslant d$

Main result

We design a Monte Carlo algorithm:

Input: algebraic variety $X \subset \mathbb{C}^n$
defined by $f_1 = \ldots = f_m = 0$, where $\deg f_i \leqslant d$

Output: An irredundant triangular decomposition of X such that

Main result

We design a Monte Carlo algorithm:

Input: algebraic variety $X \subset \mathbb{C}^n$
defined by $f_1 = \ldots = f_m = 0$, where $\deg f_i \leqslant d$

Output: An irredundant triangular decomposition of X such that

- the degrees the output polynomials
$\leqslant \deg X(\deg X + 1) \leqslant d^{2n} + d^n$

Main result

We design a Monte Carlo algorithm:

Input: algebraic variety $X \subset \mathbb{C}^n$
defined by $f_1 = \ldots = f_m = 0$, where $\deg f_i \leqslant d$

Output: An irredundant triangular decomposition of X such that

- the degrees the output polynomials
  $\leqslant \deg X(\deg X + 1) \leqslant d^{2n} + d^n$
- the degrees of the intermediate polynomials
  $\leqslant \max((n+1)d^{n+1}, d^{2n} + d^n)$

The toolbox

- Equidimensional decomposition using *Jeronimo and Sabia* (**2002**)
  Input: a variety X defined by polynomial equations
  Output: equidimensional decomposition of X defined by polynomial equations

The toolbox

- Equidimensional decomposition using *Jeronimo and Sabia* (**2002**)
  Input: a variety X defined by polynomial equations
  Output: equidimensional decomposition of X defined by polynomial equations
- Generalized resultant by *Canny* (**1990**)
  Separates components that can be represented by a regular chain with a given set of leading variables

The toolbox

- Equidimensional decomposition using *Jeronimo and Sabia* (**2002**)
  Input: a variety X defined by polynomial equations
  Output: equidimensional decomposition of X defined by polynomial equations
- Generalized resultant by *Canny* (**1990**)
  Separates components that can be represented by a regular chain with a given set of leading variables
- Algorithm based on a mixture of *Schost* (**2003**) and *Dahan*, *Moreno Maza*, *Schost*, *Wu*, *Xie* (**2005**)
  Input: a zero-dimensional variety over a field of rational function
  Output: irredundant triangular decomposition

Sketch of the algorithm

Step 1: Stratification w.r.t. dimension

Compute equidimensional decomposition

Sketch of the algorithm

Step 1: Stratification w.r.t. dimension

Compute equidimensional decomposition

Step 2: Stratification w.r.t. leading variables

Separate components with different sets of leading variables

Using the Canny's resultant and a random specialization.

Sketch of the algorithm

Step 1: Stratification w.r.t. dimension

Compute equidimensional decomposition

Step 2: Stratification w.r.t. leading variables

Separate components with different sets of leading variables
Using the Canny's resultant and a random specialization.

Step 3: Reduction to zero-dimensional case

Leading variables are fixed $\Longrightarrow$ Zero-dimensional variety over the rational functions in the free variables

Sketch of the algorithm

Step 1: Stratification w.r.t. dimension

Compute equidimensional decomposition

Step 2: Stratification w.r.t. leading variables

Separate components with different sets of leading variables
Using the Canny's resultant and a random specialization.

Step 3: Reduction to zero-dimensional case

Leading variables are fixed $\Longrightarrow$ Zero-dimensional variety over the rational functions in the free variables

Hensel lifting using our degree bounds (next slide)

The degree bound for the output

Theorem (follows from Dahan and Schost, 2004)

Let Δ be a triangular set with leading coefficients involving only free variables. Then

$$\deg f \leqslant (\deg \mathcal{V}(\Delta))^2 + \deg \mathcal{V}(\Delta) \text{ for every } f \in \Delta.$$

The degree bound for the output

Theorem (follows from Dahan and Schost, 2004)

Let Δ be a triangular set with leading coefficients involving only free variables. Then

$$\deg f \leqslant (\deg \mathcal{V}(\Delta))^2 + \deg \mathcal{V}(\Delta) \text{ for every } f \in \Delta.$$

Degree bound

- irredundancy
- only free variables in the leading coefficients

$\Longrightarrow$ degree bound in terms of $\deg X$

The degree bound for the output

Theorem (follows from Dahan and Schost, 2004)

Let Δ be a triangular set with leading coefficients involving only free variables. Then

$$\deg f \leqslant (\deg \mathcal{V}(\Delta))^2 + \deg \mathcal{V}(\Delta) \text{ for every } f \in \Delta.$$

Degree bound

- irredundancy
- only free variables in the leading coefficients

$\Longrightarrow$ degree bound in terms of $\deg X$

Application to the algorithm

degree bound $\Longrightarrow$ stopping criterion for Hensel lifting

Future work

- Reduce the degree bound to linear in $\deg X$ (this would be asymptocially tight).

Future work

- Reduce the degree bound to linear in $\deg X$
  (this would be asymptocially tight).
- Generalize to a system of equations and inequations.

Future work

- Reduce the degree bound to linear in $\deg X$
  (this would be asymptocially tight).
- Generalize to a system of equations and inequations.
- Bound the heights of the coefficients.

Support

The work was supported by

- National Science Foundation
- City University of New York
- Austrian Science Fund FWF
- Department of Mathematics at North Carolina State University