Complexity of Triangular Representations of Algebraic Sets

Mengxiao Sun

CUNY Graduate Center

April 22, 2017

Joint work with Eli Amzallag, Gleb Pogudin and N. Thieu Vo

Main Problem

- Given: $\{f_1, \ldots, f_s\} \subseteq k[x_1, \ldots, x_n]$
- Want: efficient representation of the algebraic set $V = \{x \in k^n : f_1(x) = \cdots = f_s(x) = 0\}$
- Algorithmic tools:
  Gröbner bases
  Triangular sets
- Example: Consider $\{x^2y^2 - x^2 - y^2 + 1, xy\} \subseteq k[x, y]$ and $x < y$
  Gröbner bases $\Longrightarrow \{xy, x^2 + y^2 - 1, y^3 - y\}$
  Triangular sets $\Longrightarrow$ $\Delta_1 = \{x^2 - 1, y\}$, $\Delta_2 = \{x, y^2 - 1\}$

Motivation

- To turn theoretical bounds for effective differential elimination and Nullstellensatz into bounds for practical algorithms.

  (A.Ovchinnikov, G.Pogudin, N.T.Vo, 2016)

- To reduce the complexity of Hrushovski's algorithm for computing the differential Galois group of a linear differential equation.

Goal

- Analyze the complexity of triangular representations of algebraic sets.
- Compare the complexity of computing triangular representations with the one of computing Gröbner bases.

Triangular Sets

- k: an algebraically closed field with characteristic zero
- Fix an ordering on the variables: $x_1 < x_2 < \cdots < x_n$
- class(f): the highest variable appearing in f, where $f \in k[x_1, \ldots, x_n]$

Definition

Let $\Delta = \{g_1, \ldots, g_m\} \subseteq k[x_1, \ldots, x_n]$. We say that Δ is a *triangular set* if class(g_i) $<$ class(g_j) for all $i < j$.

Example. $\Delta = \{x_1^3 + 2, x_1 - x_2, x_5^2 - x_4^2 + 5x_3 + 1\} \subseteq k[x_1, \ldots, x_{10}]$ is a triangular set because class($x_1^3 + 2$) $= x_1$, class($x_1 - x_2$) $= x_2$, and class($x_5^2 - x_4^2 + 5x_3 + 1$) $= x_5$.

Representation of an Ideal by Triangular Sets

Example(Szántó)

Consider $I = \left\langle x^2y^2 - x^2 - y^2 + 1, xy \right\rangle \subseteq k[x,y]$ and $x < y$.
$V(I) = V(\Delta_1) \cup V(\Delta_2)$ for $\Delta_1 = \{x^2 - 1, y\}$ and $\Delta_2 = \{x, y^2 - 1\}$.

Question: Can we always find such a representation?

Representation of an Ideal by Triangular Sets

Theorem (Szántó,1997)

Let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal. There exists an algorithm which computes "unmixed" triangular sets $\Delta_1 \ldots, \Delta_r$ such that

$$\sqrt{I} = \mathrm{Rep}(\Delta_1) \cap \cdots \cap \mathrm{Rep}(\Delta_r).$$

Intuition. $\sqrt{I} = \langle \Delta_1 \rangle \cap \cdots \cap \langle \Delta_r \rangle$.

Remark. In general, $\langle \Delta \rangle \subseteq \mathrm{Rep}(\Delta)$.

Example. Let $\Delta = \{x^3 - x, xy\}$ be a triangular set in $k[x, y]$ with $x < y$.
$x^3 y = y(x^3 - x) + xy \Rightarrow y \in \mathrm{Rep}(\Delta)$. But $y \notin \langle \Delta \rangle$.

Main Results(degree bounds)

Szántó's Algorithm:

Input: $\{f_1, \ldots, f_s\} \subseteq k[x_1, \ldots, x_n]$

Output: $\{\Delta_1, \ldots, \Delta_r\}$ such that $\sqrt{I} = \bigcap_{i=1}^{r} \mathrm{Rep}(\Delta_i)$, where $I = \langle f_1, \ldots, f_s \rangle$

Theorem (Amzallag, Pogudin, S, and Vo, 2016)

Let $I = \langle f_1, \ldots, f_s \rangle \subseteq k[x_1, \ldots, x_n]$ be an ideal. Assume that the degree of f_i is at most d for $1 \leq i \leq s$ and the codimension of I is m. In case s is not too large($s \leq d^m$), the degree of any polynomial in the output or during the computation of Szántó's algorithm does not exceed

$$nd^{6m^3}.$$

Main Results(number of components)

Theorem (Amzallag, Pogudin, S, and Vo, 2016)

Let $I = \langle f_1, \ldots, f_s \rangle \subseteq k[x_1, \ldots, x_n]$ be an ideal. Assume that the degree of f_i is at most d for $1 \le i \le s$ and the codimension of I is m. In case s is not too large($s \le d^m$), the number of "unmixed" triangular sets in the output of Szántó's algorithm is at most

$$\binom{n}{m}\left((m+1)d^m + 1\right)^m.$$

Gröbner Basis Methods

- It is well known that Gröbner bases provide a solution of representing a polynomial ideal or its corresponding algebraic set.
- The degree bound for computing a Gröbner basis is double-exponential in the dimension of the given polynomial ideal.

  Mayr and Ritscher(2013): $2(\frac{d^{2m^2}}{2} + \frac{d}{2})^{2^{n-m}}$

Comparison to Degree Bounds for Gröbner Basis Methods

- Laplagne(2006) proposed an algorithm for computing the generators of the radical of a polynomial ideal using Gröbner bases.

  four applications of Gröbner basis computation

- We compare our degree bound of Szántó's algorithm with the one of Laplagne's algorithm.

Comparison to Degree Bounds for Gröbner Basis Methods

Given $I = \langle f_1, \ldots, f_s \rangle \subseteq k[x_1, \ldots, x_n]$. Let m be the codimension of I and d be the degree bound of f_i, $1 \leq i \leq s$.

n	m	d	Our Bound	Laplagne's Bound
2	2	2	$6 \cdot 10^{10}$	$4 \cdot 10^{12501}$
		3	$2 \cdot 10^{13}$	$8 \cdot 10^{19787}$
		4	$9 \cdot 10^{14}$	$3 \cdot 10^{24968}$
3	2	2	$8 \cdot 10^{10}$	$2 \cdot 10^{186742}$
		3	$3 \cdot 10^{13}$	$2 \cdot 10^{303324}$
4	2	2	$2 \cdot 10^{11}$	$2 \cdot 10^{2891351}$
		3	$3 \cdot 10^{13}$	$6 \cdot 10^{4756660}$
		4	$2 \cdot 10^{15}$	$10^{6082886}$
	3	2	$2 \cdot 10^{19}$	$2 \cdot 10^{3104704}$
		3	$5 \cdot 10^{25}$	$3 \cdot 10^{4974233}$

Complexity of Triangular Representations of Algebraic Sets

Eli Amzallag, Gleb Pogudin, Mengxiao Sun, N. Thieu Vo

arXiv:1609.09824

Thank You!

References

- S.Laplagne, An algorithm for the Computation of the Radical of an Ideal, Proceedings of the 2006 International Symposium on Symbolic and Algebraic Computation, pages 191195, 2006.
- E.W.Mayr, S.Ritscher, Dimension-dependent Bounds for Gröbner Bases of Polynomial Ideals, Journal of Symbolic Computation 49, pages 78-94, 2013.
- Á.Szántó, Complexity of the Wu-Ritt decomposition, Proceedings of the Second International Symposium on Parallel Symbolic Computation, pages 139–149, 1997.
- Á.Szántó, Computation with polynomial systems, PhD Thesis, Cornell University, 1999.