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 \( \Rightarrow \) \( \{xy, x^2 + y^2 - 1, y^3 - y\} \)

Triangular sets \( \Rightarrow \) \( \Delta_1 = \{x^2 - 1, y\} \), \( \Delta_2 = \{x, y^2 - 1\} \)
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: $x_1 < x_2 < \cdots < x_n$
- $\text{class}(f)$: 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 $\Delta$ is a **triangular set** if $\text{class}(g_i) < \text{class}(g_j)$ 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 $\text{class}(x_1^3 + 2) = x_1$, $\text{class}(x_1 - x_2) = x_2$, and $\text{class}(x_5^2 - x_4^2 + 5x_3 + 1) = x_5$. 
Example (Szántó)

Consider \( I = \langle x^2y^2 - x^2 - y^2 + 1, xy \rangle \subseteq k[x, y] \) 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?
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

\[
\sqrt{I} = \text{Rep}(\Delta_1) \cap \cdots \cap \text{Rep}(\Delta_r).
\]

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

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

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

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

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

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

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

\[
\binom{n}{m} ((m + 1)d^m + 1)^m.
\]
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): \(2\left(\frac{d^{2m^2}}{2} + \frac{d}{2}\right)^{2n-m}\)

four applications of Gröbner basis computation

We compare our degree bound of Szántó’s algorithm with the one of Laplagne’s algorithm.
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 $f_i$, $1 \leq i \leq s$.

<table>
<thead>
<tr>
<th>$n$</th>
<th>$m$</th>
<th>$d$</th>
<th>Our Bound</th>
<th>Laplagne’s Bound</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2</td>
<td>2</td>
<td>$6 \cdot 10^{10}$</td>
<td>$4 \cdot 10^{12501}$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3</td>
<td>$2 \cdot 10^{13}$</td>
<td>$8 \cdot 10^{19787}$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4</td>
<td>$9 \cdot 10^{14}$</td>
<td>$3 \cdot 10^{24968}$</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>2</td>
<td>$8 \cdot 10^{10}$</td>
<td>$2 \cdot 10^{186742}$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3</td>
<td>$3 \cdot 10^{13}$</td>
<td>$2 \cdot 10^{303324}$</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>2</td>
<td>$2 \cdot 10^{11}$</td>
<td>$2 \cdot 10^{2891351}$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3</td>
<td>$3 \cdot 10^{13}$</td>
<td>$6 \cdot 10^{4756660}$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4</td>
<td>$2 \cdot 10^{15}$</td>
<td>$10^{6082886}$</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>2</td>
<td>$2 \cdot 10^{19}$</td>
<td>$2 \cdot 10^{3104704}$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3</td>
<td>$5 \cdot 10^{25}$</td>
<td>$3 \cdot 10^{4974233}$</td>
</tr>
</tbody>
</table>
Complexity of Triangular Representations of Algebraic Sets
Eli Amzallag, Gleb Pogudin, Mengxiao Sun, N. Thieu Vo
arXiv:1609.09824
Thank You!
References