An Efficient Algorithm for Computing Parametric Multivariate Polynomial GCD

Dong Lu

Key Laboratory of Mathematics Mechanization
Academy of Mathematics and Systems Science, CAS

Joint work with Deepak Kapur, Michael Monagan, Yao Sun and Dingkang Wang

July 16-19, 2018, The City University of New York, USA

Outline

Outline

The Problem

Notations

- k is a field.
- $\mathbf{e_1} := (1, 0)$ and $\mathbf{e_2} := (0, 1)$.
- $X = \{x_1, \ldots, x_n\}$ are variables.
- $U = \{u_1, \ldots, u_m\}$ are parameters.
- $k[U][X]$ is the polynomial ring in X.

The Problem

Example 1

Let $f_1, f_2 \in \mathbb{C}[a][x, y]$, where

$$\begin{cases} f_1 = ax^3 + (a^3 - a + 1)x^2y + (a^2 + 2)xy^2 + (3a^2 - 3)y^3, \\ f_2 = ax^3 + (a + 1)x^2y + 4xy^2 + 3y^3. \end{cases}$$

The results are:

$$\begin{cases} \text{when } a = 0, \ \ \gcd(f_1, f_2) = y(x + 3y); \\ \text{when } a^2 - 2 = 0, \ \ \gcd(f_1, f_2) = 2x^3 + (a + 2)x^2y + 4axy^2 + 3ay^3; \\ \text{when } a(a^2 - 2) \neq 0, \ \ \gcd(f_1, f_2) = ax^2 + xy + 3y^2. \end{cases}$$

The Problem

Problem: For any given parametric polynomials $f_1, f_2, \ldots, f_s$ in $k[U][X]$, how to divide the parametric space and obtain the corresponding GCD on each branch quickly?

Outline

Previous Works

- **Non-parametric polynomials case**
  - J. Moses and D.Y.Y. Yun: The EZ GCD algorithm. *In Proceedings of ACM' 73*, ACM Press, New York, 1973, 159-166. (Hensel lifting)
  - R. Zippel: Probabilistic algorithms for sparse polynomials. *In Proceedings of EUROSAM' 79*, Springer-Verlag, 1979, 216-226. (sparse interpolation)
  - P. Gianni and B. Trager: GCDs and factoring multivariate polynomials using Gröbner bases. *In Proceedings of EUROCAL' 85*, Springer, Berlin, Heidelberg, 1985, 409-410. (Gröbner basis)
  - T. Sasaki and M. Suzuki: Three new algorithms for multivariate polynomial GCD. *Journal of Symbolic Computation*, 1992, 395-411. (Gröbner basis)

Previous Works

- **Parametric polynomials case**
  - S.A. Abramov and K.Y. Kvashenko: On the greatest common divisor of polynomials which depend on a parameter. *In Proceedings of ISSAC 1993*, 152-156. (subresultant chain)
  - A. Ayad: Complexity of algorithms for computing greatest common divisors of parametric univariate polynomials. *International Journal of Algebra*, 2010, 173-188. (Gaussian elimination)
  - K. Nagasaka: Parametric greatest common divisors using comprehensive Gröbner systems. *In Proceedings of ISSAC 2017*, 341-348. (extended the ideas of Gianni and Trager as well as Sasaki and Suzuki)

Outline

The New Algorithm

- **Non-parametric polynomials case**

Definition 1

Let $I \subset k[X]$ be an ideal and $g \in k[X] \setminus \{0\}$. The set

$$I : g = \{f \in k[X] : fg \in I\}$$

is called the **quotient ideal** (or **colon ideal**) of I divided by g.

The New Algorithm

- **Non-parametric polynomials case**

Definition 1

Let $I \subset k[X]$ be an ideal and $g \in k[X] \setminus \{0\}$. The set

$$I : g = \{f \in k[X] : fg \in I\}$$

is called the **quotient ideal** (or **colon ideal**) of I divided by g.

Example 2

In $k[x, y, z]$, let $I = \langle xy \rangle$ and $g = xz$. Then

$$I : g = \{f : xzf \in \langle xy \rangle\} = \{f : zf \in \langle y \rangle\} = \langle y \rangle.$$

The New Algorithm

Lemma 1

Let $f_1, f_2 \in k[X] \setminus \{0\}$, then $\langle f_1 \rangle : f_2$ is a principal ideal. Suppose that $\langle f_1 \rangle : f_2 = \langle f \rangle$, then we have

$$\gcd(f_1, f_2) = \frac{f_1}{f}.$$

The New Algorithm

Lemma 1

Let $f_1, f_2 \in k[X] \setminus \{0\}$, then $\langle f_1 \rangle : f_2$ is a principal ideal. Suppose that $\langle f_1 \rangle : f_2 = \langle f \rangle$, then we have

$$\gcd(f_1, f_2) = \frac{f_1}{f}.$$

Example 3

Let $f_1 = xy$ and $f_2 = xz$. According to the Example 2, we have that $\langle xy \rangle : xz = \langle y \rangle$. Then $\gcd(f_1, f_2) = f_1/f = x$.

The New Algorithm

Problem: How to compute the generator of $\langle f_1 \rangle : f_2$?

The New Algorithm

Problem: How to compute the generator of $\langle f_1 \rangle : f_2$?

- Original Method

Lemma 2

Let $f_1, f_2 \in k[X] \setminus \{0\}$ and w be a new variable, then

$$\langle wf_1, (w-1)f_2 \rangle \cap k[X] = \langle g \rangle$$

for some $g \in k[X] \setminus \{0\}$. Moreover, we have $\langle f_1 \rangle : f_2 = \langle \frac{g}{f_2} \rangle$ and $\gcd(f_1, f_2) = \frac{f_1 f_2}{g}$.

The New Algorithm

- New Method

Lemma 3

Let $f_1, f_2 \in k[X] \setminus \{0\}$ and $\prec$ be a monomial order on $k[X]^2$ with $\mathbf{e_2} \prec \mathbf{e_1}$. Suppose G is a minimal Gröbner basis of $\langle f_1 \cdot \mathbf{e_1}, f_2 \cdot \mathbf{e_1} - \mathbf{e_2} \rangle$. Then there is a unique $f \in k[X] \setminus \{0\}$ such that $f \cdot \mathbf{e_2} \in G$ and $\langle f_1 \rangle : f_2 = \langle f \rangle$. Therefore, $\gcd(f_1, f_2) = \frac{f_1}{f}$.

The New Algorithm

- New Method

Lemma 3

Let $f_1, f_2 \in k[X] \setminus \{0\}$ and $\prec$ be a monomial order on $k[X]^2$ with $\mathbf{e_2} \prec \mathbf{e_1}$. Suppose G is a minimal Gröbner basis of $\langle f_1 \cdot \mathbf{e_1}, f_2 \cdot \mathbf{e_1} - \mathbf{e_2} \rangle$. Then there is a unique $f \in k[X] \setminus \{0\}$ such that $f \cdot \mathbf{e_2} \in G$ and $\langle f_1 \rangle : f_2 = \langle f \rangle$. Therefore, $\gcd(f_1, f_2) = \frac{f_1}{f}$.

Example 4

Let $f_1 = xy$, $f_2 = xz$. Given the lexicographic order $\prec$ and extend it to $k[X]^2$ in a position over term with $\mathbf{e_2} \prec \mathbf{e_1}$. A minimal Gröbner basis of $\langle xy \cdot \mathbf{e_1}, xz \cdot \mathbf{e_1} - \mathbf{e_2} \rangle$ is $G = \{y \cdot \mathbf{e_2}, xy \cdot \mathbf{e_1}, xz \cdot \mathbf{e_1} - \mathbf{e_2}\}$. So, $f = y$ and $\langle xy \rangle : xz = \langle y \rangle$. Moreover, $\gcd(xy, xz) = f_1/f = x$.

The New Algorithm

- **Parametric polynomials case**

Theorem 1

Let $f_1, f_2 \in k[U][X]$ and $\prec$ be a monomial order on $k[X]^2$ with $\mathbf{e_2} \prec \mathbf{e_1}$. Suppose $\{(A_i, G_i)\}_{i=1}^{I}$ is a minimal comprehensive Gröbner system of $\langle f_1 \cdot \mathbf{e_1}, f_2 \cdot \mathbf{e_1} - \mathbf{e_2} \rangle$. For each branch (A_i, G_i), let $H_i = \{f \mid f \cdot \mathbf{e_2} \in G_i\}$. Then we have

1. If $H_i = \emptyset$, then $f_1 = 0$ and $\gcd(f_1, f_2) = f_2$ on A_i.
2. If $H_i \neq \emptyset$, then $H_i = \{f\}$ and $\gcd(f_1, f_2) = \frac{f_1}{f}$ on A_i.

The New Algorithm

▶ Parametric GCD Algorithm

Input: $f_1, f_2 \in k[U][X]$, a constructible set $A \subset \bar{k}^m$, and two monomial orders $\prec_X, \prec_U$.
Output: a comprehensive GCDs: $\{(A_i, h_i)\}_{i=1}^s$, where $h_i = \gcd(f_1, f_2)$ under any specialization from A_i and $\cup_{i=1}^s A_i = A$.

Step 1: compute a minimal comprehensive Gröbner system $\{(A_i, G_i)\}_{i=1}^s$ for the module $\langle f_1 \cdot \mathbf{e_1}, f_2 \cdot \mathbf{e_1} - \mathbf{e_2} \rangle$ on A.

Step 2: For every i, let $H_i = \{h \mid h \cdot \mathbf{e_2} \in G_i\}$, then do

Step 2.1: if H_i is empty, then $h_i = f_2$ on A_i and turn to Step 2; otherwise, turn to Step 2.2.

Step 2.2: $h_i = f_1/h$ on A_i.

Step 3: return $\{(A_i, h_i)\}_{i=1}^s$.

Outline

A Simple Example

Example 5

Let $f_1, f_2, f_3 \in \mathbb{C}[a, b][x, y, z]$ be as follows:

$$\begin{cases} f_1 = ax^2 + bxy + a^2xz + abx + abyz + b^2y, \\ f_2 = ax^2 + bxy + (ab - a)xz - a^2x + (b^2 - b)yz - aby, \\ f_3 = ax^2 + bxy + a^2xz + (a^2 - ab)x + abyz + (ab - b^2)y, \end{cases}$$

Using the new algorithm to compute the GCDs of f_1, f_2, f_3.

A Simple Example

Monomial order: $\prec_X$ and $\prec_U$ are all lexicographic orders with $x > y > z$ and $a > b$, respectively. We extend $\prec_X$ to $k[X]^2$ in a position over term with $\mathbf{e_2} \prec_X \mathbf{e_1}$.

A Simple Example

Monomial order: $\prec_X$ and $\prec_U$ are all lexicographic orders with $x > y > z$ and $a > b$, respectively. We extend $\prec_X$ to $k[X]^2$ in a position over term with $\mathbf{e_2} \prec_X \mathbf{e_1}$.

Step 1: Compute a minimal comprehensive Gröbner system (CGS) $\mathcal{G}_0$ of $\langle f_1 \cdot \mathbf{e_1}, f_2 \cdot \mathbf{e_1} - \mathbf{e_2} \rangle$, and get six branches $\{(A_i, G_i)\}_{i=1}^{6}$.

The first branch of $\mathcal{G}_0$ is (A_1, G_1), where

$$A_1 = \mathbf{V}(\langle 0 \rangle) \setminus \mathbf{V}(\langle a^3 - a^2 b + a^2 \rangle),$$
$$G_1 = \{f_1 \cdot \mathbf{e_1},\ \ (x + az + b) \cdot \mathbf{e_2},\ \ ((a^2 - ab + a)xz + (a^2 + ab)x + (ab - b^2 + b)yz + (ab + b^2)y) \cdot \mathbf{e_1} + \mathbf{e_2}\}.$$

Then, $H_1 = \{x + az + b \mid (x + az + b) \cdot \mathbf{e_2} \in G_1\}$ and the GCD of f_1 and f_2 on A_1 is

$$h_1 = f_1/(x + az + b) = ax + by.$$

A Simple Example

Similarly, the GCDs of f_1 and f_2 on other five branches are:

$$(A_2, h_2) = (\mathbf{V}(\langle a - b + 1\rangle) \setminus \mathbf{V}(\langle 2b^2 - 3b + 1\rangle), (b-1)x + by),$$

$$(A_3, h_3) = (\mathbf{V}(\langle a, b - 1\rangle), y),$$

$$(A_4, h_4) = (\mathbf{V}(\langle 2a + 1, 2b - 1\rangle) \setminus \mathbf{V}(\langle b - 1\rangle), -\tfrac{1}{2}x^2 + \tfrac{1}{2}xy + \tfrac{1}{4}xz - \tfrac{1}{4}x - \tfrac{1}{4}yz + \tfrac{1}{4}y),$$

$$(A_5, h_5) = (\mathbf{V}(\langle a, b\rangle), 0),$$

$$(A_6, h_6) = (\mathbf{V}(\langle a\rangle) \setminus \mathbf{V}(\langle ab^3 - ab^2 - b^4 + 2b^3 - b^2\rangle), by).$$

A Simple Example

Step 2: For A_1, compute the GCD of h_1 and f_3.

A minimal CGS $\mathcal{G}_1$ of $\langle h_1 \cdot \mathbf{e_1}, f_3 \cdot \mathbf{e_1} - \mathbf{e_2} \rangle$ on A_1 has one branch:

$$(A_1, G_{11}) = (\mathbf{V}(\langle 0 \rangle) \setminus \mathbf{V}(\langle a^3 - a^2 b + a^2 \rangle), \{\mathbf{e_2}, h_1 \cdot \mathbf{e_1}\}).$$

Then $H_{11} = \{1\}$ and the GCD of h_1 and f_3 on A_1 is

$$h_{11} = h_1/1 = ax + by.$$

So, the GCD of f_1, f_2, f_3 on A_1 is

$$\gcd(f_1, f_2, f_3) = ax + by.$$

A Simple Example

Similarly, we can compute the GCD of h_i and f_3 on A_i, where $i = 2, \ldots, 6$. Then the parametric GCDs of $\{f_1, f_2, f_3\}$ are

$$\begin{cases} (\mathbf{V}(\langle 0\rangle) \setminus \mathbf{V}(\langle a^3 - a^2 b + a^2\rangle), ax + by), \\ (\mathbf{V}(\langle a - b + 1\rangle) \setminus \mathbf{V}(\langle 2b^2 - 3b + 1\rangle), (b-1)x + by), \\ (\mathbf{V}(\langle a, b - 1\rangle), y), \\ (\mathbf{V}(\langle 2a + 1, 2b - 1\rangle) \setminus \mathbf{V}(\langle b - 1\rangle), -x + y), \\ (\mathbf{V}(\langle a, b\rangle), 0), \\ (\mathbf{V}(\langle a\rangle) \setminus \mathbf{V}(\langle ab^3 - ab^2 - b^4 + 2b^3 - b^2\rangle), by). \end{cases}$$

Outline

Implementation

- The new algorithm and two algorithms proposed by Nagasaka have been implemented in the *Singular*.
- More comparative examples can be generated by the codes at: `http://www.mmrc.iss.ac.cn/~dwang/software.html`.
- The experimental data was obtained on a Core i7-4790 3.60GHz with 4GB Memory running Windows 7.

Implementation

Table: Timings(sec.)

Ex.	New	NGT	NSS
1	0.640	2.062	0.809
2	1.023	47.210	19.680
3	0.836	6.730	4.125
4	0.597	$>$ 1h	12.736
5	2.475	10.760	4.108
6	2.426	$>$ 1h	21.558
7	6.419	$>$ 1h	$>$ 1h
8	5.286	$>$ 1h	37.172
9	15.351	$>$ 1h	98.744
10	10.011	$>$ 1h	$>$ 1h

- NGT: K. **N**agasaka, P. **G**ianni and B. **T**rager.
- NSS: K. **N**agasaka, T. **S**asaki and M. **S**uzuki.
- K. Nagasaka: Parametric greatest common divisors using comprehensive Gröbner systems, in Proceedings of ISSAC 2017, 341-348. July 25-28, Kaiserslautern Germany.

Outline

Conclusions

1. We compute the GCDs of parametric polynomials by using quotient ideal and comprehensive Gröbner system of a module.
2. Our method does not need to compute the primitive part of parametric polynomials with respect to main variable.
3. Without any knowledge of f_1 or f_2 being zero or not on different branch, the GCDs of f_1 and f_2 can be obtained from the minimal comprehensive Gröbner system of $\langle f_1 \cdot \mathbf{e_1}, f_2 \cdot \mathbf{e_1} - \mathbf{e_2} \rangle$.
4. When we compute the GCDs of more than two parametric polynomials, the results can be obtained iteratively.

Thanks for your attention!