A Stable Computation of Multivariarte Apporximate GCD **Based on SVD and Lifting Technique**

Masaru Sanuki^{1,*,†}

¹Institute of Medicine, University of Tsukuba, Ten-noudai 1-1-1, Tsukuba-shi, Ibaraki 305-8575, Japan

Abstract

For univariate polynomials, the approximate GCD can be obtained by computing the null space of the subresultant matrix of given polynomials. In this study, for multivariate polynomials, we propose a method for computing null space of the subresultant matrix within polynomials stably and efficiently, which is based on the SVD (singular value decomposition) and lifting techniques. Therefore, we show the multivariate approximate GCD can be also computed by using subresultant matrix. In addition, we describe an ill-conditioned case (initial factors have approximate common factor) and solve them.

Keywords

Approximate GCD, Lifting technique, Ill-conditioned cases

1. Preliminaries

Let F(x, t) and G(x, t) be multivariate polynomials in $\mathbb{F}[x, t_1, \dots, t_\ell] = \mathbb{F}[x, t]$ (x is the main variable and $t = (t_1, \dots, t_\ell)$ are sub-variables), and be expressed as

$$F(x, \mathbf{t}) = \tilde{F}(x, \mathbf{t})C(x, \mathbf{t}) + \Delta_F = f_m(\mathbf{t})x^m + \dots + f_0(\mathbf{t}),$$

$$G(x, \mathbf{t}) = \tilde{G}(x, \mathbf{t})C(x, \mathbf{t}) + \Delta_G = g_n(\mathbf{t})x^n + \dots + g_0(\mathbf{t}).$$

Here, \tilde{F} , \tilde{G} , C, Δ_F , Δ_G are polynomials in $\mathbb{F}[x,t]$, and when $||\Delta_F|| \ll ||F||$ and $||\Delta_G|| \ll ||G||$, C is called an approximate factor of F and G. In particular, the approximate factor of maximum degree is called approximate GCD, which is denoted by gcd(F, G).

Various algorithm exist for the approximate GCD of univariate polynomials. However, there are few stable all-purpose methods for a large number of variables in a multivariate case. Numericalbased methods are stable but significantly less efficient, so we have tried to improve efficiency by combining lifting methods [4]. In this study, we challenge the stable computation of the null space of the subresultant within polynomial entries.

First, we review the method for the subresultant matrix for multivariate polynomials. For the resultant within polynomials, we propose a QRGCD-like method over truncated power-series polynomials, it is efficient [5]. For the null space of the subresultant matrix, Gao et al. and Zeng-Dayton proposed SVD-based methods for numeric matrices at the same conference [2, 7], where the SVD is the *singular* value decomposition for matrix. These matrices are sparse and the size are also huge extremely although the degree of given polynomial is not large. Lifting techniques is known for solving of equation modulo an ideal I and lifting them to solution modulo I^2, I^3, \ldots in order to get the ideal adic completion. Here I is an ideal as $I = \langle t_1 - s_1, \dots, t_\ell - s_\ell \rangle$ with $(s_1, \dots, s_\ell) \in \mathbb{F}^\ell$ (in this paper, (s_1, \dots, s_ℓ) is the origin). For multivariate GCD computation, the EZ-GCD method is well-known lifting method based on Hensel's lemma, however, its approximate computation will be unstable when initial factors have an approximate common factor [8].

In this paper, we propose a stable multivariate approximate GCD computation, which is based on the SVD and lifting techniques. It is able to compute the approximate GCD even though initial factors have approximate common factors.

© 2024 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).



SCSS 2024: 10th International Symposium on Symbolic Computation in Software Science, August 28-30, 2024, Tokyo, Japan *Corresponding author.

Sanuki@md.tsukuba.ac.jp (M. Sanuki)

2. Framework of algorithm

In this paper, we discuss non-singular case only, i.e., $F(x,0) \cdot G(x,0) \neq 0$ and $f_m(0) \cdot g_n(0) \neq 0$. For non-singular case, every polynomial P(x,t) is transform to $P(x,T,t) = P(x,Tt_1,\ldots,Tt_\ell)$, with T is the total-degree variable. Every polynomial P(x,T,t) is represented as the sum of homogeneous polynomials w.r.t. the total-degree variable T;

$$P(x,T,t) = P^{(0)}(x) + T \cdot \delta P^{(1)}(x,t) + \dots + T^w \cdot \delta P^{(w)}(x,t) + \dots,$$

$$P^{(w)}(x,T,t) = P^{(0)}(x) + T \cdot \delta P^{(1)}(x,t) + \dots + T^w \cdot \delta P^{(w)}(x,t).$$

In non-singular case, the following two conditions exist: $\deg(\gcd(F,G)) \leq \deg(\gcd(F^{(0)},G^{(0)}))$ and $\gcd(F,G)|\gcd(F^{(0)},G^{(0)})$. In such situations, lifting algorithms can be applied. The proposed algorithm is discussed in the next section.

2.1. Computing cofactors of F and G via lifting method

Let $S_i(F,G) = S_i \in \mathbb{F}[t,T]^{(m+n-2i)\times(m+n-2i)}$ be an *i*th-subresultant matrix of F and G w.r.t. x, and be represented as

$$S_{i} = \begin{pmatrix} f_{m} & g_{n} \\ \vdots & \ddots & \vdots & \ddots \\ f_{m-n-k} & f_{m} & g_{n-m-k} & g_{n} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ f_{m-n-k} & g_{n-m-k} \end{pmatrix}$$

$$= S_{i}^{(0)} + T \cdot \delta S_{i}^{(1)} + \dots + T^{w} \cdot \delta S_{i}^{(w)} + \dots,$$

where $\mathcal{S}_i^{(0)} = \delta \mathcal{S}_i^{(0)} \in \mathbb{F}^{(m+n-2i)\times(m+n-2i)}$ and $\delta \mathcal{S}_i^{(w)} \in \mathbb{F}[t]^{(m+n-2i)\times(m+n-2i)}$ for $w \geq 1$. When $k = \deg(\gcd(F,G)) = \deg(\gcd(F^{(0)},G^{(0)}))$, it is well-known as the null space of \mathcal{S}_{k-1} corresponds to \tilde{G} and \tilde{F} , and $\operatorname{rank}(\mathcal{S}_{k-1}) = K-1$ where K = m-(k-1)+n-(k-1).

computation of cofactors for univariate part: SVD

Cofactors of $F^{(0)}$ and $G^{(0)}$ can be obtained from the null space of $\mathcal{S}_{k-1}^{(0)}$. In this paper, we compute the null space of $\mathcal{S}_{k-1}^{(0)}$ using the SVD [1]. Using the SVD of $\mathcal{S}_{k-1}^{(0)}$, we obtain the following decomposition:

$$\mathcal{S}_{k-1}^{(0)} = U\Sigma V^T = \begin{pmatrix} \mathbf{u}_1 & \cdots & \mathbf{u}_K \end{pmatrix} \begin{pmatrix} \sigma_1 & & \\ & \ddots & \\ & & \sigma_K \end{pmatrix} \begin{pmatrix} \mathbf{v}_1^T \\ \vdots \\ \mathbf{v}_K^T \end{pmatrix},$$

where K=m-(k-1)+n-(k-1), U and V are orthogonal matrices, and σ_i are singular vectors with $\sigma_1 \geq \sigma_2 \geq \ldots \geq \sigma_{K-1} \gg \sigma_K \geq 0$, respectively. Then, $v_K \in \text{Ker}(\mathcal{S}_{k-1}^{(0)})$, and it is one of the solutions of $\mathcal{S}_{k-1}^{(0)} z = \mathbf{0}$ is $z = r^{(0)} = v_K$;

$$m{v}_K = egin{pmatrix} ilde{g}_{n-k}^{(0)} \ ilde{g}_0^{(0)} \ ilde{- ilde{f}}_{m-k}^{(0)} \ ilde{- ilde{f}}_0^{(0)} \end{pmatrix}, ext{ with } ||m{v}_K||_2 = 1.$$

Computation of cofactors for multivariate part: lifting method

Suppose we have $\mathbf{r}^{(w)} = \mathbf{r}^{(w-1)} + \delta \mathbf{r}^{(w)}$. Here, $\delta \mathbf{r}^{(w)}$ is a vector generated by homogenious polynomials with total-degree w w.r.t. T. Then, $\delta \mathbf{r}^{(w+1)}$ is generated as follows. Note that the following consists.

$$\mathcal{S}_{k-1} r^{(w+1)} \equiv \mathbf{0} \pmod{T^{w+2}}$$

 $\mathcal{S}_{k-1}^{(0)} \delta r^{(w+1)} = -\sum_{j=1}^{w+1} \mathcal{S}_{k-1}^{(j)} \delta r^{(w-j)} = \delta p^{(w)}.$

Now, $\delta r^{(w+1)}$ and $\delta p^{(w+1)}$ are transformed bases from e_1, \dots, e_K to v_1, \dots, v_K and u_1, \dots, u_K , respectively, as follows:

$$\delta \boldsymbol{z}^{(w)} = \begin{pmatrix} \delta z_1^{(w)} \\ \vdots \\ \delta z_K^{(w)} \end{pmatrix} = \delta \hat{z}_1^{(w)} \boldsymbol{v}_1 + \ldots + \delta \hat{z}_K^{(w)} \boldsymbol{v}_K, \quad \delta \boldsymbol{p}^{(w)} = \begin{pmatrix} \delta p_1^{(w)} \\ \vdots \\ \delta p_K^{(w)} \end{pmatrix} = \delta \hat{p}_1^{(w)} \boldsymbol{u}_1 + \ldots + \delta \hat{p}_N^{(w)} \boldsymbol{u}_K.$$

Then, we obtain $\delta \hat{z}_i^{(w+1)} = \delta \hat{p}_i^{(w+1)}/\sigma_i$ $(i=1,\ldots,K-1)$. Therefore, $\delta \boldsymbol{r}^{(w+1)}$ is constructed, as follows.

$$\delta \boldsymbol{r}^{(w+1)} = \delta \hat{p}_1^{(1)} / \sigma_1 \boldsymbol{v}_1 + \ldots + \delta \hat{p}_{K-1}^{(1)} / \sigma_{K-1} \boldsymbol{v}_{K-1} + \mathbb{F}[T, \boldsymbol{t}]_{w+1} \cdot \boldsymbol{v}_K,$$

where $\mathbb{F}[T, t]_{w+1}$ is homogeneous polynomial set with total-degree w+1 w.r.t. T, and we have the following as a candidate solution.

$$m{r}^{(w)} = m{t}_K + \sum_{i=1}^w \delta \hat{p}_1^{(w)} / \sigma_1 m{v}_1 + \ldots + \sum_{i=1}^w \delta \hat{p}_{K-1}^{(w)} / \sigma_{K-1} m{v}_{K-1} + \mathbb{F}[m{T}, m{t}]_{[1,w]} \cdot m{v}_K,$$

where $\mathbb{F}[T, t]_{[1,w]} = \bigcup_{j=1}^w \mathbb{F}[T, t]_j$. To compute the approximate GCD of F and G, we need to determine $q^{(w)} = \delta q^{(1)} + \ldots + \delta q_{(w)} \in \mathbb{F}[T, t]_{[1,w]}$ s.t.

$$r^{(w)}(q) = t_K + \sum_{i=1}^w \delta \hat{p}_1^{(w)} / \sigma_1 v_1 + \ldots + \sum_{i=1}^w \delta \hat{p}_{K-1}^{(w)} / \sigma_{K-1} v_{K-1} + q^{(w)} \cdot v_K,$$

To determine the approximate GCD, we must determine $q^{(i)}$. The following example shows one approach to determining each undetermined element $\delta q^{(i)}$ for $1 \le i \le w$..

Example1

Polynomials $F(x,t_1,t_2)$ and $G(x,t_1,t_2)$ having an approximate GCD $C(x,t_1,t_2)=x^3+(1+t_2-2t_1+t_1^2)x+3$ are expressed as

$$F(x,t_1,t_2) = (x^3 + (t_2^2 + t_1 + t_1 - 2)x^2 - 1) \times C(x,t_1,t_2) + M_{eps},$$

$$G(x,t_1,t_2) = (x^3 + (2t_2^2 - t_1 + 3)x^2 - 1) \times C(x,t_1,t_2) + M_{eps},$$

where M_{eps} is the machine epsilon.

In this example, k=2 is already known (K=8). Then, one solution of $\mathcal{S}_1^{(0)} z = \mathbf{0}$ is $z = r^{(0)} = v_8$;

$$\boldsymbol{r}^{(0)} = \boldsymbol{v}_8 = \begin{pmatrix} -0.242535625036333 \\ -0.727606875108999 \\ -2.24840273230668 \times 10^{-15} \\ \hline 0.242535625036333 \\ -0.485071250072665 \\ -1.32375311946987 \times 10^{-15} \\ -0.242535625036333 \end{pmatrix}.$$

A candidate of $\delta r^{(1)}|_{\delta q^{(1)}=0} = \delta \hat{p}_1^{(1)}/\sigma_1 v_1 + \ldots + \delta \hat{p}_7^{(1)}/\sigma_7 v_7 + \delta q^{(1)} \times v_8$ is

$$\delta \boldsymbol{z}^{(1)} = \begin{pmatrix} 0.0713340073 \cdots t_1 + 0.0285336029 \cdots t_2 \\ -0.0285336029 \cdots t_1 + 0.0856008088 \cdots t_2 \\ 3.65419500 \cdots \times 10^{-15}t_1 - 4.96824803 \cdots \times 10^{-15}t_2 \\ -0.0713340073 \cdots t_1 - 0.0285336029 \cdots t_2 \\ -0.0998676103 \cdots t_1 - 0.185468419 \cdots t_2 \\ 4.77577504 \cdots \times 10^{-16}t_1 - 1.10469359 \cdots \times 10^{-15}t_2 \\ 0.0713340073 \cdots t_1 + 0.0285336029 \cdots t_2 \end{pmatrix} + \delta q^{(1)} \cdot \boldsymbol{v}_8 = \begin{pmatrix} \delta \tilde{g}_{n-k}^{(1)} \\ \delta \tilde{g}_{n-k-1}^{(1)} \\ \vdots \\ \delta \tilde{g}_0^{(1)} \\ -\delta f_{m-k}^{(1)} \\ -\delta f_{m-k-1}^{(1)} \\ \vdots \\ -\delta f_0^{(1)} \end{pmatrix}.$$

Generally, it is difficult to determine $\delta q^{(1)}$ properly.

However, assuming that cofactors are also not dense or the approximate GCD is monic, several coefficients will be zero. In this example, assume the 1st element is zero, $\delta q^{(1)}$ is $\delta q_1^{(1)}=$ $(0.0713340073636269\,t_1 + 0.0285336029454512\,t_2)/0.242535625036333$ and $\delta {m r}^{(1)}$ becomes

$$\begin{pmatrix} 0 \\ 0.242535625036331t_1 \\ 0 \\ 0 \\ -0.242535625036331t_1 - 0.242535625036334t_2 \\ 0 \\ 0 \end{pmatrix}.$$

It is unlikely that many factors will be close to zero simultaneously, and this can only happen if the result is correct. Unlike the EZ-GCD method, it is more efficient because it can extract each undetermined coefficient at each lifting step. So that, "check zeros" is very efficiency.

If the coefficients are dense, lc(lc(F), lc(G)) or lc(lc(gcd(F, G))) should be calculated in advance so that the elements can be determined uniquely.

2.2. Computing approximate GCD

After obtaining cofactors, the approximate GCD is computed by solving and F $(f_m, f_{m-1}, \dots, f_0)^T \in \mathbb{F}[t]^{m+1}.$

$$\begin{pmatrix} \tilde{f}_{m-k} \\ \vdots & \ddots \\ \tilde{f}_0 & \tilde{f}_{m-k} \\ & \ddots & \vdots \\ & \tilde{f}_0 \end{pmatrix} \begin{pmatrix} c_k \\ c_{k-1} \\ \vdots \\ c_0 \end{pmatrix} = \begin{pmatrix} f_m \\ f_{m-1} \\ \vdots \\ f_0 \end{pmatrix}$$

This linear equation is solve as following step.

- 1. Solve $C_{m+1,k+1}^{(0)}(\tilde{\boldsymbol{F}})\cdot\boldsymbol{c}^{(0)}=\boldsymbol{F}^{(0)}$. Actually, we utilize the SVD as in the former case.

 2. Lifting step: solve $C_{m+1,k+1}^{(0)}(\tilde{\boldsymbol{F}})\cdot\delta\boldsymbol{c}^{(w)}=\delta\boldsymbol{F}^{(w)}-\sum_{i}C_{m+1,k+1}^{(i)}(\tilde{\boldsymbol{F}})\times\delta\boldsymbol{c}^{(w-i)}$. This step can also be solved using SVD.
- 3. Return $c_k x^k + \cdots + c_0$ as an approximate GCD.

3. Solve in ill-conditioned cases

In this section, we demonstrate that our method is stable for ill-conditioned cases [8, 5]. On the other word, we deals with cases where the initial factor is an approximate common factor. In this case, the EZ-GCD method is unstable since large cancellation errors occur [6].

Example 2 (initial factors have approximate common factor)

Compute the approximate GCD of F and G, where both polynomials are monic.

$$F(x,t_1,t_2) = (x^3 + (t_2^2 + t_1 + t_2 - 2)x^2 - 1)(x - 1.0003 + 2t_2 - t_1^2)C + M_{eps},$$

$$G(x,t_1,t_2) = (x^3 + (2t_2^2 - t_1 + 3)x^2 - 1)(x - 1.0005 + t_1 + t_2 + t_1t_2)C + M_{eps},$$

$$C(x,t_1,t_2) = x^3 + (1 + t_2 - 2t_1 + t_1^2)x + 3.$$

Initial factors $F^{(0)}$ and $G^{(0)}$ have an approximate common factor (x-1.0002) with tolerance $O(10^{-5})$. Sigular values of $\mathcal{S}_3^{(0)}(F,G)$ are $19.8>18.3>14.5>12.8>8.2>4.4>1.1>0.6\gg 1.5\times 10^{-5}\gg 1.1\times 10^{-16}$. Because give polynomials are monic, the leading coefficient of cofactors and the approximate GCD are also monic, respectively.

When w=1, Adjusting the 1st element of $\delta r^{(1)}$ by z_K only, we obtained the following.

$$\delta \boldsymbol{r}^{(1)} = \begin{pmatrix} 0. \\ -7.25814180424500 \times 10^{-8}t_1 + 0.176741414005228t_2 \\ 0.707053518826616t_1 + 0.530224242015704t_2 \\ -6.96526170074208 \times 10^{-14}t_1 + 6.29774010718620 \times 10^{-14}t_2 \\ -0.176741268890038t_1 - 0.176741414005196t_2 \\ 1.42941214420489 \times 10^{-15}t_1 + 6.38378239159465 \times 10^{-16}t_2 \\ -0.176741268889989t_1 - 0.530224096948041t_2 \\ 0.176794218725546t_1 + 0.883759874841642t_2 \\ -1.18932641512970 \times 10^{-14}t_1 - 7.57727214306669 \times 10^{-15}t_2 \\ -7.25814328778052 \times 10^{-8}t_1 + 0.353482755476628t_2 \end{pmatrix}$$

The perturbation is $||\tilde{F}^{(1)}G^{(1)} - \tilde{F}^{(1)}G^{(1)}|| \approx O(10^{-8}) \approx \sigma_K/\sigma_{K-1}$. On the other hand, by adjusting z_{K-1} , we obtained the following, It can be confirmed that the solution is not accurate; $||\tilde{F}^{(1)}G^{(1)} - \tilde{F}^{(1)}G^{(1)}|| \approx \sigma_K$.

```
\begin{pmatrix} 0. \\ -0.1988511825793107t_1 - 0.14357803747786974t_2 \\ 0.11055165805122452t_1 - 0.43065120320683287t_2 \\ 0.0002976768351589665t_1 + 0.00047951294108034004t_2 \\ 0.022318043342197766t_1 + 0.14391342019466513t_2 \\ -0.7183155936049679 \times 10^{-5}t_1 - 0.000011570991832604571t_2 \\ 0.02212670015656562t_1 - 0.20987748805445672t_2 \\ -0.22096310056080598t_1 + 0.243032215144183t_2 \\ 0.00007010876634662433t_1 + 0.00011293475597320968t_2 \\ -0.19880976332099576t_1 + 0.03323002423516758t_2 \end{pmatrix}
```

When w=2, by lifting step and adjusting the 1st element of $\delta r^{(2)}$ by z_K , we obtained the following

vector.

```
\begin{pmatrix} 0. \\ 0.353120013467623t_2^2 + 0.177466845429488t_1t_2 - 0.000362979823316206t_1^2 \\ -0.354747432749536t_2^2 + 0.355659122269873t_1t_2 - 0.177830208344029t_1^2 \\ 8.84819995 \cdots \times 10^{-13}t_2^2 - 4.59634934 \cdots \times 10^{-12}t_1t_2 + 1.03052288 \cdots \times 10^{-12}t_1^2 \\ 0.000362669479650586t_2^2 - 0.177466845422696t_1t_2 + 0.000362979818887450t_1^2 \\ \hline -9.08967345 \cdots \times 10^{-13}t_2^2 - 3.63698827 \cdots \times 10^{-12}t_1t_2 - 1.36436695 \cdots \times 10^{-12}t_1^2 \\ -0.176378671991595t_2^2 - 0.000725503949587463t_1t_2 + 0.177104321289445t_1^2 \\ -0.177413730546595t_2^2 - 0.352031674994445t_1t_2 - 0.354208569999507t_1^2 \\ -9.15635622 \cdots \times 10^{-13}t_2^2 + 2.71640175 \cdots \times 10^{-12}t_1t_2 - 1.68760838 \cdots \times 10^{-13}t_1^2 \\ -0.000362669478412958t_2^2 + 0.000725503952765407t_1t_2 - 0.177104321291319t_1^2 \end{pmatrix}
```

Adjusting only v_K is not accurate. Therefore, adjusting v_K and v_{K-1} in $\ker \mathcal{S}_k^{(0)}$ we have the following, and it obtains the expected solution one . In this case, perturbation becomes $||\tilde{F}^{(2)}G^{(2)} - \tilde{F}^{(2)}G^{(2)}|| \approx \sigma_K$, it is better.

The SVD is stable even if the matrix is irregular. Thus, the SVD of $\mathcal{S}^{(0)}$ is also stable even if initial factors have an approximate common factor. On the other hand, a lifting method using the Bezout matrix is unstable since initial matrix is assumed to be regular [4]. Hence, our method is more stable and efficient than existing methods.

References

- [1] R. Corless, P. Gianni, B. Trager and S. Watt, *The singular value decomposition for polynomial systems*, Proc. of ISSAC'95, ACM Press, 1995, 195–207.
- [2] S. Gao, E. Kaltofen, J. P. May, Z. Yang and L. Zhi, *Approximate factorization of multivariate polynomials via differential equations*, Proc. of ISSAC'04, ACM Press, 2004, 167–174.
- [3] M. Ochi, M-T. Noda and T. Sasaki, Approximate greatest common divisor of multivariate polynomials and its application to ill-conditioned systems of algebraic equations, J. Inform. Proces., 14 (1991), 292–300.
- [4] M. Sanuki. *Computing multivariate approximate GCD based on Barnett's theorem*, Proc. of Symbolic-Numeric Computation 2009 (SNC 2009), 2009, 149–157.
- [5] M. Sanuki and T. Sasaki, *Computing approximate GCDs in ill-conditioned cases*, International Workshop of Symbolic-Numeric Computation 2007 (SNC2007), ACM Press, 2007, 170-179, 25–27.
- [6] T. Sasaki and S. Yamaguchi, An analysis of cancellation error in multivariate Hensel construction with floating-point number arithmetic, Proc. of ISSAC'98, ACM Press, 1998, 1–8.
- [7] Z. Zeng and B. H. Dayton, *The approximate GCD of inexact polynomials part II: A multivariate algorithm*, Proc. of ISSAC'04, ACM Press, 2004, 320–327.
- [8] L. Zhi and M-T. Noda, *Approximate GCD of Multivariate Polynomials*, Proc. of ASCM2000, World Scientific, 2000, 9–18.