斉次な多変数多項式の近似GCD算法の比較

Comparison of Approximate GCD Methods for Homogeneous Polynomials

筑波大学医学医療系　　讃岐勝 *1
Masaru Sanuki
Faculty of Medicine, University of Tsukuba

Abstract

This manuscript describes a comparison of approximate GCD arithmetic methods for homogeneous polynomials. In particuler, we treat the EZ-GCD mehthod (polynomias-based lifting method, or it is based on the Hensel lifting) and matrix-based lifting method finding linear equation within polynomials.

1　はじめに：リフティング法を再考する

$\mathbb{F}$ を浮動小数全体の集合とする．本稿では，x を主変数，$t_1, \ldots, t_\ell$ を従変数とする浮動小数係数の多変数多項式 $F(x,\boldsymbol{t}), G(x,\boldsymbol{t}) \in \mathbb{F}[x, t_1, \ldots, t_\ell] = \mathbb{F}[x,\boldsymbol{t}]$ の近似 GCD の計算法について述べる．ここで，多項式 F と G は次で表す．

$$\begin{aligned} F(x,\boldsymbol{t}) &= f_m(\boldsymbol{t})x^m + \ldots + f_0(\boldsymbol{t}) = C(x,\boldsymbol{t})\tilde{F}(x,\boldsymbol{t}) + \Delta_F, \\ G(x,\boldsymbol{t}) &= g_n(\boldsymbol{t})x^n + \ldots + g_0(\boldsymbol{t}) = C(x,\boldsymbol{t})\tilde{G}(x,\boldsymbol{t}) + \Delta_G. \end{aligned}$$

ここで近似 GCD とは，近似共通因子 $C(x,\boldsymbol{t})$ の中で最大次数の多項式である．以下，問題が考えやすいよう $t_i \mapsto Tt_i$ $(1 \le i \le \ell)$ という変換がされた多項式が入力として与えられていることにする．この変換によって x と T の 2 つの変数だけに注目して計算することができる．また，全次数ごとに多項式を分割するため，次のように全次数で多項式を分割して斉次多項式の和として表現することにする：

$$F(x,\boldsymbol{t},T) = F^{(0)}(x) + T\cdot\delta F^{(1)}(x,\boldsymbol{t}) + T^2\cdot\delta F^{(2)}(x,\boldsymbol{t}) + \ldots = \sum_{i=0}^{w} T^i \cdot \delta F^{(i)}(x,\boldsymbol{t})$$

$F(x,\boldsymbol{0}) \times G(x,\boldsymbol{0}) = 0$，または，$\mathrm{lc}(F)|_{\boldsymbol{t}=\boldsymbol{0}} \times \mathrm{lc}(G)|_{\boldsymbol{t}=\boldsymbol{0}} = 0$ のとき，特異と呼ぶ ($\mathrm{lc}(F)$ は F の主係数)．非常に計算がしづらいことが知られて，よく問題とされる場合になる．本稿では特異な場合を検討する．

多変数多項式の近似 GCD 計算の方法を分類すると，互除法のように直接計算する方法 [13, 12]，補間法による方法 [20, 9]，巨大な数値行列を用いる方法 [7, 19] 射影によって変数を減らした空間で近似 GCD 計算を計算しリフティングによって得たい近似 GCD を復元する方法 (以下で触れる)，などがある．本稿では，リフティング法に基づく方法を検討する．リフティング法は初期因子によって，大きく精度が変わってきたり，そもそも計算ができずに計算が破綻することがある．

*1 〒 305-8575 茨城県つくば市天王台 1-1-1　E-mail: sanuki@md.tsukuba.ac.jp

Hensel 構成 (EZ-GCD 法) の場合には初期因子の組が互い素でない場合には不安定になるため，いくつかの工夫がなされているが，これらの改良はうまくいかないと予想される．拡張 Hensel 構成 [17] を用いる方法は，「初期因子の組が互い素でない場合」の Hensel 構成の問題点を解決する方法ではあるが有理関数を扱う必要があり，効率の面で問題が残ることを別の場所で報告した．Hensel 構成は初期因子が 2 つ以上の多項式の組からなるため，計算が不安定になる場合が多くなってしまうことが多い．次に計算の流れを示した．

1. 初期因子 $\tilde{C}^{(0)}$ and $\tilde{H}^{(0)}$ を計算 (互いに素であることが必要)：
   - $C^{(0)} = \gcd(F^{(0)}, G^{(0)})$, and $H^{(0)} = (aF^{(0)} + bG^{(0)})/C^{(0)}$

   ここで $a, b \in \mathbb{F}$ であり，$C^{(0)}$ と $H^{(0)}$ が互いに素になるようにするための工夫である (EEZ-GCD 法).
2. リフティング
   - $C^{(i)} = C^{(i-1)} + \delta C^{(i)}$ and $H^{(i)} = H^{(i-1)} + \delta H^{(i)}$
3. (必要あれば) 最適化

Hensel 構成に基づく方法の他，線型方程式を解をリフティングする方法を提案した [14, 16]．次は線型方程式を解をリフティングする方法を簡単に示したものである ($\mathcal{M}$ は多項式を要素とする行列，$\mathcal{M}^{(w)}$ は $\mathcal{M}$ の各要素について w までの項を取り出した行列．詳細は次の章で定義する).

$$
\begin{array}{ccc}
\mathcal{M}^{(0)}\boldsymbol{x} = \boldsymbol{b}^{(0)} & & \boldsymbol{x} = \boldsymbol{c}^{(0)} \\
 & \Downarrow & \\
\mathcal{M}^{(1)}\boldsymbol{x} = \boldsymbol{b}^{(1)} & & \boldsymbol{x} = \boldsymbol{c}^{(1)} = \boldsymbol{c}^{(0)} + \delta\boldsymbol{c}^{(1)} \\
 & \Downarrow & \\
 & \vdots & \\
 & \Downarrow & \\
\mathcal{M}^{(w)}\boldsymbol{x} = \boldsymbol{b}^{(0)} & & \boldsymbol{x} = \boldsymbol{c}^{(w)} = \boldsymbol{c}^{(w-1)} + \delta\boldsymbol{c}^{(w)}
\end{array}
$$

初期因子は数値行列となるため，計算を精度良く計算できる数値計算のアイデアを用いることができる．また，組み合わせて初期因子を構成するわけではないので，Hensel 構成のように組み合わせによる不安定さは解消されると考えられる．残るは初期因子として選択する行列が正則か非正則の方がよいのか検討する必要がある．

[14] では，Barnett の定理 [1, 2] を多変数へ拡張して多変数多項式を要素とする Bezout 行列の部分行列 $\mathcal{B}$ を利用した方法を提案した．2 つの Bezout 行列 $\mathcal{B}, \mathcal{B}^{(0)}$ はそれぞれ正則であり，正則な行列 $\mathcal{M} = \mathcal{B}$ の線型方程式をリフティング法によって解いた (解の各要素は多項式になるように問題を正規化可能である)．直接法が利用できるケースであり効率よく計算できる．ただし，問題のサイズ・次数が大きくなると行列はそれに伴って大きくなるため，条件数がすぐに大きくなる，正則であるが非常に特異になるようなケースがすぐにでるために直接法では限界がでてくる．反復法によって改善はされるが，検討が十分にできていない状況である [15].

[16] では，多変数多項式を要素に持つ Sylvester 行列の部分行列 $\mathcal{S}$ の零空間を求めるリフティング法を提案した．GCD ないし近似 GCD の計算のため部分行列 $\mathcal{S}$ および $\mathcal{S}^{(0)}$ は正則ではなく自由度が 1 である行列になる (零空間の計算が GCD 計算に直結する)．特異値分解などの計算などで $\mathcal{S}^{(0)}\boldsymbol{x} = \boldsymbol{0}$ が計算することができるので精度良く計算することが可能である[1].

[1] Bezout 行列の場合も，特異値分解によって精度良く計算できる．ただし，Sylvester 行列の場合と効率に大差がなくなる．

ここまでの議論を読む限り，行列のリフティング法に基づく方法で決着がついたように思えるが実はそうではない．$\mathcal{B}$ ないし $\mathcal{S}$ が 0 行列になる場合があり (入力が特異と呼ぶ)．このときは計算が破綻する．解決するために先に述べた拡張 Hensel 構成を検討したが問題を完全に解決するに至らなかった．

本稿では，入力が特異な場合を解決するため，代数幾何学でよく利用されるブローアップのアイデアを用いる．ブローアップとは特異点を解消するための代数幾何におけるテクニックであり，メビウスの帯を想定した写像・変換として知られる．簡単な変換で特異な場合が解消されるだけでなく，問題の本質が変わらないために近似 GCD の計算に向いていると考えられる．すると本稿で問題にするリフティング法に基づく方法は初期因子で実行するべき計算の精度・効率性を検討することによって簡単な比較が可能になり，本稿ではそれを行う．

2 特異値分解を用いる方法

項式を要素とする $k-1$ 次部分終結式行列 $\mathcal{S}_{k-1}(F,G)$ は次で表現される．

$$
\begin{aligned}
\mathcal{S}_{k-1}(F,G) &= \begin{pmatrix} \overbrace{\begin{matrix} f_m & & \\ f_{m-1} & f_m & \\ \vdots & \ddots & \ddots \end{matrix}}^{n-k+1} & \overbrace{\begin{matrix} g_n & & \\ g_{n-1} & g_n & \\ \vdots & \ddots & \ddots \end{matrix}}^{m-+1k} \end{pmatrix} \in \mathbb{F}[\boldsymbol{t},T]^{K\times K} \\
&= \mathcal{S}_{k-1} = \mathcal{S}_{k-1}^{(0)} + T\cdot\delta\mathcal{S}_{k-1}^{(1)} + \ldots + T^w\cdot\delta\mathcal{S}_{k-1}^{(w)} + \ldots
\end{aligned}
$$

ここで $K=m+n-2k+2$，$\delta\mathcal{S}_{k-1}^{(i)} \in \mathbb{F}[\boldsymbol{t}]$ である ($i\geq 0$，$\delta\mathcal{S}_{k-1}^{(0)} = \mathcal{S}_{k-1}^{(0)}$)．

本稿で述べるリフティング法において必要となる方程式系を構成する．求めるべきは次の線形方程式の解 (零空間) $\boldsymbol{x} = \boldsymbol{z} = \boldsymbol{z}^{(0)} + T\cdot\delta\boldsymbol{z}^{(1)} + \cdots + \in \mathbb{F}[\boldsymbol{t}]^K$ である ($\delta\boldsymbol{z}^{(i)} \in \mathbb{F}[\boldsymbol{t}]^K$ for $i \geq i$)．

$$
\mathcal{S}_{k-1}\boldsymbol{x} = \boldsymbol{0}. \tag{1}
$$

$\mathbb{F}[\boldsymbol{t}]^K$ 上の空間において $\mathcal{S}_{k-1}$ の階数は $K-1$ である．全次数変数 T を適切に設定することにより $\mathcal{S}_{k-1}^{(0)}$ の階数も $K-1$ にできる．この仮定のもと，$\mathcal{S}_{k-1}\boldsymbol{z}^{(w)} \equiv \boldsymbol{0} \pmod{T^{w+1}}$ を $w\geq 0$ について下から順にリフティング法で解く．ここで，$\boldsymbol{z} = \boldsymbol{z}^{(0)} + T\cdot\delta\boldsymbol{z}^{(1)} + \cdots + T^w\cdot\delta\boldsymbol{z}^{(w)} \in \mathbb{F}[\boldsymbol{t}]^K$ である

2.1 初期因子の決定 ($w=0$ の場合)

$\mathcal{S}_{k-1}^{(0)}\boldsymbol{x} = \boldsymbol{0}$ を解く．リフティング法を実行する上で $\mathcal{S}_{k-1}^{(0)}\boldsymbol{y} = \boldsymbol{c}^{(i)}$ for $i\in\mathbb{N}$ を何度も解くので $\mathcal{S}_{k-1}^{(0)} = \mathcal{A}^T\mathcal{B}$ と利用しやすい形で計算することが重要となる ($\mathcal{A}^T$ は逆行列も計算，$\mathcal{B}$ は三角行列，など)．

- $\mathcal{S}_{k-1}^{(0)} \in \mathbb{F}^{K\times K}$ のとき，特異値分解を利用すると計算が非常に効率的であり，算法を高速化できる [?].
- $\mathcal{S}_{k-1}^{(0)} \in \mathbb{F}[\boldsymbol{t}]^{K\times K}\backslash\mathbb{F}^{K\times K}$ のとき，行列の各要素は斉次多項式であり，一般的に疎である．サイズの小さい場合には LU 分解でも分解可能であるが，20 次くらいのサイズになると工夫が必要となる (現時点での課題).

2.2　リフティング $(w \geq 0)$

$z^{(w-1)} = \boldsymbol{z}^{(0)} + \sum_{i=1}^{w-1} T^i \delta z^{(i)}$ まで計算できたと仮定する．このとき，$\boldsymbol{z}^{(w)} = \boldsymbol{z}^{(w-1)} + T^w \cdot \delta \boldsymbol{z}^{(w)}$ について，$\mathcal{S}_{k-1}\boldsymbol{z}^{(w)} \equiv \boldsymbol{0} \pmod{T^{w+1}}$ を整理することによて，次の式を得る．

$$\mathcal{S}_{k-1}^{(0)}\delta\boldsymbol{z}^{(w)} \quad = \quad -\sum_{j=1}^{w}\mathcal{S}_{k-1}^{(j)}\delta\boldsymbol{z}^{(w-j)} = \delta\boldsymbol{p}^{(w)}$$

この線形方程式を解くことによって，$\delta\boldsymbol{z}^{(w)}$ を得る．

2.3　解を定めるためのアイデア

リフティング法を用いる近似 GCD 計算において問題となるのは単元の不定性であり，解の候補を得てから解を定める必要がある．

$\mathcal{S}_{k-1}\boldsymbol{x} \equiv \boldsymbol{0} \pmod{T^{w+1}}$ の計算によって得られる解は $\boldsymbol{x} = \boldsymbol{z} = \boldsymbol{z}' + r(\boldsymbol{t}) \cdot \ker \mathcal{S}_{k-1}^{(0)}$ であり，$r(\boldsymbol{t}) \in \mathbb{F}[\boldsymbol{t}]$ だけ自由度がある．近似 GCD 自身は摂動を除いて一意であるため，$r(\boldsymbol{t})$ も摂動を除いて一意に定まる．

余因子 $\tilde{G}$ と $-\tilde{F}$ の係数が次で表される．

$$\boldsymbol{z} = \begin{pmatrix} \tilde{g}_{n-k} \\ \vdots \\ \tilde{g}_0 \\ -\tilde{f}_{m-k} \\ \vdots \\ -\tilde{f}_0 \end{pmatrix} = \boldsymbol{z}' + r(\boldsymbol{t}) \cdot \ker \mathcal{S}_{k-1}^{(0)} = \begin{pmatrix} \tilde{g}'_{n-k} & + & r \cdot v_{K,1} \\ & \vdots & \\ \tilde{g}'_0 & + & r \cdot v_{K,n-k} \\ -\tilde{f}'_{m-k} & + & r \cdot v_{K,n-k+1} \\ & \vdots & \\ -\tilde{f}'_0 & + & r \cdot v_{K,K} \end{pmatrix}$$

ここで得られた解には単元の不定性によって実際にほしい値にはなっていないため，近似 GCD の主係数を求めることでこの問題を解決する．$c_k = \gcd(\mathrm{lc}(F), \mathrm{lc}(G))$ を計算する．このとき $\tilde{g}_{n-k} = g_n / c_n$ が計算できるので，$r(\boldsymbol{t}) = \tilde{g}_{n-k} - \tilde{g}'_{n-k}$ を得る．

2.4　算法の限界

初期行列と入力行列の階数が同じである必要があり，特異な場合においてはこれが満たされない．初期行列が数値であり (特異でない)，階数が同じになるような工夫を考えることが本稿の目的である．

3　ブローアップによる特異点解消；GCD 計算の正規化

ブローアップとは特異点を解消するための代数幾何におけるテクニックであり，メビウスの帯を想定した写像・変換として知られる．簡単な変換で特異な場合が解消されるだけでなく，問題の本質が変わらないために近似 GCD の計算に向いていると考えられる．

次はよく知られた例でる [18].

例 1
代数曲線 $P : y^2 - x^3$ は，原点で特異である．このとき，次の変換 (ブローアップ) によって特異点が解消できる．

- $(x,y)=(u,uv)$ なる変換：$u^2v^2-u^3=u^2(v^2-u)$
- $(u,v)=(pq,p)$ なる変換：$p^6q^3(q-1)$

逆変換 (ブローダウン) によって，もとの曲線に戻ることもすぐに確認できる．例からわかる通り，複数回のブローアップによって特異点が解消でき，どのくらいブローアップするべきかについて，さらに次の定理が知られている．

定理 1
有限回のブローアップの操作によって特異点が解消される。 ∎

それゆえ，有限回の操作で特異でない多項式に変換できる．GCD の計算においては次の点に注目して，ブローアップを行う．本稿では実例でしめす．

例 2
次の多項式は，同じ全次数をもつ斉次多項式である *(*初期因子を構成する多項式*)*.

$$F^{(0)}=y^2-x^2, G^{(0)}=x^2+2xy+y^2$$

この多項式の *GCD* は t_2+t_1 である．ブローアップによって *GCD* がどのように変化するかみる．ブローアップは次で行う．

- $(x,y)=(u,uv)$ なる変換

$$\begin{aligned} {}_1F^{(0)}(u,v) &= u^2v^2-u^2=u^2(v^2-1)=u^2(v-1)(v+1) \\ {}_1G^{(0)}(u,v) &= u^2v^22u^2v+u^2=u^2(v^2+2v+1)=u^2(v+1)^2 \end{aligned}$$

${}_1F^{(0)}$ と ${}_1G^{(0)}$ の *GCD* は $u^2(v+1)$ であり，ブローアップの操作によって u が余計にかかっているが，ブローダウンによって *GCD* そのものが得られるため，*GCD* の計算に利用できることがわかる．この例では

$$\begin{aligned} F(x,y) &= F^{(0)}+\delta F^{(1)}+\cdots \\ &\downarrow \\ {}_1F(u,y) &= u^2\times\{{}_1F^{(0)}+\delta_1F^{(1)}+\cdots\} \end{aligned}$$

であることを示しており，中括弧の中について検討することで特異でない問題が扱えることを示している．

例 3
次の多項式について考える．

$$F^{(0)}(x,u_1,u_2)={u_2}^2x^4+(u_2{u_1}^2+{u_2}^3)x^3+(2{u_1}^3u_2+{u_2}^4)x^2+(2{u_2}^2{u_1}^3+{u_2}^5)x+{u_1}^6+{u_2}^3{u_1}^3$$

主係数が特異なため，変数 u_2 を消す操作を考える．ここでは次の変換を行う．

- $x\mapsto u_2x$
- $u_1\mapsto u_1u_2$
- $u_2\mapsto u_2$

この変換の結果，次を得る．

$$\begin{aligned} F^{(0)} &\to u_2^6 \times \Big\{ x^4 + (u_1^2+1)x^3 + (2u_1^3+1)x^2 + (2u_2^2+1)x + 1 + u_2^3 \Big\} \\ &= u_2^6\{(x^2+x+u_1^3)\}\{(x^2+u_1x+1+u_1^3)\} \end{aligned}$$

このとき，入力多項式は $F \to u_2^6\Big\{{}_1F^{(0)}(x) + {}_1\delta F^{(1)}(x,u_1,u_2) + \ldots\Big\}$ となる．中括弧の中をみると初期多項式は *1* 変数多項式になっている．

入力が斉次多項式のため，主係数が単項であれば簡単に特異でない状態に変換でき，GCD 計算をこれまでの算法で実行することが可能になる．

次の例は主係数が単項でない場合である．

例 4

次の多項式について考える．

$$\begin{aligned} F^{(0)}(x,u_1,u_2) &= (u_1u_2+{u_2}^2)x^4 + ({u_1}^3+u_2{u_1}^2+{u_2}^3)x^3 + ({u_1}^3u_2+{u_1}^4+u_1{u_2}^3+{u_1}^3u_2+{u_2}^4)x^2 \\ &\quad +({u_1}^5+{u_2}^2{u_1}^3+{u_2}^5)x + {u_1}^6+{u_2}^3{u_1}^3 \end{aligned}$$

ブローアップによって，主係数が特異でないように変換できればよい．この例では，どの変数に注目すればよいかわからないので，各変数 u_1 と u_2 のそれぞれに注目をしてブローアップの操作をする．

1. u_1 に注目する．

- $x \mapsto u_1x$
- $u_1 \mapsto u_1$
- $u_2 \mapsto u_1u_2$

このとき次を得る．

$$\begin{aligned} F^{(0)} &\to u_1^6 \times \\ &\quad \Big\{(u_2+u_2^2)x^4 + (1+u_2+u_2^3)x^3 + (u_2+1+u_3^3+u_2+u_4)x^2 + (1+u_2^2+u_5)x + 1 + u_2^3\Big\} \\ &= u^6\{(1+u_2)x+u_2^2x+1\}\{(u_2x^2+x+1+u_2^3)\} \end{aligned}$$

このとき，入力多項式は $F \to u_1^6\Big\{{}_1F^{(0)}(x,u_2) + {}_1\delta F^{(1)}(x,u_2,u_1) + \ldots\Big\}$ であり，初期多項式が *1* 変数に帰着できるわけではなく，主係数は特異なままのため，中括弧の中で再度ブローアップをする必要があるが，主係数が特異でなくなるような変換が必要になる．

2. u_2 に注目する．

- $x \mapsto u_2x$
- $u_1 \mapsto u_2u_1$
- $u_2 \mapsto u_2$

次を得る．

$$\begin{aligned} &u_2^6 \times \Big\{(u_1+1)x^4 + (u_1^3+u_1^2+1)x^3 + (u_1^3+u_1^4+u_1+u_1^3)x^2 + (u_1^5+u_1^3+1)x + u_1^6 + u_1^3\Big\} \\ =\ &u_2^6\Big\{(u_1+1)x^2+x+u_1^3\Big\}\Big\{x^2+u_1^2x+u_1^3+1\Big\} \end{aligned}$$

このとき，入力多項式は $F \to u_2^6\Big\{{}_1F^{(0)}(x) + {}_1\delta F^{(1)}(x,u_1,u_2) + \ldots\Big\}$ となる．主係数の次数の高い方に注目してブローアップすると特異性が消える．これは斉次多項式であることに由来する．

次の例は 1 回のブローアップで特異点が解消されない例になる．

例 5

$$F^{(0)}(x,u_1,u_2) = u_1u_2x^4 + (u_1^3+u_2^3+u_2u_1^2)x^3 + (u_1^4+u_1u_2^3+u_2u_1^3-u_2^4)x^2 + (u_1^5+u_2^5)x + u_1^6 - u_2^6$$

次の変換を行う．

- $x \mapsto u_2x$
- $u_1 \mapsto u_2u_1$
- $u_2 \mapsto u_2$

このとき，次を得る．

$$\begin{aligned} & u_2^6 \times \{u_1x^4 + (u_1^3+1+u_1^2)x^3 + (u_1^4+u_1+u_1^3-1)x^2 + (u_1^5+1)x + (u_1^6-1)\} \\ = \; & u_2^6 \times \Big\{u_1x^2 + (1+u_1^2)x + u_1^3 - 1)\Big\}\Big\{(x^2 + u_1^2x + 1 + u_1^3)\Big\} \end{aligned}$$

1 変数に帰着できるわけではないことがわかる．主係数が特異なことが問題であったが，主係数の変数は *1* つ減少させることはできるので数回の操作によって主係数が特異でないようにできることがわかる．

この例では中括弧の中の多項式に注目して再度ブローアップを行うとよい．

参 考 文 献

[1] S. Barnett. *Greatest common divisor of two polynomials.* Linear Algebra Appl., **3**, 1970, 7–9.

[2] S. Barnett. *Greatest common divisor of several polynomials.* Proc. Camb. Phil. Soc., **70**, 1971, 263–268.

[3] V. Bhargava, S. Saraf and I. Volkovich, *Deterministic Factorization of Sparse Polynomials with Bounded Individual Degree*, 2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS), 485–496, 2018.

[4] 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.

[5] G. M. Diaz-Toca and L. Gonzalez-Vega. *Barnett's theorems about the greatest common divisor of several univariate polynomials though Bezout-like matrices. J. Symb. Compu.*, **34**, (2002), 59–81.

[6] J. zur Gathen and E. Kaltofen, *Factoring sparse multivariate polynomials*, J. of Comput. Syst. **31(2)**, 1985, 265–287.

[7] 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.

[8] F. Kako and T. Sasaki. Proposal of "effective floating-point number" for approximate algebraic computation. *Preprint of Tsukuba Univ.*, 1997.

[9] Z. Li, Z. Yang, and L. Zhi. Blind image deconvolution via fast approximate GCD *Proc. of ISSAC'10*, ACM Press, 2010, 155–162.

[10] 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.

[11] M. Sanuki, D. Inaba and T. Sasaki: Computation of GCD of sparse multivariate polynomials by extended Hensel construction, *Proc. of SYNASC 2015*, IEEE, 2015, 34–41.

[12] M. Sanuki and T. Sasaki, *Computing approximate GCDs in ill-conditioned cases*, Proc. of Symbolic-Numeric Computation 2007 (SNC 2007), 2007, 170–179.

[13] M. Sanuki, *Computing approximate GCD of multivariate polynomials (Extended abstract)*, International Workshop on Symbolic-Numeric Computation 2005 (SNC 2005), D. Wang & L. Zhi (Eds.), 2005, 308–314; full paper appear in Symbolic-Numeric Computation (Trends in Mathematics), D. Wang & L. Zhi (Eds.), Birkhäuser Verlag, 2007, 55–68.

[14] M. Sanuki. *Computing multivariate approximate GCD based on Barnett's theorem*, Proc. of Symbolic-Numeric Computation 2009 (SNC 2009), 2009, 149–157.

[15] 讃岐勝．*Jacobi* 法を基にした多項式要素の線形方程式の解法，第 42 回数値解析シンポジウム講演予稿集, 2013, 144–147

[16] 讃岐勝．多変数近似 *GCD* 計算のための *Sylvester* 部分行列の *null* 空間の効率的計算，日本数式処理学会第 28 回大会にて発表, 2019 年 5 月 31 日–6 月 2 日 (学会誌「数式処理」に掲載予定)

[17] T. Sasaki and F. Kako, *Solving multivariate algebraic equation by Hensel construction*, Japan J. Indust. Appl. Math., 16(2), 1999, 257–285.

[18] 上野健爾，代数幾何入門，岩波書店，1995.

[19] 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.

[20] L. Zhi and M-T. Noda, *Approximate GCD of Multivariate Polynomials*, Proc. of ASCM2000, World Scientific, 2000, 9–18.