数理解析研究所講究録
第1568巻 2007年 108-114

異常な多変数多項式の近似GCD計算法

讃岐 勝
Masaru Sanuki
筑波大学 数理物質科学研究科
Graduate School of Pure and Applied Sciences, University of Tsukuba *

佐々木 建昭
Tateaki Sasaki
筑波大学 数学系
Institute of mathematics, University of Tsukuba †

Abstract

浮動小数係数の剰余列計算における種々の悪条件問題 (微小主係数、微小主係数 GCD、巨大主係数、特異的な主係数) について考察し、対応策を提案する。さらに、悪条件を克服する3つの算法を提示する：それらは 1) 微小主係数多項式による除算を回避する1変数剰余列の安定した生成法、2) 安定した剰余列生成法の多変数多項式への拡張、3) QRGCD 法の多変数多項式への直接的拡張、である。

1 はじめに

1980年代末に近似代数の概念が提唱されて以来、多種多様な研究がされている。その中で近似GCDを計算する算法も数多く提案されている。1変数多項式では、quasi-GCD[Sch85]、多項式剰余列 (PRS) 法 [SN89]、特異値分解による算法 [CGTW95, Zen04]、QRGCD 法 [OST97, ZMF00, CWZ04]、ε-GCD[EGL97]、Padé-GCD[Pan01]、構造行列を用いる算法 [Zhi03]、などがある。PRS 法は効率的であるが、微小主項の多項式が現れた場合に不安定になる。計算量は多項式の次数を m とするとき $O(m^2)$ である。QRGCD 法は多くの場合に安定している算法で、計算量は $O(m^3)$ である。Corless *et al.*[CWZ04] は微小主係数 GCD を持つ場合に桁落ちすること指摘しており、それに対する解決策を与えている。Zhi [Zhi03] は構造行列を用いて計算量 $O(m^2)$ の高速算法を提案している。現在では、安定性の面から QRGCD 法が広く利用されている。

多変数多項式では、PRS 法 [ONS91] および近似 PC-PRS 法 [San05]、補間法 [CGTW95]、近似 EZ-GCD 法 [ZN00]、一般 Sylvester 行列の特異値分解による算法 [GKMYZ04, ZD04]、構造行列を用いる算法 [KYZ06]、などがある。PRS 法は近似 PC-PRS 法による改良により大幅に計算効率があがったが、1変数の場合と同様に微小主係数のときに不安定になってしまう。一般 Sylvester 行列に特異値分解を適用する算法は2つあり ([GKMYZ04] と [ZD04])、両者は行列の構成法が異なるが、変数の個数や次数が増えると一般 Sylvester 行列のサイズが急激に膨張してしまうため、変数の個数が多いか高次の場合には計算効率が大きく落ちる。

本稿では、PRS 法の安定化を考える。2 では、1変数 PRS 法において微小主係数の場合になぜ不安定になるのか考察し、安定した算法を提案する。そして、QRGCD 法と同等の精度を持つことを示す。3 では、多変数多項式においても同じ工夫で安定に計算できることを確認し、QRGCD 法を多変数多項式に直接的に拡張した算法を提案する。4 では、ほかの3つの悪条件問題（微小主係数 GCD、巨大主係数、特異的な主係数）について考察する。5 では数値実験により提案した算法の有効性を確認する。

*sanuki@math.tsukuba.ac.jp
†sasaki@math.tsukuba.ac.jp

多項式 F に対して、$\mathrm{lc}(F)$ と $\deg(F)$ は F の主係数と次数をそれぞれ表す。多項式ノルムを $||F||$ と表し、数係数の絶対値の最大値で定義する。なお、与える多項式 F は $||F|| = 1$ と規格化されているものとする。$\mathrm{quo}(F,G)$ と $\mathrm{rem}(F,G)$ は F を G で割った商と余りをそれぞれ表す。

2 1変数多項式剰余列の安定化

1変数多項式 $F(x), G(x) \in \mathbb{C}[x]$ を次のように表す：

$$F(x) = f_m x^m + \cdots + f_0, \quad G(x) = g_n x^n + \cdots + g_0 \quad (f_m, g_n \neq 0,\ m \geq n). \tag{1}$$

$|g_n|/|f_m| = \varepsilon \ll 1$ を仮定する。$Q(x) = \mathrm{quo}(F,G)$ および $\mathrm{rest}(G) = g_{n-1}x^{n-1} + \cdots + g_0$ とするとき

$$\mathrm{rem}(F,G) \quad = \quad F - \left[Q(x)/{g_n}^{m-n+1}\right] G = H \approx -Q(0)\,\mathrm{rest}(G) \tag{2}$$

となり、H が $\mathrm{rest}(G)$ に近いため、$\mathrm{rem}(G,H)$ は $O(1/\varepsilon^{m-n+1})$ の桁落ちを起こす。この桁落ち現象を**自己簡約**と呼ぶ。安定して剰余列を計算するためには自己簡約を避けなければならない。

$\gcd(F,x) = 1$ であるとき $\gcd(F,G) = \gcd(x^{m-n}G, F)$ であることに注目する。$|g_n| < |f_m|$ ならば、$\mathrm{rem}(F,G)$ の代わりに主項消去 $\mathrm{elim}(x^{m-n}G, F)$ を行い、剰余列 $(x^{m-n}G, F, \mathrm{elim}(x^{m-n}G, F), \cdots)$ を生成すると自己簡約を避けて計算できる。しかし、$\mathrm{elim}(x^{m-n}G, F)$ において微小定数項 $-[g_n/f_m]f_0$ が生じて計算が不安定になる。そこで、$\mathrm{elim}(x^{m-n}G, F)$ を次のように工夫する。

定義 (ダミー) 次式を満たす多項式を G の F に対するダミーと呼ぶ：

$$\mathrm{dummy}(G) = (x^{m-n} + a)\,G \quad (\deg(a) < m - n). \tag{3}$$

ただし、a は $||a|| = 1$ であり、$(x^{m-n} + a)$ が F と近似共通因子を持たないように選ぶ。 ∎

a の導入により微小定数項による不安定さが解消される。$P_3 = \mathrm{elim}(\mathrm{dummy}(G), F)$ の主係数は多くの場合に小さくないが、小さい場合には再び $\mathrm{elim}(\mathrm{dummy}(P_3), F)$ を計算する。そして主係数が小さくない多項式が得られるまで繰り返す。このように剰余列を生成する算法を**安定化 PRS 法**と呼ぶ。

アルゴリズム 1 (安定化 PRS 法)

Input :	*Polynomials* P_1 *and* P_2, *and tolerance* ε $(0 \leq \varepsilon \ll 1)$.
Output:	*a PRS* $(P_1, P_2, P_3, \cdots, P_k, P_{k+1})$, *where* $||P_{k+1}|| = O(\varepsilon)$ *or* $\deg(P_{k+1}) = 0$.
	$i := 2$;
LP:	*if* $\deg(P_i) = 0$ *or* $||P_i|| = O(\varepsilon)$ *then return PRS*;
REM:	*if* $\lvert\mathrm{lc}(P_i)\rvert \approx \lvert\mathrm{lc}(P_{i-1})\rvert$ *then* $P_{i+1} := \mathrm{rem}(P_{i-1}, P_i)$
	else $\langle\langle$ $P_{i+1} := \mathrm{elim}(\mathrm{dummy}(P_i), P_{i-1})$; $P_i := P_{i+1}$; *goto* REM $\rangle\rangle$;
	$i := i + 1$; *goto* LP;
	end;

命題 1 (安定化 PRS 法の停止性) 安定化 PRS 法において REM ループは停止する。 ∎

注意 (拡張 Euclid 互除法) $P_1, P_2 \in \mathbb{C}[x]$ が与えられたとき、安定化 PRS 法は $A_i(x)P_1 + B_i(x)P_2 = P_i(x)$ を満たす $A_i, B_i, P_i \in \mathbb{C}[x]$ を計算する算法にただちに拡張できるが、次数条件 $\deg(A_i) < \deg(P_2) - \deg(P_i)$ および $\deg(B_i) < \deg(P_1) - \deg(P_i)$ は満たさない。 ∎

安定化 PRS 法と QRGCD 法について比較する。QRGCD 法は Sylvester 行列を QR 分解することで近似 GCD を計算する。分解は Householder 変換あるいは Givens 回転を用いて行う (以下では Givens 回転のみを考える)。F と G の Sylvester 行列 S を次のように表す：

$$S = \begin{pmatrix} f_m & f_{m-1} & \cdots & \cdots \\ & f_m & f_{m-1} & \cdots \\ & & \ddots & \cdots \\ g_n & g_{n-1} & \cdots & \cdots \\ & g_n & g_{n-1} & \cdots \\ & & \ddots & \cdots \end{pmatrix} \in \mathbb{C}^{(m+n)\times(m+n)}. \tag{4}$$

S は QR 分解により、直交行列 Q と上三角行列 R で $S = QR$ と分解できる。このとき、$R = (r_1, r_2, \cdots, r_{m+n})^T$ の行 r_i および Euclid ノルム $||r_i||_2$ に着目する ($||r_i||_2 \geq ||r_{i+1}||_2$)。自明でない許容度 ε の近似 GCD が存在することと、$1 \approx ||r_d||_2 \gg ||r_{d+1}||_2 \approx \varepsilon$ となる列 r_{d+1} が存在することは同値である。このとき、$r_d = (0, \cdots, r_{d,d}, \cdots, r_{d,m+n})$ は F と G の近似 GCD $r_{d,d}x^{m+n-d} + \cdots + r_{d,m+n}$ の係数に対応する。R は Givens 回転による 1 次変換を繰り返すことで生成される。

$\mathrm{dummy}(G) = (x^{m-n} + a)G$ において $a = a_{m-n-1}x^{m-n-1} + \cdots + a_0$ と表すと、$\mathrm{elim}(\mathrm{dummy}(G), F) = (x^{m-n} + a_{m-n-1}x^{m-n-1} + \cdots + a_0)G - (g_n/f_m)F$ となる。行列 M を次式で定める：

$$M = \begin{pmatrix} f_m & g_n & & \\ -g_n & f_m & & \\ & & 1 & \\ & & & \ddots \end{pmatrix} \prod_{i=0}^{m-n-1} \begin{pmatrix} 1 & & & \\ & 1 & & \frac{a_i}{f_m} \\ & & \ddots & \\ & -\frac{a_i}{f_m} & & 1 \\ & & & & \ddots \end{pmatrix}. \tag{5}$$

ただし、右辺の各行列は $(m-n+2)$ 次の回転行列で、各 a_i/f_m は $(2, m-n+2-i)$ 成分に対応する。このとき、$M(F, x^{m-n}G, \cdots, G)^T \propto (f_mF + g_nx^{m-n}G, \mathrm{elim}(\mathrm{dummy}(G), F), \cdots)^T$ である。故に、$\mathrm{elim}(\mathrm{dummy}(G), F)$ は Givens 回転を $(F, x^{m-n}G, \cdots, G)^T$ に対し反復することで得られ、QRGCD 法も Givens 回転を繰り返す算法である。また、$a = 0$ のときは $\mathrm{elim}(\mathrm{dummy}(G), F)$ は 1 回の Givens 回転で得られる要素に対応する。安定化 PRS 法の計算量について考察する。$|g_n| \geq |f_m|$ ならば $\mathrm{rem}(F, G)$ を計算し、$|g_n| < |f_m|$ ならば $\mathrm{elim}(\mathrm{dummy}(G), F)$ と計算を行うが、後者が実行されるのは高々 m 回程度なので、PRS 法のときと同様に計算量は $O(m^2)$ である。故に、次が言える。

命題 2 (安定化 PRS 法と QRGCD 法の比較)

- 安定化 PRS 法の計算量は $O(m^2)$ である。
- 安定化 PRS 法の精度は QRGCD 法とほぼ同等である。

∎

3 多変数多項式近似 GCD 計算の安定化

3.1 安定化 PC-PRS 算法

[San05] は多変数多項式の近似剰余列計算を打ち切りべき級数を用いて行い、効率よく近似 GCD を計算する方法を提案したが (近似 PC-PRS 法)、その算法は 1 変数の場合と同様の理由で微小主係数の場合には大きな桁落ちを起こす。ダミーによる安定化は多変数の場合にも適用することができ、剰余列計算が安定化されて近似 GCD を精度よく計算できる。これを安定化 PC-PRS 算法と呼ぶ。

例 1 (浮動小数上での近似 GCD の計算)
2変数多項式 $F(x,u)$ と $G(x,u)$ を次のように与える。

$$\begin{aligned} F(x,u) &= (x^2+u^2+1)(x^2-u-0.5)(x^2+u+0.1), \\ G(x,u) &= (x^2+u^2+1)(x+u^3+u-0.4)(0.0001x^2+u+1). \end{aligned}$$

係数を浮動小数化した F と G の近似 GCD を安定化 PC-PRS 算法によって計算すると次が得られた：

$$x^2 + 1.0 - \underline{4.410\cdots \times 10^{-13}u} + 0.999\cdots u^2 + \underline{0.000000000378\cdots u^3} - \underline{0.0000000302\cdots u^4}.$$

下線部は誤差項であり、正確に計算した場合には消えるはずの項である。 ∎

下線部の項が発生したのは「正確に打ち消し合うはずの項同志が計算過程で別々の誤差を持ったため打ち消されなかった」からである (0-判定)。アルゴリズムが良くても、この点を解決しなければ実際の計算はうまくいかないことを例 1 は示している。そこで、加古-佐々木によって提案された有効浮動小数 [KS97] を利用する。この数は浮動小数 f とその誤差 e のリスト $\#E[f,e]$ で表される (e の初期値は $e_{\text{init}} \cdot |f|$ であり、$e_{\text{init}} \approx 5.0 \times e_M$、$e_M$ はマシンイプシロン、である。実験は 2 倍長環境で行い、$e_{\text{init}} = 10^{-15}$ とした)。相対誤差により f の有効桁数を近似的に観測することが可能であり、さらに、$|f| < e$ のとき $\#E[f,e]$ は 0 と判定される。故に、上の状況においてほぼ正確に 0-判定を行うことが出来る。

例 2 (有効浮動小数上での近似 GCD の計算)
例 1 の $F(x,u)$ と $G(x,u)$ を有効浮動小数係数に変換してから近似 GCD を計算すると次の結果が得られた：

$$x^2 + \#E[1.0, 1.246\cdots\text{e}{-14}] + u^2.$$

打ち消しが正しく行われたことにより、非常に精度よく計算できたことが確認できる。 ∎

以下では、与えられた多項式を有効浮動小数係数に変換してから計算を行うことにする。

3.2 PC-GivensGCD 算法

2 で 1 変数多項式の QRGCD 法について考察したが、Givens 回転を基本とする QRGCD 法は直接的に多変数多項式に拡張することができる。

以下、従変数の組 $(u_1,\cdots,u_\ell)$ を (u) と表し、多変数多項式 $F(x,u)$ と $G(x,u) \in \mathbb{C}[x,u]$ の主変数 x に関する次数をそれぞれ m,n とする。$S \in \mathbb{C}[u]^{(m+n)\times(m+n)}$ を F と G の Sylvester 行列とする。S の要素は F と G の x^i の係数多項式である。S は Givens 回転 (ただし、回転行列は多項式要素になる) により上三角行列に変換できるが、そのままでは計算の過程で中間式膨張を引き起こすため効率が悪い。そこで、PC-PRS 法と同様に打ち切りべき級数として計算する。また、1 変数 QRGCD 法では変換する行それぞれの頭の要素の 2 乗和の平方根により回転行列をユニタリー化するが、多変数多項式の場合、多項式の平方根操作を行うのは現実的でなく、ユニタリー化は行わない。多変数の場合にはまったく別の規格化を行うが、それについては次節で述べる。この算法を Power-series Coefficient GivensGCD (PC-GivensGCD) 算法と呼ぶ。

3.3 多項式の規格化

浮動小数係数の剰余列計算においては規格化が非常に重要である。これまで [SN89, ONS91] や [SS97] によっていくつかの規格化の方法が提案されている。本稿では、有効浮動小数を用いることを前提に規格化を行う。多項式 P に対して次のように規格化を行う：

$$\tilde{P} = P \times \frac{e_{\text{init}}}{e_{\text{rest}}}. \tag{6}$$

ただし、e_{rest} は $\text{rest}(P)$ の係数の最大絶対誤差である。PC-GivensGCD 算法において、Sylvester 行列および変換によって得られる行列の各行はそれぞれ多項式の係数とみなすことができる。よって、剰余列計算のときの多項式と同様に規格化を行うことにする。

4 悪条件問題

2 と 3 では微小主係数問題を扱ったが、本章ではその他の悪条件問題を扱う。

4.1 微小主係数 GCD

Corless *et al.*[CWZ04] は、近似 GCD が微小主係数となる場合には 1 変数 QRGCD 法は精度を大きく落とすことを指摘し、解決法を提案している。この場合、安定化 PRS 法も同様に大きな桁落ちを起こす。

命題 3 (微小主係数 GCD) 近似 GCD の主係数の絶対値を ε とし、$\varepsilon \ll 1$ とする。剰余列算法において、主項消去の回数を k とするとき、$O(1/\varepsilon^k)$ の桁落ちが起きる。 ∎

1 変数多項式のとき、Corless *et al.* は Graeffe の方法によって単位円盤の中と外に根を持つ二つの多項式に分離し、スケール変換後それぞれについて近似 GCD を計算する方法を提案している。本稿では、[SK05] にある近似除算の反復による多項式分離を用いる。こちらの方が計算が簡単である。多変数多項式の場合には、PC-PRS 法および PC-GivensGCD 算法ともに打ち切りべき級数上で計算を行うので、次の 2 段階操作により、与多項式を主係数が小さい多項式とそうでない多項式に分離する：

1. 展開点を代入した 1 変数多項式を分離する
2. 必要な次数まで Hensel リフティングする

その後、スケール変換を行い、それぞれの因子について近似 GCD を計算する。

4.2 巨大主係数

1 変数多項式について考える (多変数多項式のときは問題にならない)。式 (1) で与えられた 1 変数多項式について $|f_m| \gg ||\mathrm{rest}(F)||$ および $|g_n| \approx ||G||$ を仮定する (巨大主係数)。このとき F の主項を G で消すと、$H = F - (f_m/g_n)x^{m-n}G \approx -(f_m/g_n)x^{m-n}\,\mathrm{rest}(G)$。したがって $\mathrm{rem}(H,G)$ は自己簡約となり大きな桁落ちを起こす。QRGCD 法も同様の理由で大きな桁落ちを起こす。この場合は、$G = G_h(x) + G_\ell(x)$、ただし $G_h(x) = g_n x^n + \cdots + g_{k+1}x^{k+1}$、$G_\ell(x) = g_k x^k + \cdots + g_0$、と分けてから次の計算を行う。

1. $A(x)f_m x^m + B(x)G_\ell(x) = \mathrm{appgcd}(f_m x^m, G_\ell(x); \varepsilon)$ を満たす $A(x)$ と $B(x)$ を計算する。
2. $A(x)$ と $B(x)$ によって F を変換する：

$$\begin{aligned} \tilde{F} &= A(x)F + B(x)G \\ &= A(x)\mathrm{rest}(F) + \mathrm{appgcd}(f_m x^m, G_\ell(x)) + B(x)G_h(x). \end{aligned} \tag{7}$$

上の変換の後、$\tilde{F}$ と G の近似 GCD を計算する。

4.3 特異的な主係数

多変数多項式の近似 GCD 計算は打ち切りべき級数上で行うが、主係数の加算と除算を用いるため、主係数の定数項の扱いに注意が必要となる。$G(x,u)$ の主係数を $g_n(u) = g_n^{(0)} + g_n^{(1)}(u) + \cdots + g_n^{(E)}(u)$ と表す。ただし、$g_n^{(i)}$ は u についての全次数 i の項の和および E は打ち切り次数である。$||g_n|| \approx ||G||$ を仮定する。

1. $|g_n^{(0)}| \approx ||g_n||$ の場合
   このときは安定して計算を行うことができる。
2. $|g_n^{(0)}| \ll ||g_n||$ の場合
   多くの場合、G によるべき級数除算で得られる多項式の精度は低くなる。また、得られた近似 GCD 候補 $\tilde{P}$ から近似 GCD を計算するためには、$\mathrm{lc}(\tilde{P})$ で $\tilde{P}$ をべき級数除算するが、この計算も不安定になる。この場合は展開点を変えて計算を行わなければならない。
3. $f_m^{(0)} = g_n^{(0)} = 0$ の場合
   べき級数上で計算を行う場合、定数項が重要である。この条件の下で計算を行うためには E を非常に大きく設定する必要があり、効率が悪い。この場合も展開点を変えて計算を行う必要がある。

5 実験

GAL に安定化 PC-PRS 算法と PC-GivensGCD 算法を実装し、Ultla SPARC-IIi (440MHz) の Solaris 8 上で実験を行った。表の中で ErrMax は有効浮動小数で計測した近似 GCD の最大相対誤差を表す。

	安定化近似 PC-PRS		PC-GivensGCD	
Ex.	Ave. CPU	ErrMax	Ave. CPU	ErrMax
1	0.025	5.00×10^{-13}	0.990	2.98×10^{-15}
2	0.017	7.79×10^{-13}	1.540	2.12×10^{-14}
3	0.956	3.11×10^{-15}	12.423	7.30×10^{-10}
4	0.062	1.74×10^{-12}	0.136	3.15×10^{-8}
5	0.099	4.11×10^{-13}	1.202	4.27×10^{-12}
6	0.127	1.57×10^{-12}	9.260	Error
7	0.091	3.39×10^{-11}	0.680	2.41×10^{-14}
8	0.102	8.11×10^{-13}	0.578	Error

表 1: 安定化 PC-PRS 算法と PC-GivensGCD の比較 (秒)

Ex.1〜3 は互いに素である 3 変数多項式を与え、x に関する次数を順に大きくした (Ex.1, 2, 3 で次数はそれぞれ 5, 10, 12)。PC-GivensGCD 算法は次数に比例して Sylvester 行列が大きくなるため時間がかかった。PC-PRS 法はそれほどでもない (従変数の個数や次数を増やしても大して効率が落ちないことは [San05] が実証している)。Ex.4 では微小主係数 GCD を持つ 2 変数多項式を与えた。微小主係数多項式部分を分離することで精度よく計算できたことがわかる。Ex.5〜8 では 3 変数多項式を次のように与えた：

$$\begin{cases} F_5 = a_1c_1 + 10^{-5}e_1 \\ G_5 = b_1c_1 + 10^{-5}d_1 \end{cases}, \quad \begin{cases} F_6 = a_1c_1 + 10^{-2}e_1 \\ G_6 = b_1c_1 + 10^{-2}d_1 \end{cases},$$

$$\begin{cases} F_7 = a_2c_2 + 10^{-5}e_2 \\ G_7 = b_2c_2 + 10^{-5}d_2 \end{cases}, \quad \begin{cases} F_8 = a_2c_2 + 10^{-2}e_2 \\ G_8 = b_2c_2 + 10^{-2}d_2 \end{cases}.$$

ただし、$||a_i||, ||b_i||, ||c_i||, ||e_i||, ||e_i|| = 1$ である。Error は正しい近似 GCD を得られなかったことを表す。PC-GivensGCD 算法は摂動を $O(0.01)$ に設定した場合に不安定になったが、安定化 PC-PRS 算法は精度よく計算できた。これは両算法の計算回数の違いによるものであり、安定化 PC-PRS 算法の方が安定していることがわかる。また、Ex.5, 6, 7, 8 は [San05] の Table 9 の Ex.9, 4, 10, 5 にそれぞれ対応する。[San05] との比較により、ダミーを用いての計算が安定していることがわかる。

参 考 文 献

[CGTW95] R. Corless, P. Gianni, B. Trager and S. Watt, *The singular value decomposition for polynomial systems*, Proc. of ISSAC'95, ACM, 1995, 195–207.

[CWZ04] R. Corless, S. Watt and L. Zhi, *QR factoring to compute the GCD of univariate approximate polynomials*, IEEE Trans. Signal Proces., **52(12)** (2004), 3394–3402.

[EGL97] I. Emiris, A. Galligo and H. Lombardi, *Certified approximate univariate GCDs*, J. Pure and Applied Alge., **117&118** (1997), 229–251.

[GKMYZ04] 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, 2004, 167–174.

[KS97] F. Kako and T. Sasaki, *Proposal of "effective floating-point number" for approximate algebraic computation*, Preprint of Tsukuba Univ., 1997.

[KYZ06] E. Kaltofen, Z. Yang and L. Zhi, *Approximate greatest common divisors of several polynomials with linearly constrained coefficients and singular polynomials*, Proc. of ISSAC'06, ACM, 2006, 169–176.

[ONS91] 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.

[OST97] H. Ohsako, H. Sugiura and T. Torii, *A stable extened algorithm for generating polynomial remainder sequence (in Japanese)*. Trans. of JSIAM (Japan Society for Indus. Appl. Math.) **7** (1997), 227–255.

[Pan01] V.Pan, *Univariate polynomials: nearly optimal algorithms for factorization and rootfinding*, Proc. of ISSAC'01, ACM, 2001, 253–267.

[San05] M. Sanuki, *Computing approximate GCD of multivariate polynomilals (Extended abstract)*, International Workshop on Symbolic-Numeric Computation 2005 (SNC 2005), D. Wang & L. Zhi (Eds.), 2005, 308–314; full paper will appear in Symbolic-Numeric Computation (Trends in Mathematics), D. Wang & L. Zhi (Eds.), Birkhäuser Verlag, 2007, 55–68.

[Sch85] A. Schönhage, *Quasi-GCD*, J. Complexity, **1**, 1985, 118–147.

[SK05] T. Sasaki and F. Kako, *An algebraic method for separating close-root clusters and the minimum root separation*, International Workshop on Symbolic-Numeric Computation 2005 (SNC 2005), D. Wang & L. Zhi (Eds.),

[SN89] T. Sasaki and M-T. Noda, *Approximate square-free decomposition and root-finding of ill-conditioned algebraic equations*, J. Inform. Proces., **12** (1989), 159–168.

[SS92] T. Sasaki and M. Suzuki, *Three new algrithms for multivariate polynomial GCD*, J. Symbolic Comput., **13**(1992), 395–411.

[SS97] T. Sasaki and M. Sasaki, *Polynomial remainder sequence and approximate GCD*, SIGSAM Buletin **31**, 1997, 4–10.

[SY98] T. Sasaki and S. Yamaguchi, *An analysis of cancellation error in multivariate Hensel construction with floating-point number arithmetic*, Proc. of ISSAC'98, ACM, 1998, 1–8.

[ZD04] Z. Zeng and B. H. Dayton, *The approximate GCD of inexact polynomials part II: A multivariate algorithm*, Proc. of ISSAC'04, ACM, 2004, 320–327.

[Zen04] Z. Zeng, *The approximate GCD of inexact polynomials part I: a univariate algorithm*, Preprint, 2004.

[Zhi03] L. Zhi, *Displacement structure in computing the approximate GCD of univariate polynomials*, Proc. of ASCM2003, World Scientific, 2003, 288–298.

[ZMF00] C. J. Zarowski, X. Ma and F. W. Fairman, *QR-factorization method for computing the greatest common divisor of polynomials with inexact coefficients*, IEEE Trans. Signal Proces., **48(11)** (2000), 3042–3051.

[ZN00] L. Zhi and M-T. Noda, *Approximate GCD of multivariate polynomials*, Proc. of ASCM2000, World Scientific, 2000, 9–18.