数理解析研究所講究録
第2054巻 2017年 31-39

巨大次数の整数係数1変数多項式のGCD次数判定

讃岐 勝
MASARU SANUKI
筑波大学医学医療系臨床医学域 & 筑波大学附属病院総合臨床教育センター
DIVISION OF CLINICAL MEDICINE, FACULTY OF MEDICINE, UNIVERSITY OF TSUKUBA
&
CENTER FOR MEDICAL EDUCATION AND TRAINING, UNIVERSITY OF TSUKUBA HOSPITAL *

Abstract

本稿では，大きな次数の多項式が持つGCDの次数を見積もる方法について数値計算的手法を用いた方法について述べる．整数係数のGCD計算においても近似GCDの次数だけを如何に早く見積もるかを検討している．著者自身が提案した算法は構造行列同士の積だけであり非常に早いが，不明な点が多い．本稿では，不明点を明らかにすることで高速化を行う．

1 はじめに

整数係数の1変数多項式のGCD計算において，Euclidの互除法の高速算法であるhalf-GCD法は非常に高速である[15, 1, 24]．2015年12月現在，20,000+4次の多項式（係数は$[-100, 100]$の整数）のGCDは数秒で計算できる．次はCPU Intel core-i7 4600(2.1GHz), 16GB RAMのPC上でMaple 2015を用いて計算した結果である．4秒程度で計算が完了している（もちろん，結果は正しい）．

```
ff:=randpoly(x,dense,degree=20000):   gg:=randpoly(x,dense,degree=20000):
cc:=randpoly(x,degree=4);
                    4       3       2
                90 x  - 39 x  - 63 x  - 91 x + 43
f:=expand(ff*cc):
g:=expand(gg*cc):
t:=time():      gcd(f,g);       time() - t;
                              4.515
```

ソースコードを見ると[1)]，利用されている算法はmodular法やhalf-GCD方など基本的な算法のみが利用されている．このような現状において，整数係数の多項式の次数のみを求めることにそれほど意義はないように思う．しかし，多変数多項式のGCD計算でしばしば利用される補間法やEZ-GCD法など各次数に関する情報のみが必要な場合も多々あるため，高速化が期待できるのであれば，追求すべきである．

浮動小数係数の多項式のGCD（近似GCD）において，half-GCD法の適応は非常に難しい[18]．一方で，近似GCD算法の多くは近似GCDの次数を入力として計算を実行される．しかし，近似GCDの次数を計

*sanuki@md.tsukuba.ac.jp

[1)]利用したコマンドは次の2行：`interface(verboseproc=2): print(gcd);`

算するためにはrankを計算する以外に方法はあまり知られていない．そのため，近似GCDの次数を高速で見積もることが出来れば近似GCD計算そのものの速度を早くすることができる．

しかし，rank計算はサイズが大きい時，および摂動項が大きい時に効率良く計算することは難しい．そのため，高速で計算または高速で次数の近似値を見積もる方法が必要である．rank計算の基本方針は行列の三角化であり，高速化を考えると行列およびその要素の積・和の計算をできる限り減らす以外になく，これまでにない抜本的なアイデアが必要となる．このような条件をクリアすべく[19]にて，行列の基本演算のみで次数を見積もる提案した（3章で述べる）．行列のある1列に注目して見積もる方法であった．本稿では，ある要素に注目して見積もることができないか検討を行なっている．

2章では，本稿で用いる行列およびその性質について述べる．3章では，次数を見積もるための方法およびその方法の改良について述べる．

本稿では次の記号を用いる．$\mathbb{K}$ を標数0の数体，$\mathbb{Z}$ を整数全体の集合，$\mathbb{F}$ を浮動小数全体の集合を表す（$\mathbb{Z}$ でも $\mathbb{F}$ でも成り立つ場合には，$\mathbb{K}$ を用いる）．多項式 $f \in \mathbb{K}[x]$ に対して，$\deg(f)$ は f の次数，$||f||$ は f の多項式ノルム（係数の絶対値の最大値）を表す．与えられる多項式 f と g は $n = \deg(f) > \deg(g)$ と仮定する（$\deg(f) = \deg(g)$ のときは，g を f で頭項消去を行いその結果を g と置き直す）．

$$f(x) = f_n x^n + f_{n-1}x^{n-1} + \cdots + f_0, \quad g(x) = g_{n-1}x^{n-1} + g_{n-2}x^{n-2} + \cdots + g_0.$$

$\gcd(f,g)$ を f と g のGCDを表し，次で表す．

$$\gcd(f,g) = c(x) = c_k x^k + c_{k-1}x^{k-1} + \ldots + c_0.$$

本稿では，特に $\mathbb{Z}[x]$ に属する多項式は全て小文字 $f, g, \ldots$ で表し，$\mathbb{F}[x]$ に属する多項式は全て大文字 $F, G, \ldots$ で表すことにする．

2 準備

Bezout行列とBezout-Hankel行列を定義する．

定義 1 (Bezout行列)
$f(x)$ と $g(x)$ から構成されるBezout行列 $\mathrm{Bmat}(f,g)$ は次で定義される．

$$\mathrm{Bmat}(f,g) = \begin{pmatrix} b_{0,0} & \cdots & b_{0,n-1} \\ \vdots & \ddots & \vdots \\ b_{n-1,0} & \cdots & b_{n-1,n-1} \end{pmatrix} \in \mathbb{K}^{n\times n}. \tag{1}$$

ここで，(i,j)-要素 $b_{i-1,j-1}$ は多項式 $\dfrac{f(x)g(y) - f(y)g(x)}{x-y} = \displaystyle\sum_{0\le i,j\le n-1} b_{i,j}x^i y^j \in \mathbb{K}[x,y]$ の $x^{i-1}y^{j-1}$-係数である． ∎

特に，$\mathrm{Bmat}(f,1)$ は $f(x)$ の係数から構成される次の行列である．

$$\mathrm{Bmat}(f,1) = \begin{pmatrix} f_1 & f_2 & \cdots & f_n \\ f_2 & \iddots & \iddots & \\ \vdots & \iddots & & \\ f_n & & & \end{pmatrix} \in \mathbb{K}^{n\times n}. \tag{2}$$

定義 2 (Bezout-Hankel 行列)
$f(x)$ と $g(x)$ から構成される Bezout-Hankel 行列 $\mathrm{Hmat}(f,g)$ は次で定義される.

$$\mathrm{Hmat}(f,g) = \begin{pmatrix} h_1 & h_2 & \cdots & h_n \\ h_2 & \iddots & \iddots & h_{n+1} \\ \vdots & \iddots & \iddots & \vdots \\ h_n & h_{n+1} & \cdots & h_{2n-1} \end{pmatrix} \in \mathbb{K}^{n\times n}, \tag{3}$$

ここで，各要素 h_i は $\frac{g}{f}$ を無限遠点上（$x=\infty$）で Taylor 展開したときの x^{-i} 次の係数である：

$$\frac{g(x)}{f(x)} = h_1x^{-1} + h_2x^{-2} + h_3x^{-3} + \cdots \in \mathbb{K}\{x\}.$$

∎

$\mathrm{Bmat}(f,g)$ は対称行列，$\mathrm{Bmat}(f,1)$ と $\mathrm{Hmat}(f,g)$ は Hankel 行列である：行列 $M=(m_{i,j})$ が $m_{i,j} = m_{i+1,j-1}$ をみたすとき，行列 M は Henkel 行列であるという.

$\mathrm{Bmat}(f,g)$ と $\mathrm{Hmat}(f,g)$ の間に，次の関係式が成立する [13].

$$\mathrm{Bmat}(f,g) = \mathrm{Bmat}(f,1)\mathrm{Hmat}(f,g)\mathrm{Bmat}(f,1). \tag{4}$$

2.1 多項式の悪条件化

多項式の共通因子の主係数を小さくする変換を考える．次の変換によってできる.

注意 1 (微小主係数をもつ共通因子への変換)
$P(x) \in \{F(x), G(x)\}$ に対して次の方法によって微小主係数な近似 *GCD* をもつ多項式の組に変換可能なことが多い（数回繰り返すことによって，必ず実現される）.

1. $P(x) \mapsto x^{\deg(p)}P(1/x)$
2. $P(x) \mapsto aP(x) + bxP(x) = (a+bx)P(x)$ *with* $a \ll b$. *このとき，Bezout 行列および Bezout-Hankel 行列のサイズは 1 だけ増える.*

3 見積もりの方法

次数の見積もりは次の方法で行う．与えられた多項式 f,g にそれぞれ適当な摂動 Δ_f, Δ_g を加え，係数を浮動小数に変換する[2].

$$F \leftarrow f + \Delta_f, \quad G \leftarrow g + \Delta_g.$$

このとき，F と G の近似 GCD は $\gcd(f,g)$ である．ゆえに，$\gcd(\gcd(f,g)) = k$ は F と G の近似 GCD の次数を見積もればよい．k を見積もるため，式 (4) を利用する．加えて，注意 1 の方法により共通因子の主係数を微小にする．微小主係数の近似 GCD を持つ時，次の性質を満たす.

[2] 次数 20000 次の多項式の係数を浮動小数に変換するのに 0.032 秒かかる．高速化のため複雑なことはできない.

補題 3 (Bezout 行列の生成 [17])
微小主係数な近似共通因子を持つ $F(x)$ と $G(x)$ が与えられた時，*Bezout* 行列 $\mathrm{Bmat}(F,G)$ の構成において，微小主係数に依存した桁落ち誤差は発生しない．∎

補題 4 (Bezout-Hankel 行列の生成)
微小主係数な近似共通因子を持つ $f(x)$ と $g(x)$ が与えられた時，*Bezout-Hankel* 行列 $\mathrm{Hmat}(f,g)$ の構成において，桁落ち誤差は発生しない．∎

命題 5
F と G が近似 *GCD* を持つ時，$\gamma = |c_k| \ll 1$ とする．このとき，*Bezout-Hankel* 行列は γ によって次のように評価できる．

$$\mathrm{Hmat}(F,G) \propto \left(\begin{array}{ccc|ccc|c} O(1) & \cdots & O(1) & O(1/\gamma) & \cdots & \cdots & O(1/\gamma^{n-k-1}) \\ \vdots & \iddots & \iddots & \iddots & \iddots & \iddots & \vdots \\ O(1) & \iddots & O(1/\gamma^{k-1}) & \iddots & \iddots & \iddots & \vdots \\ \hline O(1/\gamma) & \iddots & \iddots & \iddots & \iddots & \iddots & O(1/\gamma^{n}) \\ \vdots & \iddots & \iddots & \iddots & \iddots & \iddots & \vdots \\ \vdots & \iddots & \iddots & \iddots & \iddots & \iddots & \vdots \\ O(1/\gamma^{n-k-1}) & \cdots & \cdots & O(1/\gamma^{n}) & O(1/\gamma^{n}) & \cdots & O(1/\gamma^{n}) \end{array}\right). \tag{5}$$

ここで，上記行列は前方 k 次の行列で区切られている．∎

命題 6
$\gamma = |c_k| \ll 1$ のとき，*Bezout* 行列 $\mathrm{Bmat}(f,g)$ の各要素は次のように評価できる。

$$\mathrm{Bmat}(f,g) \propto \left(\begin{array}{ccc||c} O(1) & \cdots & O(1) & O(\gamma) \\ \vdots & \ddots & \vdots & \vdots \\ O(1) & \cdots & O(1) & O(\gamma) \\ \hline\hline O(\gamma) & \cdots & O(\gamma) & O(\gamma^2) \end{array}\right). \tag{6}$$

それゆえ，$\mathrm{Bmat}(f,1)\mathrm{Hmat}(f,g)\mathrm{Bmat}(f,1)$ の桁落ち量は次のように見積もることができる．

命題 7
$\mathrm{Bmat}(F,1)\mathrm{Hmat}(F,G)\mathrm{Bmat}(F,1)$ の計算において，桁落ち誤差が発生する．

Amount of Cancellation error of $\mathrm{Bmat}(f,1)\mathrm{Hmat}(f,g)\mathrm{Bmat}(f,1)$

$$\propto \left(\begin{array}{ccc|cc} O(1/\gamma^{k-1}) & \cdots & O(1/\gamma^{0}) & 0 & \cdots \\ \vdots & \iddots & \iddots & \vdots & \cdots \\ O(1/\gamma^{0}) & \iddots & \iddots & 0 & \cdots \\ \hline 0 & \cdots & 0 & 0 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{array}\right).$$

例 1 (近似 GCD の次数見積もり)
F と G は次で与えられる.

$$\begin{aligned} F(x) &= (0.01x^3+x^2-x+1)(x^4+3x^2-3x+4)+0.001x^5-0.00001x^3-0.0004, \\ g(x) &= (0.01x^3+x^2-x+1)(x^3-3x^2-3x+4)+0.001x^4+0.00001x^2. \end{aligned}$$

次の行列は $\mathrm{Bmat}(F,G)$ と $\mathrm{Bmat}(F,1)\mathrm{Hmat}(F,G)\mathrm{Bmat}(F,1)$ をそれぞれ計算後に差を計算した結果である.

$\mathrm{Bmat}(F,G)-\mathrm{Bmat}(F,1)\mathrm{Hmat}(F,G)\mathrm{Bmat}(F,1)$

$$= \left(\begin{array}{ccc|cccc} 678 & 78 & 0.69 & 9\times10^{-4} & -6\times10^{-5} & -5\times10^{-7} & -5\times10^{-15} \\ 78 & 0.69 & 9\times10^{-4} & -5\times10^{-7} & -5\times10^{-7} & 4\times10^{-15} & 0.0 \\ 0.69 & 9\times10^{-4} & -6\times10^{5} & -5\times10^{-7} & -1\times10^{-14} & 4\times10^{-16} & 7\times10^{-18} \\ \hline 9\times10^{-4} & -6\times10^{5} & -5\times10^{-7} & 7\times10^{-15} & -2\times10^{-15} & 0.0 & 0.0 \\ -6\times10^{5} & -5\times10^{-7} & -7\times10^{-15} & 0.0 & -2\times10^{-16} & 0.0 & 0.0 \\ -5\times10^{-7} & -9\times10^{-16} & -9\times10^{-16} & 2\times10^{-16} & 0.0 & 0.0 & 0.0 \\ -8\times10^{-15} & 0.0 & 7\times10^{-18} & 0.0 & 7\times10^{-18} & 0.0 & 0.0 \end{array}\right).$$

(1,1), (1,2) ,(1,3), (2,1), (2,2), (3,1) 要素にて，大きな桁落ちが起きた．上部分 3×3 行列の上三角行列部のみ桁落ちがおきた．部分行列のサイズは近似 *GCD* の次数 $k=3$ に一致している.

例 2 (整数係数の次数)
次の多項式 f,g の次数を求める.

$$\begin{aligned} f(x) &= (\frac{1}{100}x^3+x^2-x+1)(x^4+3x^2-3x+4), \\ g(x) &= (\frac{1}{100}x^3+x^2-x+1)(x^3-3x^2-3x+4). \end{aligned}$$

まず，f,g に任意の摂動をつけ，近似 *GCD* の次数を求める.

$$F(x)=f(x)+\epsilon\times\texttt{randpoly},\ \texttt{G(x)}=\texttt{g(x)}+\epsilon\times\texttt{randpoly}.$$

次の表は，摂動の大きさ ϵ に対して，*100* 回の試行で互いに素ではないと返した回数を表す.

	$\epsilon=0.01$	$\epsilon=0.001$	$\epsilon=0.0001$
10 桁	100	96*	92

表 1: 共通因子を持つかの判定（それぞれ 100 回試行）

また，$\epsilon=0.001$ の場合（共通因子があると判定：96 回）に得られた次数は次の通りである.

- 次数 $=2$： *8* 回
- 次数 $=3$： *81* 回
- 次数 $=4$： *7* 回

実際，摂動のとり方は次に注意する必要がある.

- 摂動多項式のノルムは $f(x),g(x)$ のノルムの $\frac{1}{1000}$ 程度まで小さくすること．小さすぎると，算法が摂動項のある多項式と認識しないため，桁落ち誤差が発生しないことがある.

- 摂動多項式の主係数は $f(x), g(x)$ の主係数より十分に小さくすること．ここで述べる算法は主係数の大きさに非常に敏感である．

これに注意すると，多くの場合には正しい次数を得ることができる．

3.1 計算量：改良前

計算量は次の通りである．

- 多項式の積（Bezout 行列作成）：$M_{\mathrm{poly}}(n)$
- 有理式のローラン展開（Hankel 行列）⇒ 多項式の積：$O(\mathrm{const.} \times n)$
- Hankel 行列 × ベクトルの計算量は $O(n \log n)$ であり，$\mathrm{Bmat}(f,1)\mathrm{Hmat}(f,g)\mathrm{Bmat}(f,1)$ の 1 列目のみ計算できればよいので、

$$2O(n \log n).$$

- $S_{\mathrm{mat}}(n)$ ： n 回の差の計算で十分（1 列目）

故に，n が十分に大きい時，計算量は $O(n^2)$ より小さく，演算はすべて浮動小数演算のため，全体としても早い．

4 どの計算で桁落ち誤差が発生するのか？

行列の積和でを見る．理解を深めるため次で多項式で話をすすめる．

- $\deg(f) = 4 > 3 = \deg(g)$
- $k = \deg(\gcd(f,g))$ は動かす

このとき，次の行列の積について考える．

$$\begin{pmatrix} f_4 & f_3 & f_2 & f_1 \\ f_3 & f_2 & f_1 & \\ f_2 & f_1 & & \\ f_1 & & & \end{pmatrix} \begin{pmatrix} h_1 & h_2 & h_3 & h_4 \\ h_2 & h_3 & h_4 & h_5 \\ h_3 & h_4 & h_5 & h_6 \\ h_4 & h_5 & h_6 & h_7 \end{pmatrix} \begin{pmatrix} f_4 & f_3 & f_2 & f_1 \\ f_3 & f_2 & f_1 & \\ f_2 & f_1 & & \\ f_1 & & & \end{pmatrix}.$$

この結果について，要素ごとに考える．

4.0.1 (1,1)-要素

(1,1)-要素は次で表される．

$$\begin{aligned} & (f_4h_1 + f_3h_2 + f_2h_3 + f_1h_4)f_4 + (f_4h_2 + f_3h_3 + f_2h_4 + f_1h_5)f_3 \\ & +(f_4h_3 + f_3h_4 + f_2h_5 + f_1h_6)f_2 + (f_4h_4 + f_3h_4 + f_2h_6 + f_1h_7)f_1 \qquad (7) \\ = \ & s_{11}f_4 + s_{12}f_3 + s_{13}f_2 + s_{14}f_1 \qquad (8) \\ = \ & b_{0,0} \qquad (9) \end{aligned}$$

結果は計算の順番に依存しないことを確認している．本稿では，始め 2 つの行列の積を計算した後に（(7) の括弧の中：s_{1i} for $1 \le i \le 4$），3 つ目の行列との積を計算している．

補題 8

$s_{11}, s_{12}, s_{13}, s_{14}$ にて桁落ち誤差は発生しないが，$s_{11}f_4 + s_{12}f_3 + s_{13}f_2 + s_{14}f_1$ にて桁落ち誤差が発生する．

証明 h_i について眺めると，

$$h_i = c_k \times (terms) + c_{k-1} \times (terms) + \ldots + c_1 \times (terms) + c_0 \times (terms) + \epsilon$$

ここで，$s_{11}, s_{12}, s_{13}, s_{14}$ の計算にて c_0 の項が消える．すなわち，$s_{11}f_4 + s_{12}f_3 + s_{13}f_2 + s_{14}f_1$ にて，*dominant terms*（$c_{k-1}, \ldots, c_0$ の項）が全て消去するため，桁落ち誤差が発生する． ∎

4.0.2 (i,j)-要素

一般の (i,j)-要素について見る．

$$\begin{pmatrix} f_4 & f_3 & f_2 & f_1 \\ f_3 & f_2 & f_1 & \\ f_2 & f_1 & & \\ f_1 & & & \end{pmatrix} \begin{pmatrix} h_1 & h_2 & h_3 & h_4 \\ h_2 & h_3 & h_4 & h_5 \\ h_3 & h_4 & h_5 & h_6 \\ h_4 & h_5 & h_6 & h_7 \end{pmatrix} \begin{pmatrix} f_4 & f_3 & f_2 & f_1 \\ f_3 & f_2 & f_1 & \\ f_2 & f_1 & & \\ f_1 & & & \end{pmatrix}$$

始め 2 つの行列の積によって得られる 1 列目の要素は次の形である．

- $s_i = f_4h_i + f_3h_{i+1} + f_2h_{i+2} + f_1h_{i+3}$

このとき，(第 1・第 2) 第 3 行列の積は次のように分類でき，それぞれ桁落ち誤差の有無および桁落ち誤差の大きさを見積もることができる．

1. $w_i = s_if_4 + s_{i+1}f_3 + s_{i+2}f_2 + s_{i+3}f_1$ について： $O(1/\gamma^{k-i})$ の誤差発生
2. $w_{i,3} = s_if_3 + s_{i+1}f_2 + s_{i+2}f_1$ について：$O(1/\gamma^{k-(3-i)})$ の誤差発生

Bezout 行列は対称行列（$b_{i,j} = -b_{i,j}$）なので，次が言える

- $t_i = f_3h_i + f_2h_{i+1} + f_1h_{i+2}$
- $t_2f_3 + t_3f_2 + t_4f_1$ について $O(1/\gamma^{k-i})$ の誤差発生

Bezout-Henkel 行列のから Bezout 行列を構成する際，c_k の項および，$c_{k-1}, \ldots, c_1$ のある項が消去される．そのため，大きな桁落ち誤差が発生する．h_i の分母には c_k のべき乗の項が必ずあるため i と k を用いた評価が可能になる．

4.1 算法の効率化

これまでの算法は 1 列目だけを評価する方法であるが，微小主係数の大きさはわかるので，(1,1)-要素だけ見れば次数を見積もることができる．これによって，計算は更に効率化することができる[3)]．

[3)] 正確な次数を求めることを目的としていないことに注意

4.2 計算量：改良後

計算量は次の通りである.

- 多項式の積（Bezout 行列作成）：$M_{\mathrm{poly}}(n)$
- 有理式のローラン展開（Hankel 行列）⇒ 多項式の積：$O(\mathrm{const.} \times n)$
- Hankel 行列 × ベクトルの計算量は $O(n \log n)$ であり，$\mathrm{Bmat}(f,1)\mathrm{Hmat}(f,g)\mathrm{Bmat}(f,1)$ の (1,1)-要素のみ計算できればよいので、

$$2O(n \log n).$$

最後の差の計算がなくなり，Hankel 行列 × ベクトルの計算の回数が減った.

参 考 文 献

[1] A. V. Aho, J. E. Hopcroft and J. D. Ullman. *The design and analysis of computer algorithms.* Addison-Wesley, 1974.

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

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

[4] D. Bini and P. Boito, *Structured matrix-based methods for polynomial ϵ-gcd: analysis and comparisons*, Proc. of ISSAC'07, ACM Press, 2007, 9–16.

[5] B. Beckermann and G. Labahn, *When are two numerical polynomials relatively prime?*, J. Symb. Comput., **26** (1998), 677–689.

[6] B. Beckermann and G. Labahn, *A fast and numerically stable Euclidean-like algorithm for detecting relatively prime numerical polynomials*, J. Symb. Comput., **26** (1998), 691–714.

[7] D. Bini and V.Pan, *Polynomial and Matrix Computations*, Birkhäuser, 1994.

[8] 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.

[9] 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.

[10] E.-W. Chionh, M. Zhang and R. N. Goldman. *Fast computation of the Bezout and Dixon resultant matrices.* J. Symb. Compu., **33**(2002), 13–20.

[11] 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.

[12] G. H. Golub and C. F. Van Loan, *Matrix computations*, Johns Hopkins Univ. Press, Baltimore, Maryland, 1989.

[13] U. Helmke and P. A Fuhrmann. *Bezoutians.* Linear Algebra Appl., **122/123/124**, 1989, 1039–1097.

[14] D.E. Knuth. *The Art of Computer Programming, Volume 2 (3rd Ed.): Seminumerical Algorithms*, Addison-Wesley Longman Publishing Co., Inc. 1997.

[15] R. T. Moenck. *Fast computation of GCDs. Proc. 5th ACM Symp. Thory of Comput.*, 1973, 142–151.

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

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

[18] M. Sanuki. *Challenge to fast and stable computation of approximate univariate GCD, based on displacement structures*, Proc. of SNC2011, ACM Press, 2011, 178–186.

[19] 讃岐 勝. 悪条件性に注目した近似 GCD の見積もり、京都大学数理解析研究所講究録、2015 (to appear)

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

[21] 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 (SN C 2005), D. Wang & L. Zhi (Eds.), 2005, 126–143.

[22] 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.

[23] M. Sanuki and T. Sasaki, *Computing approximate GCDs in ill-conditioned cases*, Proc. of SNC 2007, 2007, 170–179.

[24] K. Thull and C. K. Yap. A unified approach to HGCD algorithms for polynomials and integers. Manuscript, Available from `http://cs.nyu.edu/cs/faculty/yap/papers/`.

[25] J. R. Winkler and X. Lao, *The calculation of the degree of an approximate greatest common divisor of two polynomials*, J. of Comp. and Appl. Math., **235(6)**, 2011, 1587–1603.

[26] T. Y. Li and Z. Zeng, *A rank-revealing method with updating, downdating, and applications*, SIAM J. Matrix Anal. Appl., **26** (2005), no. 4, 918–946.

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

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

[29] 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.