Bezoutの終結式行列を用いたGPGCD法による1変数多項式の近似GCDの計算
Algorithm for Calculating Approximate GCD of Univariate Polynomials with the Bezout Resultant Matrix

池 泊明
Chi Boming
筑波大学数理物質科学研究科
Graduate School of Pure and Applied Sciences University of Tsukuba *

照井 章
Akira Terui
筑波大学数理物質系
Faculty of Pure and Applied Sciences University of Tsukuba †

Abstract

我々は，これまでに1変数多項式に対する近似GCD計算の反復算法であるGPGCD法を提案している．GPGCD法は，与えられた多項式および次数と，近似GCDの次数に対し，可能な限り摂動を小さくし，その時の摂動および近似GCDを求める算法である．本算法では，Sylvesterの終結式行列を用い，与えられた近似GCD計算問題を制約付き最適化問題に帰着させ，最適化問題を修正Newton法で解いている．本稿では，元のGPGCD法に用いたSylvesterの終結式行列に代えて，Bezoutの終結式行列を用いたGPGCD算法を提案する．

Abstract

We have presented the GPGCD algorithm, which is an iterative algorithm for calculating approximate greatest common divisor (GCD) of univariate polynomials with real or complex coefficients. For a given pair of polynomials and a degree of the approximate GCD, our algorithm finds a pair of polynomials which has the GCD of the given degree, and makes the perturbations of whose coefficients from those in given polynomials as small as possible. We transfer the approximate GCD problem to a constrained minimization problem with the Sylvester matrix, then solve it with so-called the modified Newton method. In this paper, in place of the Sylvester matrix, we present an algorithm which uses the Bezout matrix to transfer the problem.

*hakumei-t@math.tsukuba.ac.jp
†terui@math.tsukuba.ac.jp

1　はじめに

最大公約子 (GCD) 計算は数式処理において最も基本的かつ重要な計算の一つであり，近似 GCD 計算は数式・数値融合計算 [16] の中でも古くから研究されているテーマの一つである．近似 GCD 計算には，多項式剰余列 (PRS) ([11], [10]),（部分）終結式行列の特異値分解 (SVD) [4]，QR 分解 [5]，LU 分解 [1]，最適化など ([14], [3], [12], [17])，さまざまなアプローチがある．

本稿では，最適化法に基づく近似 GCD 計算アルゴリズムの一つである Sylvester の終結式行列を用いた GPGCD 計算アルゴリズム (以下は Sylvester 法という)[14] をもとに，Bezout の終結式行列を用いた GPGCD 計算アルゴリズム (以下は Bezout 法という) を提案する．

2　近似 GCD 計算の制約付き最適化問題への帰着

本稿では，近似 GCD 計算を以下の問題を解く形で考える．

問題 1
実係数の m 次多項式 $f(x)$, n 次多項式 $g(x)$ と正整数 k に対し，

$$\begin{gathered}\tilde{f}(x) = f(x) + \Delta f(x) = h(x)\bar{f}(x), \quad \tilde{g}(x) = g(x) + \Delta g(x) = h(x)\bar{g}(x), \\ \deg(h(x)) = k, \quad \gcd(\bar{f}(x), \bar{g}(x)) = 1, \\ \deg(\Delta f(x)) \leq \deg(f(x)), \quad \deg(\Delta g(x)) \leq \deg(g(x)),\end{gathered} \tag{1}$$

を満たし，$\|\Delta f(x)\|^2 + \|\Delta g(x)\|^2$ を最小化する $\tilde{f}(x)$, $\tilde{g}(x)$, $h(x)$ を求めよ． □

本稿では，多項式のノルム $\|\cdot\|$ を 2 ノルム $\|\cdot\|_2$ とする．
与えられた多項式 $f(x), g(x)$ を

$$f(x) = f_m x^m + \cdots + f_0 x^0, \quad g(x) = g_n x^n + \cdots + g_0 x^0 \tag{2}$$

とし，求める近似多項式 $\tilde{f}(x)$, $\tilde{g}(x)$ を

$$\tilde{f}(x) = \tilde{f}_m x^m + \cdots + \tilde{f}_0 x^0, \quad \tilde{g}(x) = \tilde{g}_n x^n + \cdots + \tilde{g}_0 x^0 \tag{3}$$

とおく．一般性を失うことなく，$m \geq n$ と仮定する．以下では，$g(x)$ を m 次多項式 $g_m x^m + \cdots + g_0 x^0$, $g_m = \cdots = g_{n+1} = 0$ として扱う．
Bezout の終結式行列の定義と性質を以下に述べる．

定義 1 (Bezout の終結式行列 [2])
m 次多項式

$$f(x) = f_m x^m + \cdots + f_0 x^0, \quad g(x) = g_m x^m + \cdots + g_0 x^0$$

に対し，

$$\begin{gathered}\mathrm{Bez}(f, g) = (b_{ij})_{i,j=1,\ldots,m}, \\ b_{ij} = \sum_{k=1}^{m_{ij}} f_{j+k-1} g_{i-k} - f_{i-k} g_{j+k-1}, m_{ij} = \min\{i, m+1-j\},\end{gathered}$$

を満たす行列 $\mathrm{Bez}(f, g)$ を f と g の ***Bezout*** の終結式行列と呼ぶ． □

補題 2 (Bezout の終結式行列の性質 [2])
m 次多項式 f, g に対し，$\mathrm{Bez}(f,g)$ は m 次正方行列かつ対称行列であり，以下の関係を満たす．ここに，行列 A の階数を $\mathrm{rank}(A)$ で表す．

$$m - \mathrm{rank}(\mathrm{Bez}(f,g)) = \deg(\gcd(f,g)). \tag{4}$$

□

以下では，$\tilde{B} = \mathrm{Bez}(\tilde{f}, \tilde{g})$ とおく．
問題 1 の条件式 (1) より

$$\deg(\tilde{f}, \tilde{g}) = \deg(h(x)) = k \tag{5}$$

とおく．このとき，式 (5) と補題 2 より，

$$\mathrm{rank}(\tilde{B}) = m - k, \tag{6}$$

が成り立つ．
$\tilde{B} = (\tilde{b}_{ij})$ の特異値分解 [7] を $\tilde{B} = \tilde{U}\tilde{\Sigma}\tilde{V}^T$ とし，特異ベクトルである行列 $\tilde{V} = (\tilde{\boldsymbol{v}}_1, \cdots, \tilde{\boldsymbol{v}}_m)$ の後ろ k 個の列ベクトルで構成される行列を $\tilde{V}' = (\tilde{\boldsymbol{v}}_{m-k+1}, \cdots, \tilde{\boldsymbol{v}}_m)$ とおく．補題 2 と特異値分解の性質より，

$$\tilde{B}\tilde{V}' = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix} \tag{7}$$

が得られる．よって，制約条件を

$$G_{ij} = \tilde{b}_{i1}\tilde{v}_{1j} + \cdots + \tilde{b}_{im}\tilde{v}_{mj} = 0, \quad i \le m, \quad m - d + 1 \le j \le m \tag{8}$$

とおく．
与えられた多項式 $f(x)$, $g(x)$ の Bezout 行列を $B = \mathrm{Bez}(f(x), g(x))$ とする．$B = (b_{ij})$ の特異値分解を $B = U\Sigma V^T$ とし，$V = (\boldsymbol{v}_1, \cdots, \boldsymbol{v}_m)$ の後ろ k 個の列ベクトルで構成される行列を $\bar{V} = (\boldsymbol{v}_{m-k+1}, \cdots, \boldsymbol{v}_m)$ とする．$\tilde{B}$ と B の間の変動を最小化するため，ここでは，$\tilde{B}$ の B からの摂動，および $\tilde{V}'$ の $\bar{V}$ からの摂動を最小化する．補題 1 より Bezout 行列は対称行列であるので，$\tilde{B}$ の要素として上三角の要素のみをとればよい．よって，目的関数を

$$F = \sum_{i \le j} (\tilde{b}_{ij} - b_{ij})^2 + \sum_{\substack{i \le m \\ m-d+1 \le j \le m}} (\tilde{v}_{ij} - v_{ij})^2 \tag{9}$$

とおく．
以上により，

$$\begin{aligned} \boldsymbol{x} &= (x_1, x_2, \ldots, x_{m(m+1)/2+md}) \\ &= (\tilde{b}_{11}, \ldots, \tilde{b}_{1m}, \tilde{b}_{22}, \ldots, \tilde{b}_{2m}, \ldots, \tilde{b}_{mm}, \tilde{v}_{1,m-d+1}, \ldots, \tilde{v}_{m,m-d+1}, \tilde{v}_{1,m-d+2}, \ldots, \tilde{v}_{m,m-d+2}, \ldots, \tilde{v}_{mm}) \end{aligned}$$

に対し，制約条件を $\boldsymbol{G}(\boldsymbol{x}) = (G_{1,m-d+1}(\boldsymbol{x}), \ldots, G_{mm}(\boldsymbol{x})) = \boldsymbol{0}$，目的関数を $F(\boldsymbol{x})$ とおき，制約付き最適化問題を以下の通り定める．

問題 2 (制約付き最適化問題)
制約条件 $\boldsymbol{G}(\boldsymbol{x}) = \boldsymbol{0}$ のもとで，目的関数 $F(\boldsymbol{x})$ を最小化する $\boldsymbol{x}$ を求めよ． □

3　近似 GCD と近似多項式の計算

本稿では，問題 2 を修正 Newton 法 [13] によって解く．

修正 Newton 法に与える $md \times (m(m+1)/2 + md)$ のヤコビ行列 $J_{\boldsymbol{G}}(\boldsymbol{x})$ の構成を以下に示す．

$$J_{\boldsymbol{G}}(\boldsymbol{x}) = \begin{pmatrix} J_{\tilde{B}} & \tilde{B} & & \\ \vdots & & \ddots & \\ J_{\tilde{B}} & & & \tilde{B} \end{pmatrix},$$

ここに，$m \times (m(m+1)/2)$ の行列 $J_{\tilde{B}}$ は

$$J_{\tilde{B}} = \begin{pmatrix} \tilde{v}_1 & \tilde{v}_2 & \cdots & \cdots & \tilde{v}_m & & & & & & & & & & \\ & \tilde{v}_1 & & & & \tilde{v}_2 & \cdots & \cdots & \tilde{v}_m & & & & & & \\ & & \ddots & & & & \ddots & & & \tilde{v}_3 & \cdots & \tilde{v}_m & & & \\ & & & \ddots & & & & \ddots & & & \ddots & & \cdots & \tilde{v}_{m-1} & \tilde{v}_m \\ & & & & \tilde{v}_1 & & & & \tilde{v}_2 & & & \tilde{v}_3 & \cdots & & \tilde{v}_{m-1} & \tilde{v}_m \end{pmatrix}$$

である．与えられた多項式 $f(x)$ と $g(x)$ の Bezout 行列を $B = (b_{ij})$ とし，特異値分解 $B = U\Sigma V^T$ の特異ベクトル $V = (v_{ij})$ とする．初期値を $\boldsymbol{x}_0 = (b_{11}, \ldots, b_{1m}, b_{22}, \ldots, b_{2m}, \ldots, b_{mm}, v_{1,m-d+1}, \ldots, v_{m,m-d+1}, v_{1,m-d+2}, \ldots, v_{m,m-d+2}, \ldots, v_{mm})$ と与え，修正 Newton 法によって問題 2 を解く．

修正 Newton 法の計算結果 $\boldsymbol{x}$ から $(\tilde{b}_{11}, \ldots, \tilde{b}_{mm})$ を得ることで，$\tilde{B}$ を得る．

次に，$\tilde{B}$ から k 次の近似 GCD $\gcd(\tilde{f}, \tilde{g})$ を求める．

補題 3 (Barnett の定理 [6])

f, g を m 次多項式とする．k を $\deg(\gcd(f,g))$ とする．$\mathrm{Bez}(f,g) = (\boldsymbol{b}_1, \cdots, \boldsymbol{b}_m)$ の前から $(m-k)$ 列 $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_{m-k}$ は一次独立であり，後ろから k 列 $\boldsymbol{b}_{m-k+1}, \ldots, \boldsymbol{b}_m$ が前の $(m-k)$ 列で

$$\boldsymbol{b}_i = \sum_{j=1}^{m-k} c_{i,j}\boldsymbol{b}_j, \quad i = m-k+1, \ldots, m \tag{10}$$

のように張られる．さらに，f, g のモニックな最大公約子 $\gcd(f,g)$ は次のように表される．

$$\gcd(f,g) = x^k + c_{m-k+1,m-k}x^{k-1} + \cdots + c_{m,m-k}. \tag{11}$$

□

求めた近似 GCD を $h(x) = h_k x^k + \cdots + h_0$ とする．$(m-k)$ 次余因子 $\bar{f}(x)$ と $(n-k)$ 次余因子 $\bar{g}(x)$ をそれぞれ

$$\bar{f}(x) = \bar{f}_{m-k}x^{m-k} + \cdots + \bar{f}_0 x^0, \quad \bar{g}(x) = \bar{g}_{n-k}x^{n-k} + \cdots + \bar{g}_0 x^0$$

とおき，近似多項式 $\tilde{f}$ に関する摂動量 $\|f - \tilde{f}\|^2 = \|f - h\bar{f}\|^2 = (f_i - \sum_{i=0}^{m} \bar{f}_{m-i}h_i)^2$ を最小化する余因子 $\bar{f}$ を求める．この問題は凸二次計画問題であるため，二次計画法 [9] で解く．同様に $\bar{g}$ も求める．そして近似多項式 $\tilde{f}$ と $\tilde{g}$ を $\tilde{f} = h\bar{f}, \tilde{g} = h\bar{g}$ により求める．

4　実験結果

本章では，100 組の近似 GCD を持つ多項式の組を用いて，第 4 章で述べた Bezout 法の実験結果について述べる．

与えられた多項式		近似GCD		余因子		摂動項
$\hat{f}(x)$	$=$	$h(x)$	$\times$	$\bar{f}(x)$	$+$	$\Delta f(x)$
$\hat{g}(x)$	$=$	$h(x)$	$\times$	$\bar{f}(x)$	$+$	$\Delta g(x)$
10 次		5 次		5 次		摂動量: 0.1

図 1: テスト用多項式の構成

100 組の多項式の組 $\hat{f}(x)$ と $\hat{g}(x)$ は，係数を無作為に与えた 5 次の GCD $h(x)$ を持つ 10 次の多項式 $h(x)\bar{f}(x)$ および $h(x)\bar{g}(x)$ に，係数を無作為に与えた摂動量 0.1 の 10 次多項式 $\Delta f(x)$ および $\Delta g(x)$ をそれぞれ加えたものである (図 1 を参照)．本実験に用いられたモニックな多項式の組 $f(x)$ と $g(x)$ は，Sylvester 法 [14] の実験例 [15] で与えた，$\hat{f}(x)$ と $\hat{g}(x)$ それぞれのノルムを 1 にしたもの，すなわち $f(x) = \hat{f}(x)/\|\hat{f}(x)\|$，$g(x) = \hat{g}(x)/\|\hat{g}(x)\|$ である．今回は，CPU Intel(R) Core(TM) i5-6600 @3.30GHz，メモリ 8.00GB，Windows 10，数式処理システム Maple 2018 を用いて，実験を行った．実験結果を表 1 に示す．

表 1: テスト用多項式に対する実験結果

平均摂動量			平均計算時間 (秒)	
与えられた多項式	Sylvester 法	Bezout 法	Sylvester 法	Bezout 法
7.0×10^{-3}	1.2×10^{-3}	1.3×10^{-2}	1.3×10^{-2}	9.0×10^{-1}

摂動量の結果を見ると，Bezout 法で求めた多項式の摂動量は最初に与えられた多項式の摂動量より大きく，Sylvester 法による摂動量と比較すると，10 倍程度の大きさである．

また，平均計算時間を見ると，Bezout 法の平均計算時間は Sylverster 法のそれの 10 倍程度になっている．原因の一つとして，修正 Newton 法で用いられるヤコビ行列のサイズの差が考えられるが，詳しい分析は今後の研究課題である．

5 まとめ

本稿では，Bezout の終結式行列を用いた GPGCD 計算アルゴリズムを提案し，実験を行い，アルゴリズムの動作を確かめた．実験結果より，現在の Bezout 法は，摂動量および計算時間とも Sylvester 法の結果に達していない．

今後は，近似 GCD の次数が大きい場合，与えられた多項式の係数が大きい場合，与えられた摂動量が大きい場合など，様々な例に対する実験を行い，Bezout 法の検証を行う．また，Sylvester 法に対し，Bezout 法の摂動量および計算時間の縮小によるアルゴリズムの性能の改善を目指す．

参 考 文 献

[1] D. A. Bini, and P. Boito. Structured Matrix-Based Methods for Polynomial ϵ-Gcd. In *Proc. ISSAC '07*, 9–16. ACM Press, 2007.

[2] W. S. Burnside and A. W. Panton. *The Theory of Equations*, Vol. II. Dublin University Press, 75–80, 1901.

[3] P. Chin, R. M. Corless, and G. F. Corliss. Optimization Strategies for the Approximate GCD Problem. In *Proc. ISSAC '98,* 228–235, ACM Press, 1998.

[4] R. M. Corless, P. Gianni, B. M. Trager, and S. M. Watt. 1995. The Singular Value Decomposition for Polynomial Systems. In *Proc. ISSAC '95,* 195–207. ACM Press, 1995.

[5] R. M. Corless, S. M. Watt, and L. Zhi. QR Factoring to Compute the GCD of Univariate Approximate Polynomials. *IEEE Transactions on Signal Processing,* 52 (12): 3394–3402, 2004.

[6] G. M. Diaz-Toca, L. Gonzalez-Vega. Barnett's Theorems About the Greatest Common Divisor of Several Univariate Polynomials Through Bezout-like Matrices, *Journal of Symbolic Computation* (2002) 34, 59–81, 2002.

[7] G. H. Golub and C. F. van Loan. Matrix Computations (4th Edition). Johns Hopkins University Press, 2013.

[8] J. Grabmeie, E. Kaltofen and V. Weispfenning (Eds.) , Computer Algebra Handbook, Springer-Verlag Berlin Heidelberg New York, 2003.

[9] J. Norcedal and S. J. Wright, Numerical Optimization (2nd Ed.), Springer, 2006.

[10] T. Sasaki and M-T. Noda. Approximate Square-Free Decomposition and Root-Finding of III-Conditioned Algebraic Equations. *Journal of Information Processing,* 12 (2): 159–168, 1989.

[11] A. Schönhage. Quasi-GCD Computations. *Journal of Complexity,* 1 (1): 118-137, 1985.

[12] È. Schost, and P.-J. Spaenlehauer. 2016. A Quadratically Convergent Algorithm for Structured Low-Rank Approximation. *Foundations of Computational Mathematics* 16 (2), 457–492, 2016.

[13] K. Tanabe. A geometric method in nonlinear programming. *J. Optim. Theory Appl.,* Vol. 30, No. 2, pp. 181–210, 1980.

[14] A. Terui. GPGCD: An iterative method for calculating approximate GCD of univariate polynomials. *Theoretical Computer Science,* 479, 127–149, 2013.

[15] A. Terui. Dataset for the GPGCD Algorithm. `https://github.com/atelierateru i/tcs-snc2011-data`, (参照 2018-02-13).

[16] S. M. Watt, J. Verschelde, L. Zhi (eds). Proceedings of the 2014 Symposium on Symbolic-Numeric Computation (Shanghai, China, 2014), ACM, New York, 2014.

[17] Z. Zeng. The Numerical Greatest Common Divisor of Univariate Polynomials. In *Randomization, Relaxation, and Complexity in Polynomial Equation,* Contemporary Mathematics, 556, 187–217, AMS, 2011.