制約つき最適化に基づく1変数多項式の近似GCDの反復算法*

照井　章

筑波大学大学院 数理物質科学研究科

概要

本稿では, 与えられた実係数 1 変数多項式の組に対し, 近似最大公約子 (GCD) を計算する反復算法を提案する. 本算法は, 与えられた問題を制約つき最小化問題に帰着させ, 勾配射影法の一般化である修正 Newton 法を用いて反復計算で最適解を求めるもので, 同様に最適化法を用いる他の近似 GCD 算法と比較して, 同等の精度で大幅な効率化が図られている.

An Iterative Method for Calculating Approximate GCD of Univariate Polynomials based on Constrained Optimization

Akira Terui

Graduate School of Pure and Applied Sciences, University of Tsukuba

Abstract

We present an iterative algorithm for calculating approximate greatest common divisor (GCD) of univariate polynomials with the real coefficients. The problem of approximate GCD is transfered to a constrained minimization problem, then solved with the so-called modified Newton's method, which is a generalization of the gradient-projection method, by searching the solution iteratively. Our algorithm remarkably exceeds similar algorithms which use optimization methods in efficiency, while keeping accuracy almost the same.

1　はじめに

本稿では, 近似代数計算 [9] の算法として, 近似最大公約子 (GCD) の問題を取り上げる. これは, 多項式の組（一般的には互いに素）と, 次数 d が与えられたときに, 与えられた多項式の係数に摂動を加え, d 次の GCD をもつような系を探索し, 見つかった GCD を, 与えられた多項式の近似 GCD と呼ぶものである.

近似 GCD は, 近似代数計算の中でも最も古くから活発に研究が行われてきた問題の一つで, これまでに様々な算法が提案されている（詳細は論文 [6] およびその参考文献を参照）. 本稿では, これらの中で, 近似 GCD の問題を制約つき最小化問題に帰着させ, 反復解法で解く最適化法に着目する. 最適化法を用いた既存の算法では, Levenberg-Marquard 法 [1] や Gauss-Newton 法 [7], 構造化行列を用いた最小二乗法の一種である STLN 法 (Structured Total Least Norm) ([2], [3]) 等が用いられており, 特に, 最近提案された STLN 法に基づく算法は, 近似 GCD を得るのに要する係数の摂動を小さく抑える点で注目を集めている.

本稿では, 勾配射影法の一般化と位置づけることのできる, 田邉 ([5], [8, 第 4 章]) による修正 Newton 法を用いる算法を提案する. 本算法の実験結果では, STLN 法に基づく算法と同程度の摂動で近似 GCD を探索でき, かつ大幅な効率化が図られている. なお, 本稿の内容の詳細については論文 [6] を参照されたい.

2　近似 GCD 問題と制約つき最小化問題への帰着

$F(x), G(x)$ を互いに素な実係数 1 変数多項式の組とし, 次式で与えられるものとする.

$$\begin{aligned} F(x) &= f_m x^m + f_{m-1} x^{m-1} + \cdots + f_0, \\ G(x) &= g_n x^n + g_{n-1} x^{n-1} + \cdots + g_0. \end{aligned} \tag{1}$$

*第 38 回数値解析シンポジウム講演予稿集, pp. 95–98 (2009 年 6 月 17 日, 熱川ハイツ).

($m \geq n > 0$ とする.) 与えられた次数 d（ただし $n \geq d > 0$）に対し, $F(x)$ と $G(x)$ の係数に摂動を加えることにより, 次式のような $\tilde{F}(x)$ と $\tilde{G}(x)$ を計算することを考える.

$$\begin{aligned}\tilde{F}(x) &= F(x) + \Delta F(x) = H(x) \cdot \bar{F}(x), \\ \tilde{G}(x) &= G(x) + \Delta G(x) = H(x) \cdot \bar{G}(x).\end{aligned} \tag{2}$$

ここに, $\Delta F(x)$, $\Delta G(x)$ は, 次数がそれぞれ $F(x)$, $G(x)$ の次数を超えないような多項式, $H(x)$ は d 次の多項式で, $\bar{F}(x)$ と $\bar{G}(x)$ は互いに素とする. 式 (2) をみたす $\tilde{F}$, $\tilde{G}$, $\bar{F}$, $\bar{G}$, H が計算されたとき, H を F と G の**近似 GCD** と呼ぶ. 本稿では, **与えられた次数 d に対し, 摂動のノルム $\|\Delta F(x)\|_2^2 + \|\Delta G(x)\|_2^2$ をなるべく小さく保ちつつ, F と G の d 次の近似 GCD H を探索する問題を解く**.

$\tilde{F}(x)$, $\tilde{G}(x)$ を, それぞれ

$$\begin{aligned}\tilde{F}(x) &= \tilde{f}_m x^m + \cdots + \tilde{f}_0 x^0, \\ \tilde{G}(x) &= \tilde{g}_n x^n + \cdots + \tilde{g}_0 x^0\end{aligned} \tag{3}$$

と表す. $\tilde{F}$ と $\tilde{G}$ が d 次の GCD をもつとき, 部分終結式の理論により, $\tilde{F}$ と $\tilde{G}$ の $d-1$ 次の部分終結式は 0 になる. ゆえに, $\tilde{F}$ と $\tilde{G}$ の $d-1$ 次の部分終結式行列

$$N_{d-1}(\tilde{F}, \tilde{G}) = \underbrace{\left(\begin{array}{cccccc}\tilde{f}_m & & & \tilde{g}_n & & \\ \vdots & \ddots & & \vdots & \ddots & \\ \tilde{f}_0 & & \tilde{f}_m & \tilde{g}_0 & & \tilde{g}_n \\ & \ddots & \vdots & & \ddots & \vdots \\ & & \tilde{f}_0 & & & \tilde{g}_0\end{array}\right)}_{n-d+1 \qquad\qquad m-d+1} \tag{4}$$

（式 (4) のように, $\tilde{F}$ の係数を $n-d+1$ 列, $\tilde{G}$ の係数を $m-d+1$ 列並べた行列）はランクが full rank から 1 落ちるため, 互いに素な多項式 $A(x)$ と $B(x)$ が存在して

$$A\tilde{F} + B\tilde{G} = 0 \tag{5}$$

（ただし $\deg(A) = n-d$, $\deg(B) = m-d$）をみたす. ゆえに, 本稿で考える問題は, 与えられた $F(x)$, $G(x)$, d に対し, 方程式 (5) をみたすような $\Delta F(x)$, $\Delta G(x)$, $A(x)$, $B(x)$ で, $\|\Delta F\|_2^2 + \|\Delta G\|_2^2$ がなるべく小さくなるものを探索する問題に帰着される.

$A(x)$, $B(x)$ を, それぞれ

$$\begin{aligned}A(x) &= a_{n-d} x^{n-d} + \cdots + a_0 x^0, \\ B(x) &= b_{m-d} x^{m-d} + \cdots + b_0 x^0\end{aligned} \tag{6}$$

と表すことにより, 方程式 (5) は

$$N_{d-1}(\tilde{F}, \tilde{G}) \cdot {}^t(a_{n-d}, \ldots, a_0, b_{m-d}, \ldots, b_0) = \mathbf{0} \tag{7}$$

と表され, $\|\Delta F\|_2^2 + \|\Delta G\|_2^2$ は

$$\begin{aligned}&\|\Delta F\|_2^2 + \|\Delta G\|_2^2 = \\ &\quad (\tilde{f}_m - f_m)^2 + \cdots + (\tilde{f}_0 - f_0)^2 \\ &\qquad + (\tilde{g}_n - g_n)^2 + \cdots + (\tilde{g}_0 - g_0)^2\end{aligned} \tag{8}$$

と表される. ゆえに, 方程式 (7) は, $\tilde{f}_m, \ldots, \tilde{f}_0$, $\tilde{g}_n, \ldots, \tilde{g}_0$, $a_{n-d}, \ldots, a_0$, $b_{m-d}, \ldots, b_0$ を変数とする $m+n-d+1$ 個の連立方程式

$$\begin{aligned}g_1 &= \tilde{f}_m a_{n-d} + \tilde{g}_n b_{m-d} = 0, \\ &\vdots \\ g_{m+n-d+1} &= \tilde{f}_0 a_0 + \tilde{g}_0 b_0 = 0\end{aligned} \tag{9}$$

と表される（式 (7) における第 j 行の方程式を g_j とおいた）. さらに, $A(x)$ と $B(x)$ に対し, $\|A(x)\|_2^2 + \|B(x)\|_2^2 = 1$ なる制約を加える. これを

$$g_0 = a_{n-d}^2 + \cdots + a_0^2 + b_{m-d}^2 + \cdots + b_0^2 - 1 = 0 \tag{10}$$

とし, 方程式 (9) に加える.

ここで, これまでの多項式の係数を表す変数

$$\begin{aligned}&(\tilde{f}_m, \ldots, \tilde{f}_0, \tilde{g}_n, \ldots, \tilde{g}_0, \\ &\qquad a_{n-d}, \ldots, a_0, b_{m-d}, \ldots, b_0)\end{aligned} \tag{11}$$

を, それぞれ $\boldsymbol{x} = (x_1, \ldots, x_{2(m+n-d+2)})$ に置き換える. すると, 式 (8) および方程式 (9)（方程式 (10) を含む）は, それぞれ

$$\begin{aligned}f(\boldsymbol{x}) &= (x_1 - f_m)^2 + \cdots + (x_{m+1} - f_0)^2 \\ &\quad + (x_{m+2} - g_n)^2 + \cdots + (x_{m+n+2} - g_0)^2,\end{aligned} \tag{12}$$

$$\begin{aligned}&\boldsymbol{g}(\boldsymbol{x}) = \\ &\quad {}^t(g_0(\boldsymbol{x}), g_1(\boldsymbol{x}), \ldots, g_{m+n-d+1}(\boldsymbol{x})) = \mathbf{0}\end{aligned} \tag{13}$$

と表される.

以上により, 本稿で考える近似 GCD の問題は, 以下の制約つき最小化問題に帰着される.

問題 1 方程式 (13) ($\boldsymbol{g}(\boldsymbol{x}) = \mathbf{0}$) の下で, 式 (12) の $f(\boldsymbol{x})$ を最小化せよ. □

3 勾配射影法と修正 Newton 法

本章では, $\boldsymbol{x} \in \mathbf{R}^n$ に対し, 制約条件 $\boldsymbol{g}(\boldsymbol{x}) = \boldsymbol{0}$（ただし $\boldsymbol{g}(\boldsymbol{x}) = {}^t(g_1(\boldsymbol{x}), g_2(\boldsymbol{x}), \ldots, g_m(\boldsymbol{x}))$, $m \le n$ とする）のもとで, 目的関数 $f(\boldsymbol{x}) : \mathbf{R}^n \to \mathbf{R}$ を最小化する問題を考える. 許容領域を $V_{\boldsymbol{g}} = \{\boldsymbol{x} \in \mathbf{R}^n \mid \boldsymbol{g}(\boldsymbol{x}) = \boldsymbol{0}\}$ とするとき, $\boldsymbol{x} \in V_{\boldsymbol{g}}$ に対し, ヤコビ行列 $J_{\boldsymbol{g}}(\boldsymbol{x}) = \left(\dfrac{\partial g_i}{\partial x_j}\right)$ が full rank, すなわち $\mathrm{rank}(J_{\boldsymbol{g}}(\boldsymbol{x})) = m$ が成り立つならば, $V_{\boldsymbol{g}}$ は $\mathbf{R}^n$ の $n - m$ 次元微分多様体となる. このとき, $V_{\boldsymbol{g}}$ 上で f を最小化する局所解の候補として, “1 次の必要条件” [8, 第 1 章] をみたす点を探索する.

勾配射影法 [4]（詳細は紙面の都合で省略）は, $V_{\boldsymbol{g}}$ 上の点 $\boldsymbol{x}_k$ に対し, 以下の計算を繰り返すことにより, $V_{\boldsymbol{g}}$ 上で f を最小化する局所解を探索する.

1. **[射影]** 点 $\boldsymbol{x}_k$ における f の最急降下方向 $-\nabla f(\boldsymbol{x}_k)$ を, $\boldsymbol{x}_k$ における $V_{\boldsymbol{g}}$ の接平面に射影したベクトルを探索方向 $\boldsymbol{d}_k$ とし, $\boldsymbol{y}_k = \boldsymbol{x}_k + \alpha_k \cdot \boldsymbol{d}_k$（$\alpha_k$ は適当なステップ幅で, $0 < \alpha_k \le 1$ をみたす）とする.

2. **[引き戻し]** 点 $\boldsymbol{y}_k$ を適当な方法で $V_{\boldsymbol{g}}$ 上に引き戻し, これを $\boldsymbol{x}_{k+1}$ とする.

田邉 ([5], [8, 第 4 章]) による修正 Newton 法は, Newton 法で用いられる Lagrange 関数の Hesse 行列を修正することにより, さまざまな解法を導出するものである. 勾配射影法と同値な解法では, $V_{\boldsymbol{g}}$ 上の点 $\boldsymbol{x}_k$ に対し, 探索方向 $\boldsymbol{d}_k$ と, Lagrange 乗数 $\boldsymbol{\lambda}_{k+1}$ を, 次式の連立 1 次方程式を解くことによって求める.

$$\begin{pmatrix} I & -{}^t(J_{\boldsymbol{g}}(\boldsymbol{x}_k)) \\ J_{\boldsymbol{g}}(\boldsymbol{x}_k) & \boldsymbol{O} \end{pmatrix} \begin{pmatrix} \boldsymbol{d}_k \\ \boldsymbol{\lambda}_{k+1} \end{pmatrix} = -\begin{pmatrix} \nabla f(\boldsymbol{x}_k) \\ \boldsymbol{g}(\boldsymbol{x}_k) \end{pmatrix}. \tag{14}$$

（I は単位行列.）探索方向 $\boldsymbol{d}_k$ は, $\boldsymbol{x}_k$ が許容領域 $V_{\boldsymbol{g}}$ 内にあるならば f の最急降下方向 $-\nabla f(\boldsymbol{x}_k)$ になり, $\boldsymbol{x}_k$ が許容領域から外れると, これに $\boldsymbol{x}_k$ を許容領域 $V_{\boldsymbol{g}}$ に引き戻す方向が加わる. この意味で, 方程式 (14) による修正 Newton 法は, 勾配射影法における「射影」と「引き戻し」の 2 つのステップが, 方程式 (14) を解くという 1 ステップで実行可能であるという特徴をもつ.

4 近似 GCD の算法

実際の近似 GCD の算法を構築するにあたっては, 主に以下の問題を考慮する必要がある.

1. 反復計算の過程において, ヤコビ行列 $J_{\boldsymbol{g}}(\boldsymbol{x})$ が full rank である（ランクが $J_{\boldsymbol{g}}(\boldsymbol{x})$ の行数に等しい）こと.

2. 反復計算の初期値の設定.

3. GCD となる多項式の実際の計算.

以下では, 上記の項目 1. および 2. について述べる (3. は紙面の都合で省略する. 論文 [6] を参照). その後, 実際の近似 GCD 算法を示す.

4.1 ヤコビ行列のランク

反復計算の過程において, ヤコビ行列 $J_{\boldsymbol{g}}(\boldsymbol{x})$ が full rank であることが保証される必要がある（そうでないと, 方程式 (14) の係数行列が特異になり, 探索方向を決定できない）. この問題については, 許容領域 $V_{\boldsymbol{g}}$ 上の点 $\boldsymbol{x}$ に対応する多項式 $\tilde{F}$, $\tilde{G}$ の GCD が d を超えないならば, $J_{\boldsymbol{g}}(\boldsymbol{x})$ は full rank であることが示される（詳細は論文 [6] を参照）. よって, 最小解の探索方向が適切（近似 GCD の次数が d を超えないような探索方向をとり続ける）ならば, $J_{\boldsymbol{g}}(\boldsymbol{x})$ は full rank であることがわかる.

4.2 初期値の設定

初期値の設定は, F と G の $d-1$ 次の部分終結式行列 $N_{d-1}(F,G)$ の特異値分解 (SVD) をもとに行う. $N_{d-1}(F,G)$ の特異値分解 $N_{d-1}(F,G) = U\,\Sigma\,{}^tV$ を

$$\begin{aligned} U &= (\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{m+n-2d}), \\ \Sigma &= \mathrm{diag}(\sigma_1, \ldots, \sigma_{m+n-2d}), \\ V &= (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{m+n-2d}) \end{aligned}$$

で表す. ここに, $\boldsymbol{u}_j \in \mathbf{R}^{m+n-d}$, $\boldsymbol{v}_j \in \mathbf{R}^{m+n-2d}$, $\Sigma = \mathrm{diag}(\sigma_1, \ldots, \sigma_{m+n-2d})$（対角行列で, (j,j) 成分が σ_j）で, $\sigma_1 \ge \cdots \ge \sigma_{m+n-2d}$ をみたす. 最小特異値 σ_{m+n-2d} および特異ベクトル $\boldsymbol{u}_{m+n-2d}, \boldsymbol{v}_{m+n-2d}$ は $N_{d-1} \cdot \boldsymbol{v}_{m+n-2d} = \sigma_{m+n-2d}\boldsymbol{u}_{m+n-2d}$ をみたす.

そこで, $\boldsymbol{v}_{m+n-2d} = {}^t(\bar{a}_{n-d}, \ldots, \bar{a}_0, \bar{b}_{n-d}, \ldots, \bar{b}_0)$ に対し

$$\bar{A}(x) = \bar{a}_{n-d}x^{n-d} + \cdots + \bar{a}_0 x^0,$$
$$\bar{B}(x) = \bar{b}_{m-d}x^{m-d} + \cdots + \bar{b}_0 x^0$$

とおくと, $\bar{A}(x)$ と $\bar{B}(x)$ は, $A(x) = \bar{A}(x)$, $B(x) = \bar{B}(x)$ とおくことにより, $\|A\|_2^2 + \|B\|_2^2 = 1$ をみたす多項式 $A(x)$, $B(x)$ の中で $\|AF + BG\|_2$ を最小にする. 以上より, 反復計算の初期値は, F, G, $\bar{A}$, $\bar{B}$ の係数を用いて

$$\boldsymbol{x}_0 = (f_m, \ldots, f_0, g_n, \ldots, g_0, \bar{a}_{n-d}, \ldots, \bar{a}_0, \bar{b}_{m-d}, \ldots, \bar{b}_0) \quad (15)$$

で与える.

4.3 算法

実際の近似 GCD の算法は以下の通りである.

算法 1 (GPGCD: 修正 Newton 法（勾配射影法）に基づく近似 GCD の算法)

- 入力:
  - $F(x), G(x) \in \mathbf{R}[x]$（ただし $\deg(F) \geq \deg(G) > 0$）,
  - $d \in \mathbf{N}$ (ただし $d \leq \deg(G)$): 近似 GCD の次数,
  - $\varepsilon > 0$: 残差のしきい値,
  - $u \in \mathbf{N}$: 反復回数のしきい値.
- 出力: $\tilde{F}(x), \tilde{G}(x), H(x) \in \mathbf{R}[x]$
  $\tilde{F}$, $\tilde{G}$ は, それぞれ F, G の係数に摂動を与えたもので, d 次の GCD H をもつ.

Step 1 [**初期値の設定**] 第 4.2 節の議論より, 式 (15) のように初期値 $\boldsymbol{x}_0$ を与える.

Step 2 [**反復計算**] 修正 Newton 法により, 式 (12) および方程式 (13) に対し, 制約条件 $\boldsymbol{g}(\boldsymbol{x}) = \boldsymbol{0}$ の下で $\bar{f}(\boldsymbol{x}) = \frac{1}{2}f(\boldsymbol{x})$ の最小解を求める（$\bar{f}(\boldsymbol{x}) = \frac{1}{2}f(\boldsymbol{x})$ とおくことについての詳細は論文 [6] を参照）. 探索方向 $\boldsymbol{d}_k$ が $\|\boldsymbol{d}_k\|_2 < \varepsilon$ をみたすか, 反復回数が u を超えた段階で, 反復計算を終了する.

Step 3 [$\tilde{F}$**,** $\tilde{G}$**,** H **の計算**] 実際の GCD となる $H(x)$ と, H を GCD としてもつ $\tilde{F}(x)$, $\tilde{G}(x)$ の計算を行い, $\tilde{F}$, $\tilde{G}$, H を返す. もし Step 2 が u 回の反復で終了しなかった場合は, その旨をユーザに報告する.

参考文献

[1] P. Chin, R. M. Corless, and G. F. Corliss. Optimization strategies for the approximate GCD problem. In *Proc. 1998 International Symposium on Symbolic and Algebraic Computation*, pages 228–235. ACM, 1998.

[2] E. Kaltofen, Z. Yang, and L. Zhi. Approximate greatest common divisors of several polynomials with linearly constrained coefficients and singular polynomials. In *Proc. 2006 International Symposium on Symbolic and Algebraic Computation*, pages 169–176. ACM, 2006.

[3] E. Kaltofen, Z. Yang, and L. Zhi. Structured low rank approximation of a Sylvester matrix. In D. Wang and L. Zhi, editors, *Symbolic-Numeric Computation*, pages 69–83. Birkhäuser, 2007.

[4] J. B. Rosen. The gradient projection method for nonlinear programming. II. Nonlinear constraints. *J. Soc. Indust. Appl. Math.*, 9:514–532, 1961.

[5] K. Tanabe. A geometric method in nonlinear programming. *J. Optim. Theory Appl.*, 30(2):181–210, 1980.

[6] A. Terui. An iterative method for calculating approximate GCD of univariate polynomials. In *Proc. 2009 International Symposium on Symbolic and Algebraic Computation*, pages 351–358. ACM, 2009.

[7] Z. Zeng. The approximate GCD of inexact polynomials, Part I: a univariate algorithm (extended abstract). preprint. 8 pages.

[8] 藤田宏, 今野浩, 田邉國士. 最適化法. 岩波講座応用数学 [方法 7]. 岩波書店, 1994.

[9] 佐々木建昭, 加古富士雄. 「近似代数」とは？. 数理科学, 36(11):8–20, 1998.