有理関数を基にした多変数近似GCD計算

讃岐, 勝
筑波大学医学医療系&筑波大学附属病院総合臨床教育センター

出版情報：COE Lecture Note. 49, pp.97-103, 2013-08-09. 九州大学マス・フォア・インダストリ研究所
バージョン：
権利関係：

セッション６

Session 6

数式・数値融合計算

Symbolic-numeric computation

有理関数を基にした多変数近似GCD計算

Computing the Approximate Multivariate Greatest Common Divisor via Rational Function

讃岐 勝
筑波大学医学医療系 & 筑波大学附属病院総合臨床教育センター
Masaru Sanuki
Faculty of Medicine, University of Tsukuba
Center for Medical Education and Training, University of Tsukuba Hospital
sanuki@md.tsukuba.ac.jp

Abstract

In this paper, we propse two method to compute the approximate multivarite GCD for polynomial with floating-point numbers. One is based on Páde approximation, the other is based on Barnett's theorem. Also, we propose one refinement technique solving the linear equation within polynomial entries.

1 はじめに

1 変数多項式の近似 GCD（最大公約子）計算に比べて，多変数多項式の近似 GCD の計算に関する研究は盛んではない．本稿では，1 変数多項式の近似 GCD は精度よく計算できると仮定して，多変数多項式の近似 GCD 計算法を新たに提案する．

まず，多項式 F と G の近似 GCD を次のように定義する．

定義 1 (近似 GCD)**.** F と G が $F = C\tilde{F} + \Delta_F$ と $G = C\tilde{G} + \Delta_G$ と多項式の要素でかけるとき，C を許容度 $\varepsilon = \varepsilon(\Delta_F, \Delta_G)$ の近似共通因子といい，次数が最大の近似共通因子を近似 GCD といい $\mathrm{appGCD}(F, G) = C$ でかく（近似 GCD は一意に決定しない）. □

注意 1. 許容度を $\varepsilon = \varepsilon(\Delta_F, \Delta_G)$ と Δ_F, Δ_G の関数で表記した．いろいろ流儀があるが，本稿では

$$\varepsilon(\Delta_F, \Delta_G) = \max\left\{\frac{||\Delta_\mathrm{F}||}{||\mathrm{F}||}, \frac{||\Delta_\mathrm{G}||}{||\mathrm{G}||}\right\} \tag{1}$$

と係数の最大値の大きさを比較することで摂動部を見積もることにする. □

定義から，近似 GCD の許容度を正確に見積もる場合には C の計算以外に $\tilde{F}$ と $\tilde{G}$ を計算する必要がある．これまでの研究では，1. C だけを計算（許容度は正確ではない），2. C を求めた後，除算によって $\tilde{F}$ と $\tilde{G}$ を計算，3. $\tilde{F}$ と $\tilde{G}$ を先に計算し，除算によって C を計算，が主流であ

り，除算の方法によって許容度は変化する（多くの方法は 2-ノルムの意味で最小になるように除算を行う）．実際，すべての要素の決定は refinement（精度の改善）によって行われる．本稿では，すべての要素 $C, \tilde{F}, \tilde{G}$ を求め許容度も正確に計算することを念頭に考える．

上記の目的を達成するため，本稿では有理関数による近似法である Páde 近似を用いた多変数近似 GCD 計算法を提案する．多項式を要素に持つ線形連立方程式を解く必要があるが効率が悪いとされている．[讃岐 2012] では数値計算の算法に帰着する方法が提案され効率は悪くない．また，1 変数 GCD が既知であれば線形連立方程式を解くまでもなく多変数近似 GCD ができることを示す．

近似 GCD の計算では，近似 GCD または余因子のみが計算される．そのため，除算および refinement を通して全ての情報を得る必要があるが，本稿では多項式の関係式から refinement する方法を提案する．多項式要素の線形連立方程式を解くことが可能なため，非効率ではないと推測される．

本稿では次の記号を用いる．主変数 x，従変数 $\boldsymbol{u} = (u_1, \ldots, u_\ell)$ からなる浮動小数係数多項式 $F(x, \boldsymbol{u}), G(x, \boldsymbol{u}) \in \mathbb{F}[x, \boldsymbol{u}]$ を次で表現する．

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

$\deg(F)$ を主変数 x に関する次数とする．多項式 $F(x, \boldsymbol{u}) \in \mathbb{F}[x, \boldsymbol{u}]$ に対して，従変数 $\boldsymbol{u}$ に関する全次数 w の斉次式を $\delta F^{(w)} \in \mathbb{F}[x, \boldsymbol{u}]$ で表す：$F = \sum_{i=0} \delta F^{(i)}$．ただし，$j = 0$ の場合には $\delta F^{(0)} = F^{(0)}$ と表記する場合もある．また，$[F]_i^i = \delta F^{(i)}$ と表記する場合もある．多項式に限らず，行列・ベクトルに関しても同様の表記法を用いる．ベクトル $\boldsymbol{v} \in \mathbb{F}[\boldsymbol{u}]^m$ に対して，$\delta \boldsymbol{v}^{(w)} \in \mathbb{F}[\boldsymbol{u}]^m$ はベクトルの各要素が全次数 w の斉次式から構成されるベクトルである．

1.1 線形方程式の解法

[**?**, 讃岐 2012] では，多項式を要素に持つ線形連立方程式を反復法により求める方法を提案した．以降，何度も利用するので簡単に述べる．次の線形連立方程式を考える．

$$A\boldsymbol{x} = \boldsymbol{b}. \tag{2}$$

ここで，$A \in \mathbb{F}[\boldsymbol{u}]^{m \times m}$ および $\boldsymbol{b} \in \mathbb{F}[\boldsymbol{u}]^m$ である．

$A^{(0)} \in \mathbb{F}^{m \times m}$ が正則と仮定する．このとき，$A^{(0)}\boldsymbol{x} = \boldsymbol{b}^{(0)}$ は線形代数・数値計算で知られた方法で簡単に解くことができる．

今，$A\boldsymbol{x} \equiv \boldsymbol{b} \pmod{I^w}$ が解くことができたと仮定する：$\boldsymbol{x} = \boldsymbol{c}^{(w-1)}$．このとき，$A\boldsymbol{x} \equiv \boldsymbol{b} \pmod{I^{w+1}}$ は次のように解く．この式において，全次数 w の斉次項のみを集めると，

$$\begin{aligned} \delta A^{(w)}\delta\boldsymbol{x}^{(0)} + \ldots + \delta A^{(1)}\delta\boldsymbol{x}^{(w)} + A^{(0)}\delta\boldsymbol{x}^{(w)} &= \delta\boldsymbol{b}^{(w)} \\ A^{(0)}\delta\boldsymbol{x}^{(w)} &= \delta\boldsymbol{b}^{(w)} - \sum_{j=1}^{w} \delta A^{(j)}\delta\boldsymbol{x}^{(w-j)}. \end{aligned} \tag{3}$$

方程式 (3) の右辺について $\delta\boldsymbol{x}^{(j)}$ $(j = 0, \ldots, w-1)$ は仮定より計算済みである．方程式 (3) は行列 $A^{(0)}$ の要素がすべて数値なので，線形代数による方法で解くことが可能である．

逆行列を用いる方法

方程式 (3) において，$w = 0$ のとき，すなわち $A^{(0)}\boldsymbol{x} = \boldsymbol{b}^{(0)}$ の計算を逆行列の計算によって行うと，$w \geq 1$ のとき $(A^{(0)})^{-1}$ はすでに既知なので行列とベクトルの積の計算のみのよって解 $\delta\boldsymbol{x}^{(w)}$ を計算することができる．

反復法による方法

Gauss-Seidel 法，Jacobi 法また Krylov 部分空間法に基づく方法によって計算することができる．ただ，多項式同士の加減算を多く行う必要があり反復回数が多くなったり行列の次数が大きくなると効率的でなくなる．

2　有理関数を利用する方法

今，有理関数 G/F の主変数 x に関する級数展開が得られたとする．

$$\frac{G(x,\boldsymbol{u})}{F(x,\boldsymbol{u})} = h_0(\boldsymbol{u}) + h_1(\boldsymbol{u})x + h_2(\boldsymbol{u})x^2 + \ldots \in \mathbb{F}\{x,\boldsymbol{u}\}. \tag{4}$$

$F = C\tilde{F} + \Delta_F$，$G = C\tilde{G} + \Delta_G$ とかくとき，

$$\begin{aligned}\frac{G}{F} = \frac{C\tilde{G}+\Delta_G}{C\tilde{F}+\Delta_F} &= \frac{C\tilde{G}+\Delta_G}{C\tilde{F}\Big(1+\dfrac{\Delta_F}{C\tilde{F}}\Big)} \\ &= \frac{C\tilde{G}+\Delta_G}{C\tilde{F}}\Big(1-\frac{\Delta_F}{C\tilde{F}}+\tilde{\Delta}^2\Big) \\ &= \frac{\tilde{G}}{\tilde{F}} + \frac{\tilde{F}\Delta_G - \tilde{G}\Delta_F + \Delta^2}{C\tilde{F}^2}\end{aligned} \tag{5}$$

と近似できるので，有理関数の場合においても許容度 $O(\Delta)$ の摂動が入っているとみなすことができる．ここで，$\Delta^2 \in \mathbb{F}\{x\boldsymbol{u}\}$ であり，$||\Delta^2|| = O(\varepsilon^2)$ である．

べき級数展開の方法

G/F の級数展開は実際に次の前処理を行った後，Henrici による方法を用いて行う．べき級数 $A = \sum_{i=0} a_i(\boldsymbol{u})x^i$ と $B = \sum_{i=0} b_i(\boldsymbol{u})x^i$ の積は Cauchy の積法則により，$P = AB$ の x^q の係数 $p_q(\boldsymbol{u})$ は $p_q = \sum_{i=0}^{q} a_i b_{q-i}$ と多項式の積と同様の表現で書くことができる．これによって P/B の係数 a_q は次でかける（$b_0 \neq 0$）．

$$a_p = \frac{p_q - \sum_{i=0}^{q-1} a_i b_{q-i}}{b_0}. \tag{6}$$

ゆえに b_0 に定数項があれば，$1/b_0$ が級数展開することができるため，$a_p \in \mathbb{F}\{\boldsymbol{u}\}$ になるように展開できる．この式は次数の低い項から順に構成される展開式になっていることに注意する．

2.1 Páde 近似による方法

主変数に関する近似 GCD の次数 k が既知とする．このとき，(4) で得た級数を分母の多項式の次数 $m-k$，分子の多項式の次数 $n-k$ の有理関数近似したものは，与えられた多項式から近似 GCD を取り除いた余因子によって構成されたものになる．このような分子・分母を求める方法として Páde 近似による方法がある．1 変数の場合には既知の方法であるが [Pan01]，多変数の場合は多項式を要素に持つ線形連立方程式を解く必要があるため避けられる傾向がある．

実際に次の関係式でかける．

$$L(F)_q \boldsymbol{h}_q = \boldsymbol{g}_q. \tag{7}$$

ここで，各行列，ベクトルは次で表される．

$$L(F)_q = \begin{pmatrix} f_0 & & & \\ f_1 & f_0 & & \\ \vdots & \ddots & \ddots & \\ f_q & f_{q-1} & \cdots & f_0 \end{pmatrix} \in \mathbb{F}[\boldsymbol{u}]^{(q+1)\times(q+1)}, \boldsymbol{g}_q = \begin{pmatrix} g_0 \\ g_1 \\ \vdots \\ g_q \end{pmatrix}, \boldsymbol{h}_q = \begin{pmatrix} h_0 \\ h_1 \\ \vdots \\ h_q \end{pmatrix} \in \mathbb{F}[\boldsymbol{u}]^{q+1}.$$

G/F の級数展開から $\tilde{G}/\tilde{F}$ の分子・分母を求めるためには．近似 GCD の次数 k とするとき，分母の次数 $m-k$，分子の次数 $n-k$ となる Páde 近似により有理関数近似すればよく，各係数は次の関係式で表現される．

$$L(H)_{m+n-2k} \tilde{\boldsymbol{f}}_{m+n-2k} = \tilde{\boldsymbol{g}}_{m+n-2k}. \tag{8}$$

これをみたす $\tilde{F}$ および $\tilde{G}$ のすべての係数を求めるためには，係数を 1 つ定める必要がある．1 変数近似 GCD 計算の場合，$\tilde{F}^{(0)}$ または $\tilde{G}^{(0)}$ の定数係数を 1 にし，その上で補間法によって関係式をみたす係数を計算する．多変数多項式の場合も，同様の方法がとることができるが非常に効率が悪い．

2.2 1 変数 GCD が既知の場合

1 変数 GCD の主変数 x に関する次数 k および近似 GCD $\mathrm{appGCD}(F,G) = C^{(0)} \pmod I$ がわかっていると仮定する（$\tilde{F}^{(0)}$ および $\tilde{G}^{(0)}$ も既知）．あらかじめ，$\mathrm{appGCD}(f_0(\boldsymbol{u}), g_0(\boldsymbol{u})) = c_0(\boldsymbol{u})$ を計算し，$\tilde{f}_0$ を f_0 と c_0 による近似除算によって計算する．定数項を計算した上で，

$$F \to F/f_0 \tag{9}$$

とべき級数除算することによって，入力多項式 F の定数項を 1 にする（数にする）．実際には，計算に必要な従変数の最大全次数 t がわかっているものとし，$F \to F/f_0 \pmod{I^{t+1}}$ を計算する．

このとき，

- $\tilde{F}^{(1)}$ と $\tilde{G}^{(1)}$ の定数項：
  $\delta\tilde{f}_0^{(1)}$ は既知であり，$\delta\tilde{g}_0^{(1)}$ は $h_0\tilde{f}_0 = \tilde{g}_0$ より $\delta\tilde{g}_0^{(1)} = h_0^{(0)}\delta\tilde{f}_0^{(1)} + \delta h_0^{(1)}\delta\tilde{f}_0^{(0)}$ と和・積のみによって計算可能である．

- $\tilde{F}^{(1)}$ と $\tilde{G}^{(1)}$ の x^1 の係数：
  $\delta\tilde{g}_1^{(1)} = [\delta h_0\delta f_1 + \delta h_1\delta f_0]_1^1 = [\delta h_0\delta f_1 + \delta h_1]_1^1$ であり，$\delta g_1^{(1)} = h_0^{(0)}\delta f_1^{(1)} + \delta h_0^{(1)}\delta\tilde{f}_1^{(0)} + \delta h_1^{(1)}$ なる関係式が得られるが，$\delta\tilde{g}_1^{(1)}$ および $\delta\tilde{f}_1^{(1)}$ は定まらない．

- $\tilde{F}^{(1)}$ と $\tilde{G}^{(1)}$ の x^p の係数：
  $\delta\tilde{g}_p^{(1)} = [\sum_{i=0}^{p-1} \delta h_i \delta f_{p-j}^{(1)}]_1^1$ であり，$\tilde{F}^{(1)}$ および $\tilde{G}^{(1)}$ について x^{p-1} までの係数がわかっていたとしても，$\delta\tilde{g}_p^{(1)}$ および $\delta\tilde{f}_p^{(1)}$ は定まらない．

以上のように，1 変数 GCD がわかっていても状況は変わらず，求めるためには $p = m + n - 2k$ まで計算を行い，全次数ごとで Páde 近似そのものを行う必要がある．問題サイズが少し小さくなる．

2.3 Barnett の定理の改良

Diaz-Toca と G. Vega によって，べき級数の係数から構成する行列の線形結合から GCD を得る方法が提案されている [DG02]．これは [Sanuki09] により次のように拡張できる．

定理 1 (Barnett の定理の拡張 [DG02, Sanuki09])**.** 行列 Q_m を次で定義する．

$$Q_m = \begin{pmatrix} h_0 & h_1 & \dots & h_{m-1} \\ h_1 & h_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ h_{m-1} & \dots & h_1 & h_0 \end{pmatrix} = (\boldsymbol{q}_1, \dots, \boldsymbol{q}_m) \in \mathbb{F}[\boldsymbol{u}]^{m\times m}.$$

近似 GCD の主変数 x に関するが k のとき，前から $m-k$ 列 $\boldsymbol{q}_1, \dots \boldsymbol{q}_{m-k}$ は $\mathbb{F}[\boldsymbol{u}]$-線形独立であり，後ろ k 列 $\boldsymbol{q}_{m-k+1}, \dots \boldsymbol{q}_m$ は前から $m-k$ 列のベクトルで張ることができる：

$$\boldsymbol{q}_{m-k+j} = \sum_{i=1}^{m-k-1} r_{j,i}\boldsymbol{q}_i + r_{j,m-k}\boldsymbol{q}_{m-k} \quad (j = 1, \dots, k). \tag{10}$$

このとき，$r_{j,m-k}$ は GCD の x^{k-j} の係数である． □

3 Refinement

多変数多項式 GCD の refinement は 1 変数の場合と同じ方法を選択すると多項式の和・積の計算する必要がある，また行列のサイズが病徴する傾向があるため計算時間がかかってしまう．

本稿では行列のサイズを減らすことに重みを置き，次のような行列 $T(\tilde{F}, \tilde{G}, C, F, G)$・ベクトル $U(\tilde{F}, \tilde{G}, C)$ を考える．

$$T(\tilde{F}, \tilde{G}, C, F, G) = \begin{pmatrix} \tilde{F} & 0 & 0 \\ 0 & 0 & C \\ 0 & G & F \end{pmatrix} \in \mathbb{F}[x, \boldsymbol{u}]^{3\times 3}, U = \begin{pmatrix} C \\ \tilde{F} \\ \tilde{G} \end{pmatrix} \in \mathbb{F}[x, \boldsymbol{u}]^3. \tag{11}$$

まず，次を保証する．

補題 1. $\det(T) = -G(\tilde{F}C) \neq 0.$ □

行列 T が正則であるので，線形連立方程式 $T\boldsymbol{x} = (F, G, 0)^T$ を考えると解 $\boldsymbol{x} = U$ が得られるので，refinement を行うための関係式を導くことができる．行列のサイズが小さいので，逆行列を用いて計算しても効率がよい．実際には次のように計算をする．

算法 1 (多変数多項式の refinement)**.**

- 入力：$C_0, \tilde{F}_0, \tilde{G}_0 \in \mathbb{F}[x, \boldsymbol{u}]$
  $T_0 = T(\tilde{F}_0, \tilde{G}_0, C_0, F, G)$ ，$U_0 = (\tilde{F}_0, \tilde{G}_0, C_0)^T$, $S = (F, G, 0)^T$
- 残差が小さくなるまで，次を繰り返す.
  $i = 0$
  $r_i = T_i U_i - S$;
  $r_i = T_i \boldsymbol{y}$ を解く（3 次正方行列の線形方程式）
  $U_{i+1} = U_i + r_i$
  r_i が十分小さくなったら計算終了

補題 2 (条件数)**.** 各 T_i の条件数は近似 *GCD* の定数項に依存する．定数項が $O(1)$ であれば計算は安定する． □

注意 2. 1 変数近似 GCD をあらかじめ refinement しないと計算は収束しない．そのため，上記の方法以外の方法であらかじめ refienment をする必要がある.

4 まとめ

本稿では，有理関数のべき級数を基にした多変数多項式の近似 GCD 算法について考察した．いずれにおいても 1 変数の場合を拡張しただけにとどまった．refinement に関しては，多項式要素で線形連立方程式が解けることによりこれまでできなかった方法ができるようになったことを確認した．ただ，1 変数多項式の近似 GCD をあらかじめ処理しなければいけないなど，改良の余地はまだある.

参考文献

[Barnett70] S. Barnett. *Greatest common divisor of two polynomials.* Linear Algebra Appl., **3**, 1970, 7–9.

[Barnett71] S. Barnett. *Greatest common divisor of several polynomials.* Proc. Camb. Phil. Soc., **70**, 1971, 263–268.

[BP94] D. Bini and V. Pan. *Polynomial and matrix computations: volume 1 fundamental algorithms.* Birkhäuser, 1994.

[DG02] G. M. Diaz-Toca and L. Gonzalez-Vega. *Barnett's theorems about the greatest common divisor of several univariate polynomials though Bézout-like matrices. J. Symb. Compu.*, **34**, (2002), 59–81.

[DG06] G. M. Diaz-Toca and L. Gonzalez-Vega. *Computing greatest common divisors and squarefree decompositions through matrix methods: The parametric and approximate cases. Linear Algebra Appl.*, **412(2-3)**, (2006), 222–246.

[Henrici56] P. Henrici. Automatic computations with power series. *Journal of the ACM*, 1956 **(3)**, 10–15.

[Knuth97] D. E. Knuth. Art of Computer Programming, Volume 2: Seminumerical Algorithms (Third Edition), Addison-Wesley Professional, 1997.

[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.

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

[Sanuki08] M. Sanuki. A Study on the Approximate GCD, Ph. D. Thesis, University of Tsukuba, 2008.

[Sanuki09] M. Sanuki. Computing multivariate approximate GCD based on Barnett's theorem, *Proc. of SNC'09*, ACM Press, 2009, 149–157.

[讃岐 2012] 讃岐勝, 多項式を要素にもつ線形連立方程式の解法：その 2, 数式処理研究の新たな発展 2012, 京都大学数理解析研究所, (2012 年 7 月 4-6 日)

[讃岐 2013] 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.

[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.