数理解析研究所講究録
第1927巻 2014年 115-121

Barnettの定理に基づく多変数近似GCD計算の改良：モニックでない場合

Improvements of multivariate approximate GCD computation based on Barnett theorem : case of non-monic GCD

讃岐 勝
Masaru Sanuki
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
Faculty of Medicine, University of Tsukuba,
&
Center for Medical Education and Training, University of Tsukuba Hospital *

Abstract

本稿では打ち切りべき級数上で計算を行った（近似）GCD候補から（近似）GCDを構成するために必要なGCDの主係数の構成法について検討する.

1 はじめに

本稿では次の記号を用いる．数体 $\mathbb{K}$ を係数とする多変数多項式環 $\mathbb{K}[x, \boldsymbol{u}] = \mathbb{K}[x, u_1, \ldots, u_\ell]$ において，x を主変数，$\boldsymbol{u} = u_1, \ldots, u_\ell$ を従変数として扱うことにする（$\mathbb{K}[\boldsymbol{u}]$ を係数とする x の多項式とみなす）．$F(x, \boldsymbol{u}) \in \mathbb{K}[x, \boldsymbol{u}]$ の主変数 x に関する次数を $\deg(F)$ で表す．$F(x, \boldsymbol{u})$ の主係数を $\mathrm{lc}(F)$ で表す．多項式 $F(x, \boldsymbol{u})$ と $G(x, \boldsymbol{u})$ の（近似）GCDを $\gcd(F, G)$ で表し，本稿では許容度の表示については省略する．

多変数多項式の近似GCD計算において，数式処理ベースの算法EZ-GCD法 [12]，PC-PRS法 [8]，安定化PC-PRS法・PC-GivensGCD法 [10]，Barnettの方法による拡張 (Bezout構成)[9] を選択した場合，すなわち，打ち切りべき級数上で四則演算によってGCD計算する場合にはGCDの主係数を別に計算する必要がある．表1は，上記アルゴリズムの流れである．2., 3. において，利用するアルゴリズムは異なるが流れは同じである．

通常，与えられた多項式のGCDを求める方法と同様の方法によって主係数のGCDの計算を行う．しかし，主係数は小さい場合近似GCDの許容度と主係数の許容度は異なる．許容度の大きさによって，設定をするパラメータ（許容度）は変化するため，計算するアルゴリズム自体を別に選択することも考慮する必要があるかもしれない．

本稿では，GCDの主係数のみを既存の近似GCD計算をすることなく出力する方法について検討し，近似GCDの主係数の情報が多く含まれているBezout行列を利用する．Bezout行列自信はGCD計算にも利用でき [4, 9]，Sylvester行列よりサイズが小さく，かつ様々な情報を持つ行列である．

*sanuki@md.tsukuba.ac.jp

1.	mod I 上で近似 GCD の候補を計算 $\gcd(F,G) \equiv \tilde{C} \pmod{I}$
2.	GCD の主係数を計算
3.	近似 GCD を計算 $\tilde{C}/\mathrm{lc}(\tilde{C}) \times \mathrm{lc}(C) \equiv \gcd(F,G) \pmod{I}$
4.	試し除算

表 1: 近似 GCD 計算の流れ

2 Barnett の定理

与えられた多項式 $F(x,\boldsymbol{u}), G(x,\boldsymbol{u}) \in \mathbb{K}[x,\boldsymbol{u}]$ に対して，Bezout 行列 $\mathrm{Bez}(F,G)$ は次で定義される．

$$\mathrm{Bez}(F,G) = \begin{pmatrix} b_{0,0} & b_{0,1} & \cdots & b_{0,n-1} \\ b_{0,0} & b_{0,1} & \cdots & b_{0,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n-1,0} & b_{n-1,1} & \cdots & b_{n-1,n-1} \end{pmatrix} = (\boldsymbol{b}_0, \boldsymbol{b}_1, \ldots, \boldsymbol{b}_{n-1}) \in \mathbb{K}[\boldsymbol{u}]^{n\times n}. \tag{1}$$

行列の各要素 $b_{i,j}$ は Bezout 多項式 $\dfrac{F(x,\boldsymbol{u})G(y,\boldsymbol{u}) - F(y,\boldsymbol{u})G(x,\boldsymbol{u})}{x-y} = \displaystyle\sum_{i,j<n} b_{i,j}(\boldsymbol{u})x^i y^j$ の係数であり，Bezout 行列は対称行列である．Dias-Toca & G. Vega による Bezout 行列と GCD の関係を表す定理として Barnett の定理が知られている [4]．この方法は多変数多項式に対しても拡張可能である [9].

定理 1 (Barnett の定理 [4])
$k = \deg(\gcd(f,g))$ とする．このとき，後ろから $(n-k)$ 列 $\boldsymbol{b}_k, \ldots, \boldsymbol{b}_{n-1}$ は一次独立であり，前から k 列 $\boldsymbol{b}_0, \ldots, \boldsymbol{b}_{k-1}$ は後ろの $(n-k)$ 列で張ることができる；

$$\boldsymbol{b}_i = c_{i,1}\boldsymbol{b}_k + \sum_{j=2}^{n-k} c_{i,j}\boldsymbol{b}_{k-1+j} \text{ for } 0 \le i \le k-1. \tag{2}$$

更に，各 $c_{i,1}$ はモニックな GCD の i 次の係数になる：$\gcd(f,g) = x^k + c_{k-1,1}x^{k-1} + \ldots + c_{0,1}$. ∎

アルゴリズム 1 (Barnett の定理の拡張 [9])

Input : $F(x,u)$ *and* $G(x,u) \in \mathbb{K}[x,u]$
Output : $\gcd(F,G)$

Choose an expansion point $\boldsymbol{s} \in \mathbb{K}^{\ell}$.
% Compute the degree of GCD.
$k = \deg(\gcd(F(x,\boldsymbol{s}), G(x,\boldsymbol{s})))$.
% Compute univariate GCD.
LU-decomposition of $\mathrm{Bez}^{(0)}_{k,n-1}(F,G) \pmod{I}$;
$\mathrm{Bez}^{(0)}_{k,n-1}(F,G) = PLU$.
Solve linear equations ($i = 0,\ldots,k-1$), *as follows.*
(Backward and Forward substitutions)
$\mathrm{Bez}^{(0)}_{k,n-1}(F,G)\boldsymbol{c}_i = L(U\boldsymbol{x}_i) = P\tilde{\boldsymbol{b}}_i$.
% Compute multivariate GCD (Bézout lifting).
for $j = 1,\ldots,w$
for $i = 0,\ldots,k-1$
compute $\delta\boldsymbol{c}_i^{(j)}$ *satisfying with*
$\tilde{\boldsymbol{b}}_i \equiv \mathrm{Bez}_{k,n-1}(F,G)(\boldsymbol{c}_i^{(j-1)} + \delta\boldsymbol{c}_i^{(j)}) \pmod{I^{j+2}}$
end do;
end do;
From $\boldsymbol{c}_i^{(w)}$, *compute* $\tilde{C} \equiv \gcd(F,G) \pmod{I^{w+1}}$.
% Power-series multiplication.
$C(x,u) \equiv \tilde{C}(x,u) \times c_k(u) \pmod{I^{w+1}}$.
Return $C(x,u)$.

---

3 主係数の構成

Bezout 行列の正則な部分行列 Bmat_{n-k}

$$\begin{pmatrix} b_{k,k} & b_{k,k+1} & \cdots & b_{k,n-1} \\ b_{k+1,k} & \ddots & & \\ \vdots & & \ddots & \\ b_{n-k,k} & \cdots & \cdots & b_{n-k-1,n-k-1} \end{pmatrix} \in \mathbb{F}[\boldsymbol{u}]^{(n-k)\times(n-k)}$$

について，行列式は

$$\det(\mathrm{Bmat}_{n-k}) \Big| c_k.$$

である．さらに，詳しく見ると実は次が成り立っている [9].

$$\boldsymbol{x} = \boldsymbol{c}_i \propto \begin{pmatrix} O(1/c_k) \\ O(1/{c_k}^2) \\ \vdots \\ O(1/{c_k}^{n-k}) \end{pmatrix}.$$

そのため，次が言える．

$$\det(\mathrm{Bmat}_{n-k}) \Big| {c_k}^{n-k}. \tag{3}$$

3.1 固有値から

行列 M とその固有値 λ_i について

$$\det(M) = \prod_i \lambda_i, \text{ where } \lambda_i \text{ is an eigen-value of } M)$$

が成立する．そこで，次のことが想像できる．

- ある λ_i が c_k になるのか？
- いくつかの λ_i の積が c_k になるのか？
- いくつかの λ_i の因子の積が c_k になるのか？

次の例より，いずれも満たすことはないことがすぐにわかる．

例 1
次の多項式 $f(x)$ と $g(x)$ について，部分 *Bezout* 行列および固有値を見る．

$$f(x) = c(x)(x^3 - 1), g(x) = c(x)(x^3 - x + 2), c(x) = 5x^2 + 2x + 3.$$

このとき，部分 *Bezout* 行列 Bmat_3 は次のようになる．

$$\left(\begin{array}{rr|rrr} 9 & 6 & -12 & -18 & -45 \\ 6 & -23 & -17 & -51 & -15 \\ \hline -12 & -17 & -65 & -41 & -65 \\ -18 & -51 & -41 & -55 & 25 \\ -45 & -15 & -65 & 25 & 0 \end{array}\right) = \left(\begin{array}{cc|c} * & * & * \\ \hline \tilde{b}_0 & \tilde{b}_1 & \mathrm{Bmat}_3 \end{array}\right)$$

- 線形方程式系を解く

$$\mathrm{Bmat}_3 \boldsymbol{x} = \tilde{b}_0 \quad \Rightarrow \quad \boldsymbol{c}_0 = \begin{pmatrix} \frac{3}{5} \\ -\frac{6}{25} \\ \frac{33}{125} \end{pmatrix},$$

$$\mathrm{Bmat}_3 \boldsymbol{x} = \tilde{b}_1 \quad \Rightarrow \quad \boldsymbol{c}_1 = \begin{pmatrix} \frac{2}{5} \\ \frac{11}{25} \\ \frac{52}{125} \end{pmatrix}.$$

- 固有値
  部分 *Bezout* 行列の固有値は次の３つの値である *(出力は Maple による)*.

$$56.9838270670302 + 0. * I, -114.979702523430 + 0. * I, -62.0041245435998 + 0. * I$$

- 行列式：$\det(\mathrm{Bmat}) = 406250 = 2 \times 5^6 \times 13$

以上より，固有値と主係数の間に関係性はない．

3.2 行列式から

次の関係が成立する.

$$\det(\mathrm{Bmat_{n-k}}) = \mathrm{lc}(C)^{(n-k)\times k} \times P, \text{ where } P \text{ is polynomial in } \mathbb{F}[\boldsymbol{u}]. \tag{4}$$

さらに P は $\mathrm{lc}(C)$ で割ることはできない. この関係式を利用して GCD の主係数を計算することを検討する. 次の方針で計算することを考える.

- $\mathrm{lc}(C)$ の次数上界はわかる ($< q$)
- modulo I^{q+1} で計算できないか？, i.e.,

$$\det(\mathrm{Bmat_{n-k}}) \equiv \mathrm{lc}(C)^{(n-k)\times k} \times P \pmod{I^{q+1}}$$

を計算した時に, $\mathrm{lc}(C)$ は計算できるのか？

指数部と多項式の次数が既知の場合

まずは次の例を見る.

例 2 (Exact な場合)
$Q = (1+2u-u^2)^5$ の展開式が与えられており, 指数部が既知の場合に無平方部 $a_0 + a_1u + a_2u^2 + a_3$ を計算できるのか検討する.

打ち切り次数を 3 とした場合, $Q \equiv 1 + 10u + 35u^2 + 40u^3 \pmod{\langle u^4 \rangle}$ が入力として与えられる. このとき係数比較によって無平方部を取り出すことは可能である.

- 定数部：${}_5\mathrm{C}_0 a_0^5 = 1$ なので, $a_0 = 1$.
- u^1：${}_5\mathrm{C}_1 a_0^4 a_1 = 10u$ より $a_1 = 2$.
- u^2：${}_5\mathrm{C}_1 a_0^4 a_2 + {}_5\mathrm{C}_2 a_0^3 a_1^2 = 35u^2$ より $a_2 = -1$
  ここで試し割りを行うと割り切れることが確認できる.

$$Q/(1+2u-u^3) \equiv 0 \pmod{\langle u^4 \rangle}.$$

- ちなみに $a_3 = 0$ も計算可能であり, 次数上限から $(1+2u-u^2)^5$ がわかる.

∎

例 3 (Exact な場合：因子が増えた場合)
$Q = (1+2u)(1+2u-u^2)^5$ の展開式が与えられており, 指数が 5 の無平方部だけを取り出すことが可能であるか検討する.

$\dfrac{\partial}{\partial u}Q$ で行う. 微分をするので, 少し高い次数の係数も必要であり, 変数の個数が 3 個以上になるとこの方法は破綻する. ∎

例 4 (Exact な場合：変数が複数の場合)
$Q(u,v) = (1+u+2v+v^2+uv)(1+2u-2v+u^2)^5$ のの展開式が与えられており, 指数部 5 が既知の場合に指数部 5 の無平方部 $a_0 + a_1u + a_2u^2 + a_3$ を計算できるのか検討する.

変数が複数の場合，全次数変数 t を利用する．$u \mapsto tu$ および $v \mapsto tv$ と変換することで，$Q(u,v,t) = (1+tu+2tv+t^2v^2+t^2uv)(1+2tu-2tv+t^2u^2)^5$ の展開式が入力となる．このとき，Q を t の関数としてみると 1 変数の場合と似たケースになる．

$$\begin{aligned} Q &= (1+b_1t+b_2t^2+b_3t^3)(1+a_1t+a_2t^2+a_3t^3)^5 \\ &\equiv 1+(b_1 +_5 \mathrm{C}_1 a_1)t+(b_2 +_5 \mathrm{C}_1 b_1 a_1 +_5 \mathrm{C}_2 a_1^2 +_5 \mathrm{C}_1 a_2)+\ldots \end{aligned}$$

このような場合，次が選択肢としてある．

1. 微分したものと *GCD* を取る *(*意味がない*)*.
   厳密な *GCD* が必要になる *(modulo* I^{q+1} の世界で計算を終えたい*)*.
   - $Q(u,v,t) = Q_0 = \tilde{Q}_0 L^5$
   - $Q_1 = \dfrac{\partial}{\partial t} Q_0 = \tilde{Q}_1 L^4$
2. 係数比較＆補間法
   これは計算可能である（例 2 に帰着する）.

∎

故に，求めたい多項式の次数および指数部が既知の場合その因子を求めることができる．

行列式 $(\mathrm{mod}\ I^{q+1})$ **の計算**

行列式を計算する方法として，

入力の次数 $\min\{\deg(F),\deg(G)\}$ が大きい場合，行列式 modulo I^{w+1} の計算は重くなる．しかし，主係数を求めるために Bmat_{n-k} の行列式を計算することは必要なく，Bmat_{n-k} の部分行列でよい．$\deg(\gcd(F,G)) = k$ とするとき，Bezout 行列の各要素について c_k のオーダーは次になることが知られている [9].

$$\left(\begin{array}{ccc||ccc} O(1) & \ldots & O(1) & O(c_k) & \ldots & O(c_k) \\ \vdots & & \iddots & & & \\ O(1) & \iddots & & & & \\ \hline\hline O(c_k) & & & O(c_k) & \ldots & O(c_k) \\ \vdots & & & \vdots & \ddots & \vdots \\ O(c_k) & \ldots & & O(c_k) & \cdots & O(c_k{}^2) \end{array}\right)$$

右下の行列は $\mathrm{Bmat}_{n-k} \in \mathbb{K}[x,\boldsymbol{u}]^{(n-k)\times(n-k)}$ に対する．右下の行列の部分行列については，指数部をすぐに計算することができる．実際には 5 次の正方行列程度で主係数を求めることが可能である．

浮動小数係数への適応の際の注意

上で紹介した方法は，多重因子を求めること他ならない．$Q^m + \epsilon$ where $||\epsilon|| \ll 1$ で与えられた多項式について，Q を求めると許容度は $\sqrt[m]{||\epsilon||}$ となり，求めたい精度で計算することはできない．

そのため，近似 GCD 候補を作成した時点，または，近似 GCD が得られて時点で refinement を行い近似 GCD 全体の精度を改善することが必要となる．

参 考 文 献

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

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

[3] P. Boito. fastGCD: `http://www.mathcs.emory.edu/~boito/software.html`

[4] 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.

[5] 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.

[6] J. Moses and D. Y. Y. Yun. *The EZGCD algorithm.* Proc. ACM National Conference, ACM, 1973, 159–166.

[7] 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.

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

[9] M. Sanuki. *Computing multivariate approximate GCD based on Barnett's theorem*, Proc. of Symbolic-Numeric Computation 2009 (SNC 2009), H. Sekigawa & H. Kai (Eds.), 2009, 149-157, Kyoto, Japan, 3-5 August 2009.

[10] M. Sanuki and T. Sasaki. *Computing approximate GCDs in ill-conditioned cases.* Proc. of Symbolic-Numeric Computation 2007 (SNC 2007), J. Verschelde & S. M. Watt (Eds.), 2007, 170–179, London, Ontario, Canada, 25-27 July, 2007.

[11] P. S. Wang. *The EEZ-GCD algorithm.* SIGSAM Bulletin **14** (1980), 50–60.

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