京都大学学術情報リポジトリ
KURENAI 紅
Kyoto University Research Information Repository

京都大学
KYOTO UNIVERSITY

Title	近似共通因子を持つ多項式の規格化 (数式処理 : その研究と目指すもの)
Author(s)	讃岐, 勝
Citation	数理解析研究所講究録 (2013), 1843: 94-100
Issue Date	2013-07
URL	http://hdl.handle.net/2433/195007
Right	
Type	Departmental Bulletin Paper
Textversion	publisher

Kyoto University

数理解析研究所講究録
第1843巻 2013年 94-100

近似共通因子を持つ多項式の規格化
Regularization for Polynomials Having Common Factor

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

近似GCD計算では，共通因子の係数の大きさよって問題が悪条件になることが知られている．本稿では，共通因子の係数の大きさを調整する多項式の規格化の方法について述べる．

1 はじめに

本稿では数体 $\mathbf{K}$ を係数に持つ1変数多項式 $f(x), g(x) \in \mathbf{K}[x]$ を扱う．

浮動小数係数の多項式・行列を扱うにあたり，与えられた問題が良条件であるか・悪条件であるか，また悪条件である場合において問題の良条件化を考えることは，数値計算の分野では当たり前のように行われていることだが近似代数（数式処理）の分野ではそれほど考えられていない．多項式やベクトルの場合で入力が一つの場合，正規化や規格化を行うことにより問題を変換したりスケール化することも多い．2つの言葉は同じ意味で使われることが多いが，本稿では2つの言葉を次のように区別する．

定義 1 (正規化・規格化)
多項式の係数・ベクトルの要素全体に数値をかけて全体を一様に操作する変換を正規化，多項式・ベクトルを一般に作用させる変換を規格化と呼ぶ．

このため，正規化は規格化に含むことにする．実際に例を上げる．

例 1 (正規化・規格化)
多項式 $f(x) = f_n x^n + f_{n-1}x^{n-1} + \ldots + f_0$ について：

- 正規化： $f/\|f\|$
- 規格化： $f(x) \to f(1/x)x^{\deg(f)} = f_0 x^n + f_1 x^{n-1} + \ldots + f_n$, $\mathrm{FFT}(f)$

複数多項式の場合に上の変換を行うと共通因子などの有効な情報が失われてしまう．

近似GCD計算 [SN89] において，悪条件問題の克服は大きなテーマの一つである．これまでGCD計算の悪条件の克服方法をとして次がある．

*sanuki@md.tsukuba.ac.jp

- 微小主係数 GCD 問題：因子分離法 [CWZ04, SS07]
- 巨大主係数問題：多項式の分離 [SS07]

いずれの方法も各多項式に関して分解・変換を行なっており，変換には与えられた多項式の次数 n に関して $O(n^2)$ の計算量が必要である．また，実際に適応すると次数の大きな問題には適応が難しいという欠点がある．

ベズー行列を用いた GCD 計算法 (Barnett の定理)[Barnett70, Barnett71, DG02] は GCD 計算の問題をベズー行列の要素を元にした連立線形方程式に帰着する．互除法・シルベスター行列同様に微小主係数 GCD を持つ場合には悪条件になることが知られているが [Sanuki09]，対策は何も講じられていない．

上に上げた方法はいずれも 1 つの多項式単体を扱う変換で合った．本稿では複数多項式を扱う規格化の方法を提案する．本稿で扱うベズー行列は与えられた複数多項式から構成される行列のため，共通因子などの情報を失うことを避けることができると期待できる．

2 規格化の方法

2.1 Bezout 行列と GCD の関係

与えられた多項式 $f(x), g(x) \in \mathbb{K}[x]$ に対して，ベズー行列 $\mathrm{Bez}(f,g)$ は次で定義される．

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

行列の各要素 $b_{i,j}$ はベズー多項式 $\dfrac{f(x)g(y) - f(y)g(x)}{x-y} = \displaystyle\sum_{i,j<n} b_{i,j} x^i y^j$ の係数であり，ベズー行列は対称行列である．Dias-Toca & G. Vega によるベズー行列と GCD の関係を表す定理として Barnett の定理が知られている [DG02].

定理 2 (Barnett の定理 [DG02])
$k = \deg(\gcd(f,g))$ 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：$\gcd(f,g) = x^k + c_{k-1,1}x^{k-1} + \ldots + c_{0,1}$. ∎

実際には次の連立方程式系を解いて GCD を求める．

$$\tilde{B}_k \boldsymbol{x} = \boldsymbol{b}_i (i = 0, \ldots, k-1). \tag{3}$$

行列 B_k はベズー行列 $\mathrm{Bez}(f,g)$ の後ろから $n-k$ 行，$n-k$ 列の要素からなる正則な対称行列である．

2.2 規格化

式 (4)，すなわち式 (3) の解（の第 1 要素）を変化させると GCD が変化する．連立方程式系 (3) を変化させた $\tilde{B}_k x = \alpha b_i$ は解 $x = \alpha c_i$ を持つ．この条件を保持したまま，ベズー行列全体について

$$\alpha b_i = c_{i,1} b_k + \sum_{j=2}^{n-k} c_{i,j} b_{k-1+j} \tag{4}$$

をみたすような対称行列は次の行列 $B_{k,\alpha}$ になる．

$$B_{k,\alpha} = \left(\begin{array}{ccc|c} & & & \alpha\tilde{b}_0^T \\ & \alpha^2\tilde{B}_{0,k-1} & & \vdots \\ & & & \alpha\tilde{b}_{k-1}^T \\ \hline \alpha\tilde{b}_0 & \cdots & \alpha\tilde{b}_{k-1} & \tilde{B}_k \end{array}\right) \tag{5}$$

$$= (b_0^{(\alpha)}, \ldots, b_{n-1}^{(\alpha)}). \tag{6}$$

ここで，$\tilde{B}_{0,k-1} = (b_{i,j})_{i,j \le k-1}$ である．行列 $B_{k,\alpha}$ は階数 k の対称行列であり，次からベズー行列になることがわかる．

命題 3
任意の対称行列に対するベズー行列が存在する． ∎

また，一意性についても保証が可能である．

命題 4 (ベズー行列の一意性)
2 つの多項式の組 (f,g) と (f',g') のベズー行列が異なるとき，(f,g) と (f',g') は一致しない．

証明　相異なる多項式の組 (f,g) と (f',g') のそれぞれのベズー行列が一致したと仮定する，すなわちベズー多項式が一致すると仮定する $\mathrm{Bpol}(f,g) = \mathrm{Bpol}(f_1,g_1)$．このとき，

$$\begin{aligned} \mathrm{Bpol}(f-f_1, g_1) &= \mathrm{Bpol}(f, g-g_1), \\ \mathrm{Bpol}(f_1, g-g_1) &= -\mathrm{Bpol}(f-f_1, g_1), \end{aligned}$$

であり次が成立する．

$$\begin{aligned} \mathrm{Bpol}(f-f_1, g-g_1) &= \mathrm{Bpol}(f,g) - \mathrm{Bpol}(f,g_1) - \mathrm{Bpol}(f_1, g-g_1) \\ &= \mathrm{Bpol}(f,g) - \mathrm{Bpol}(f,g_1) + \mathrm{Bpol}(f-f_1, g_1) \\ &= \mathrm{Bpol}(f,g) - \mathrm{Bpol}(f_1,g_1) = 0. \end{aligned}$$

したがって，*1)* $f - f_1 = g - g_1$，または *2)* $f - f_1 = 0$ または $g - g_1 = 0$ である．$f - f_1 = g - g_1 = a \neq 0$ のとき，

$$\begin{aligned} \mathrm{Bpol}(f,g) &= \mathrm{Bpol}(a,a) + \mathrm{Bpol}(a,g_1) + \mathrm{Bpol}(f_1,a) + \mathrm{Bpol}(f_1,g_1) \\ &= \mathrm{Bpol}(a, g_1 - f_1) + \mathrm{Bpol}(f_1, g_1) \end{aligned}$$

から $g_1 = f_1$ となり矛盾する．上から $a = 0$ であり，$f - f_1 = 0$ かつ $g - g_1 = 0$ であることがわかる．以上より，仮定に矛盾する． ∎

以上より，$B_{k,\alpha}$ はベズー行列となり，行列を満たすような多項式が存在することがわかる．満たす多項式の GCD は次になる．

$$x^k + \alpha(c_{k-1,1}x^{k-1} + \ldots + c_{0,1}). \tag{7}$$

行列 $B_{k,\alpha}$ に対応する変換の他にも次のような変換が考えられる．

1. 低次の ℓ 項の係数を操作．

$$\left(\begin{array}{cccccc|c} \alpha^2 b_{0,0} & \cdots & \alpha^2 b_{\ell-1,0} & \alpha b_{\ell,0} & \cdots & \alpha\tilde{\boldsymbol{b}}_0^T \\ \vdots & \ddots & \vdots & \vdots & \cdots & \vdots \\ \alpha^2 b_{\ell-1,0} & \cdots & \alpha^2 b_{\ell-1,\ell-1} & \alpha b_{\ell,\ell-1} & \cdots & \alpha\tilde{\boldsymbol{b}}_{\ell-1}^T \\ \alpha b_{\ell,0} & \cdots & \alpha b_{\ell,\ell-1} & b_{\ell,\ell} & \cdots & \tilde{\boldsymbol{b}}_\ell^T \\ \vdots & \cdots & \vdots & \vdots & \cdots & \vdots \\ \hline \alpha\tilde{\boldsymbol{b}}_0 & \cdots & \alpha\tilde{\boldsymbol{b}}_{\ell-1} & \tilde{\boldsymbol{b}}_\ell & \cdots & \tilde{B}_k \end{array}\right) \tag{8}$$

このとき，GCD は $x^k + c_{k-1,1}x^{k-1} + \ldots + c_{\ell,1}x^\ell + \alpha(c_{\ell-1,1}x^{\ell-1} + \ldots + c_{0,1})$ になる．この変換を複数回繰り返すことで，GCD の係数を任意に操作することができる．

2. GCD が変わらない変換．ベズー行列は変換されるが GCD は変わらない．

$$\left(\begin{array}{ccc|cc} & B_{0,k-1} & & & \boldsymbol{b}_0^T \\ & & & & \vdots \\ \hline & & & B_{k,k_1} & \\ \boldsymbol{b}_0^T & \cdots & & & \beta B_{k_1+1} \end{array}\right). \tag{9}$$

2.3 多項式の組の構成

対称行列が与えられた時，それをベズー行列とする多項式の組 (f', g') をどのように求めるかについて解説する．まず多項式の係数とベズー行列の要素について次が成り立つ．

命題 5 ([CZG02])
多項式の組 (f, g) のベズー行列の係数は $P_{i,j} = f_i g_j - f_j g_i$ の和でかける．

$$b_{i,j} = \sum_{k=\max\{0,i-j\}}^{\min\{i,n-1-j\}} P_{i-k,j+1+k}. \tag{10}$$

[CZG02] では各 $P_{i,j} = f_i g_j - f_j g_i$ から $b_{i,j}$ を構成できることを示しているが，$b_{i,j}$ から各 $P_{i,j} = f_i g_j - f_j g_i$ の構成が次の方法で可能である．

アルゴリズム 1 (Find $P_{i,j}$ by marching)

Input: Bezout matrix $B \in \mathbf{F}^{n\times n}$;

P = *upper triangular and diagonal part of* B;
for i *from* $n-1$ *to* 1 *do by* -1
  for j *from* $i-1$ *to* $n-1$ *do*
    $P_{i,j} \leftarrow P_{i,j} - P_{i-1,j+1}$
  end do;
end do;

return $P_{i,j}$

ゆえに，係数の積差 $P_{i,j}$ から各係数を求める問題に帰着される．

$f_n = g_n = 1$ と仮定する．このとき，

$$P_{i,n} = f_i - g_i \in \mathbf{K}, P_{i,j} = f_i g_j - f_j g_i \in \mathbf{K}$$

であり，これらから

$$-P_{i,n} f_j + P_{i,j} = -f_i P_{j,n}$$
$$-P_{i,n} P_{i,k} f_j + P_{k,j} P_{i,n} - (-f_i P_{k,n} P_{j,k} + P_{i,k} P_{j,n}) = 0$$

であり，f_i および f_j を求めることができる．1つわかれば残りの係数もすぐに計算することができる．

2.4 許容度の変化

Barnett の定理より，

$$b_i = c_{i,1} b_k + \sum_{j=2}^{n-k} c_{i,j} b_{k-1+j} + \epsilon_i.$$

ϵ_i の第1要素は GCD の係数 $c_{i,1}$ の摂動に対応する．$c_{i,1}$ を α 倍，すなわち c_i を α 倍すると，摂動の大きさも α 倍される．したがって，規格化によって許容度は次のように変化することがわかる．

命題 6
ベズー行列による規格化を適応すると，許容度が $O(\varepsilon)$ から $O(\alpha\varepsilon)$ に変化する． ∎

2.5 条件数の変化

条件数とは，数値的安定さを表す尺度として次のように定義される（大きいほど，不安定になる）．

$$\mathrm{cond}(M) = ||M|| \cdot ||M^{-1}||.$$

ここで $||M|| = \max_j \sum_{i=1}^{n} ||M_{i,j}||$ である．条件数に関して，次が成り立つ．

補題 7
正則な行列 M に対して

$$\mathrm{cond}(\alpha M) = \mathrm{cond}(M) \quad \textit{with } \alpha \in \mathbf{K}^*.$$

∎

補題 8
行列 M の部分行列 $M_{p,q}^{(i,j)}$ を

$$M_{p,q}^{(i,j)} = \begin{pmatrix} m_{p,q} & \cdots & m_{p,q+j-1} \\ \vdots & \ddots & \vdots \\ m_{p+i-1,q} & & m_{p+i-1,q+j-1} \end{pmatrix} \in \mathbb{K}^{i\times j},$$

行列 M の作用 $T_{i,\alpha}(M)$ を次で定義する.

$$T_{i,\alpha}(M) = \begin{pmatrix} \alpha M_{1,1}^{(i,i)} & M_{1,i+1}^{(i,n-i)} \\ M_{i+1,1}^{(n-i,i)} & \frac{1}{\alpha} M_{i+1,n}^{(n-i,n-i)} \end{pmatrix}$$

このとき,

$$\mathrm{cond}(M) \approx \mathrm{cond}(T_{i,\alpha})(M).$$

∎

行列の変換は条件数などの改善を行うものではなく，多項式としてみたときに微小主係数 GCD 問題，巨大主係数問題を避ける変換である.

3 計算量

共通因子を持つ多項式の規格化は次のステップで実行され，それぞれの計算量は次の通りである.

1. 入力多項式からベズー行列を生成し，$B_{k,\alpha}$ を生成
   多項式の積 $f(x)g(y)$ の計算に $(n+1)(n+1)$ 回の積，および n^2-1 回の和の計算
2. $P_{i,j}$ を構成
   $\frac{n(n+1)}{2}$ の和の計算
3. 各係数を求める
   $O(n)$ で計算可能である.

ゆえに，計算量は $O(n^2)$ であり，両端消去による互除法 [Sanuki11] より計算量は少ない.

4 規格化を含めて GCD 計算法

4.1 微小主係数 GCD 問題

有効浮動小数 [KS97] または 1 回の主係数消去によって，微小主係数の大きさ $|\delta| \ll 11$ はおおよそ見積もることができる (第 2 主係数に $O(1/\delta)$ の桁落ちが起きる). そのため，$\alpha = O(\delta)$ とし $B_{k,\alpha}$ という変換を行うことで微小主係数 GCD 問題を避けることができる.

4.2 巨大主係数問題

GCD を変化されない変換を利用する. 入力多項式の係数から判断することができる (滅多に発生する悪条件問題ではない).

4.3 GCD計算

規格化によって条件数はほぼ変化しないことは既に指摘済みであり，規格化によってGCDが変化することだけが保証される．このため，GCDを計算するためには一度規格化を行い，両条件化された問題を互除法などの高速算法で解き，最後得られたGCDを元に戻すという手順でGCDを計算する必要がある．

5 まとめ

本稿では，ベズー行列を用いた複数多項式に関する規格化について提案した．規格化そのものでGCDを変換することはできたが，条件数まで変化させる変換ではなかったため，ベズー行列をみたす多項式を求める必要がある．条件数を変化させることは今後の課題である．

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.

[BB07] 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.

[CWZ04] 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.

[CZG02] E.-W. Chionh, M. Zhang and R. N. Goldman. *Fast computation of the Bezout and Dixon resultant matrices.* J. Symb. Compu., **33**(2202), 13–20.

[DG02] 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.

[KS97] F. Kako and T. Sasaki. Proposal of "effective floating-point number" for approximate algebraic computation. *Preprint of Tsukuba Univ.*, 1997.

[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.

[Sanuki09] 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.

[Sanuki11] M. Sanuki. Challenge to fast and stable computation of approximate univariate GCD, based on displacement structures,. Proc. of SNC2011, 2011, 178-186.

[SS07] 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.