数理解析研究所講究録 第2104巻 2019年 1-7

桁落ち判定による（整数係数）1変数多項式の互いに素である判定法

Finding Out Whether Univariate Polynomials are Relatively Prime Through Cancellation Errors

讃岐 勝

Masaru Sanuki

筑波大学医学医療系臨床医学域*

Division of Clinical Medicine, Faculty of Medicine, University of Tsukuba

Abstract

多項式の組 $f(x), g(x) \in \mathbb{Z}[x]$ が互いに素であるか判定する.

Abstract

In this paper, we propose how to find out whether univariate polynoamils are relatively prime through cancellation errors.

1 はじめに

本稿では，与えられた1変数多項式の組 $f(x)$ と $g(x)$ が互いに素であるか否かについて述べる．本稿では係数が浮動小数の場合を扱うが，係数が整数の場合についても多くの文献が残っていないので少しだけ触れる．

互いに素でないときは多項式の組 $f(x)$ と $g(x)$ は自明でない共通因子を持ち，その中で次数が一番大きな共通因子は最大公約子 (greatest common divisor，GCD と表記する) と呼ばれる．特に，浮動小数係数の多項式の GCD は互いに素であるか否かを判定する方法として，すぐに思いつくのは GCD そのものを計算する直接法であり，ユークリッドの互除法に始まり古くから計算方法が知られている．高速算法も開発されており，互いに素であるか否かを判定するより直接計算した方がよいと思われる方もいるので，先に触れることにする．

そこで，次の2つのサブセクションでは整数係数と浮動小数係数の多項式の組について直接法による互いに素か否かの判定に必要な計算量ついて述べる．

以下，n を多項式 $f(x)$ と $g(x)$ の次数と最大値する．

*sanuki@md.tsukuba.ac.jp

1.1 整数係数の場合

互いに素であるかを判定するためユークリッドの互除法を用いた場合には最悪計算量を見積もればよく，その計算量は $O(n^2)$ であることが知られている．また，ユークリッドの互除法の高速算法である half-GCD 法の計算量は $O(n \cdot \log n)$ であることが知られている．そのため，互いに素であるか" だけ" を判定するための専用の算法を開発するとなると，計算量 $O(n \cdot \log n)$ 未満の算法を開発する必要があり，実用面から考えると計算量 $O(n)$ 程度の算法が要求されることになる．この計算量は係数を上から眺めていくのと同等の計算量であり，すぐに困難であることが予想される．

ただし，係数から互いに素か否かを判定する方法の研究は全くされていないわけではない．2 つの論文 [7, 5] では，素数 p からなる有体限 $\mathbb{Z}_p$ 上およびその拡大体 $\mathbb{Z}_q = \mathbb{Z}_{p^t}$ 上での多項式において互いに素になる確率を見積もっている：$n+1$ 個の数の集合 $\{d_n, \ldots, d_0\}$ を係数に持つ多項式が互いに素になる確率は

$$1 - \frac{1}{q} + \frac{q-1}{q^{2n}} \tag{1}$$

であり，拡大次数を上げていくと（徐々に整数に近づけると），ほとんどの場合で互いに素になるとの報告がある．

以上のことから，整数の場合においては直接計算するのが効率の面からも良いことがわかる．

1.2 本稿の話題：浮動小数係数

浮動小数を係数に持つ多項式に対しては half-GCD 法を適応させるのは非常に困難なため，計算量 $O(n \cdot \log n)$ で GCD を計算することは非常に難しく [12]，整数係数の場合とは状況が異なる．互いに素であるか否かについて，直接 GCD を計算することによって判定するのであれば Sylvester 行列，Bezout 行列ないし Bezout-Hankel 行列などの構造行列を利用するのがよく，その計算量は $O(n^2)$ である [4].

そこで，本稿では計算量 $O(n^2)$ 未満で互いに素であるか否かを判定できないか検討をおこなう．以下，係数は浮動小数として話をすすめる．

1.3 記号

本稿では次の記号を使用する．浮動小数の集合 $\mathbb{F}$ を係数とする 1 変数多項式全体を $\mathbb{F}[x]$ で表し，以下では浮動小数係数の多項式はすべて大文字で表記することにする．

多項式 $F(x)$ に対して，次数を $\deg(F)$ で表す．多項式 $F(x)$ と $G(x)$ の GCD を $\gcd(F, G)$ で表す．

$f(x), g(x) \in \mathbb{Z}[x]$ が整数係数の GCD $c(x)$ をもつとき，この多項式の係数を浮動小数に変換した多項式 F と G の厳密な GCD は 1 である．変換した途端にマシンイプシロン程度の誤差を持ってしまうからである．このため，以下ではすべて近似 GCD を考えることにする．また，多項式 F と G の摂動はマシンイプシロン程度とは限らない．意図的に誤差項を加えることも以下では許す．すなわち，多項式 F と G は次のように表記される．

$$F = f + \Delta_f = c\tilde{f} + \Delta_f, \quad G = g + \Delta_g = c\tilde{g} + \Delta_g.$$

ここで，$||\Delta_f|| \ll ||f||$，$||\Delta_g|| \ll ||g||$ であり $c(x)$ は式 F と G の近似 GCD と呼ぶ．

2　特異値の利用

行列 M の特異値分解とは次の分解である．

$$M = U^T D V = U^T \begin{pmatrix} \sigma_1 & & & \\ & \sigma_2 & & \\ & & \ddots & \\ & & & \sigma_n \end{pmatrix} V \tag{2}$$

ここで，U, V はユニタリ行列である（一意には決まらない）．また，σ_i は特異値と呼ばれ $\sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_n \geq 0$ をみたす．階数（ランク）が k のとき，

$$\sigma_1 \geq \sigma_2 \geq \sigma_k \geq 1 \gg \sigma_{k+1} \geq \cdots \geq \sigma_n \geq 0. \tag{3}$$

であり，$M + E$ がランク k であるための摂動 E の条件は

$$||E||_2 = \sigma_{k+1}$$

であることが知られている．GCD の最小許容度もこれに基づき計算される（3.2 を参照）．

3　微小主係数の共通因子の有無の判定と最小許容度

3.1　共通因子の有無の判定

まず，微小主係数の共通因子を持つか否かの判定法について述べる．ここで述べることは新しい事実でなく，[13] ですでに示していることの繰り返しである．

例 1 (微小主係数の共通因子をもつ多項式による主項消去)
多項式 $F(x)$ と $G(x)$ が微小主係数の共通因子を持つと仮定する．このとき，主項の消去を行うと，

$$\begin{aligned} F &= (a_2x^2 + a_1x + a_0)(\varepsilon x^2 + c_1x + c_0) \\ &= \varepsilon a_2x^4 + \underline{(\varepsilon a_1 + c_1a_2)x^3} + (\varepsilon a_0 + c_1a_1 + c_0a_2)x^2 + \cdots, \\ G &= (b_2x^2 + b_1x + b_0)(\varepsilon x^2 + c_1x + c_0) \\ &= \varepsilon b_2x^4 + \underline{(\varepsilon b_1 + c_1b_2)x^3} + (\varepsilon b_0 + c_1b_1 + c_0b_2)x^2 + \cdots. \end{aligned}$$

$$b_2F - a_2G = \underline{\varepsilon(a_1b_2 - a_2b_1)x^3} + \big[\varepsilon(a_0b_2 - b_0a_2) + c_1(a_1b_2 - b_1a_2)\big]x^2 + \cdots.$$

x^3 の係数（消去後の主係数）で桁落ち誤差が発生する．桁落ち誤差をきちんと観測するには $|\varepsilon| < 0.3$ 程度が必要である． ∎

共通因子を持つ場合にそれが微小主係数とは限らない．次の変換は共通因子を持つ場合にその共通因子の主係数を微小にする変換の一例である．

1. $f(x) \to (\delta x - 1)f(x)$ and $g(x) \to (\delta x - 1)g(x)$ with $|\delta| \ll 1$
2. $f(x) \to f(\delta x)$ and $g(x) \to g(\delta x)$ with $|\delta| \ll 1$
3. $f(x) \to x^n f(1/x)$ and $g(x) \to x^{n-1} g(1/x)$

4. 上記の組み合わせ

ただし，これらの変換によって例 1 で示すような桁落ち誤差が発生するとは限らない. また変換によって，全体の係数が小さくなる場合があり，そのとき上の例で示したような桁落ちは観測しづらい．そのため，主項消去を何度か行い主係数を眺める必要がある．

3.2 最小許容度に関して

最小許容度について，与多項式 F と G から構成される Sylvester 行列 $S(F,G)$ の特異値をよる評価が用いられ，$S(F,G) - S(f,g) = E$ を $||E||_2$ すなわち特異値によって評価される．この評価は次の評価によってもなされる．

$$\Delta_S = ||\tilde{g}F - \tilde{f}G||_2$$

これは Sylvester 行列の最小特異値にほぼ等しく，これによる評価が一般的である．

3.3 本稿で取りあげる問題（繰り返し）

上で述べたとおり，共通因子をもつか否かについては実はそれほど難しくない．問題は

- 互いに素なのか
- 互いに素であるための最小許容度は

を一緒に考えることである．

4 Bezout-Hankel 行列

多項式 $F(x)$ と $G(x)$ からなる Bezout-Hankel 行列 $H_n(F,G) = H_n$ は次で定義される行列である．

$$\mathrm{H}_n(F,G) = \mathrm{H}_n = \begin{pmatrix} h_1 & h_2 & \dots & h_n \\ h_2 & \dots & \dots & \dots \\ \vdots & \dots & \dots & \dots \\ h_n & h_{n+1} & \dots & h_{2n-1} \end{pmatrix} \in \mathbb{F}^{n\times n}. \tag{4}$$

ここで，各要素 h_i は G/F を無限遠点上で Taylor 展開したときの係数である：

$$G/F = h_1 x^{-1} + h_2 x^{-2} + \ldots = \sum_{i=1}^{\infty} h_i x^{-i}. \tag{5}$$

4.1 特異値による最小許容度の評価できるための条件

3.2 節では Sylvester 行列に関して述べた．本節では Bezout-Hankel 行列に関して考える．
最初に次の 2 つの関係について考える．

- H_n の最小特異値

- $\dfrac{G}{F}-\dfrac{\tilde{g}}{\tilde{f}}$ の多項式ノルム

これらはほぼ同様の値として見なすとができるように思えるが実はそうではない．[10] では正規化 $||F||, ||G|| \approx 1$ の必要性を指摘している．加えて，主係数の大きさ（微小主係数が否か）にも注意を払う必要がある．

$$\begin{aligned}\frac{G}{F}-\frac{\tilde{g}}{\tilde{f}} &= \frac{\tilde{g}F-\tilde{f}G}{\tilde{f}F}\\ &= \frac{\tilde{g}F-\tilde{f}G}{(\tilde{f}_k x^{n-k}+\cdots)(((f_n+{\Delta_f}^{(n)})x^n+\cdots))}\\ &= \frac{\tilde{g}F-\tilde{f}G}{\tilde{f}_k f_n(x^{2n-k}+P/(\tilde{f}_k f_n))}\\ &= \frac{\tilde{g}F-\tilde{f}G}{\tilde{f}_k f_n}(1-\Gamma+\Gamma^2-\cdots)\end{aligned}$$

ここで，$\Gamma = P/(\tilde{f}_k f_n))$ であり，級数 P は GCD とは無関係の多項式から構成されている．この式から，$||F||, ||G|| \approx 1$ に加えて

$$\tilde{f}_k f_n = 1 \tag{6}$$

と変換する必要があり，Sylvester 行列と同様に H_n の特異値で最小許容度を検討するのであれば微小主係数でないことが条件として必要となる．これらの条件のもとであれば

$$\Delta_S = \Delta_H \times \text{const.} \tag{7}$$

がいえる．そのため，以下ではこれらの条件を仮定する．

4.2 最小許容度の計算

本節では，互いに素になるか否かについて考える．$H_n+\Delta_H$ の摂動 Δ_H の大きさを考えれば良く，最小特異値 σ_n を考えれば良い．ただし，最小特異値の計算は難しいので逆行列の目的の特異値を計算する．

$$||H_n^{-1}||_2 = 1/\sigma_n. \tag{8}$$

まず，逆行列 H_n^{-1} を求める．Hankel 行列の逆行列の計算法はよく知られている [9, 8].
$H_n\boldsymbol{x}=\boldsymbol{e}_1$ and $H_n\boldsymbol{x}=\boldsymbol{e}_n$ の解を利用して，次でかける．

$$\begin{aligned}H_n^{-1} = \frac{1}{y_1}\times\Bigg\{&\begin{pmatrix} y_1 & & & \\ y_2 & y_1 & & \\ \cdots & \cdots & \cdots & \\ y_n & \cdots & \cdots & y_1\end{pmatrix}\begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ x_2 & \cdots & \cdots & \\ \cdots & \cdots & & \\ x_n & & & \end{pmatrix}\\ &-\begin{pmatrix} 0 & & & \\ x_1 & & & \\ \cdots & \cdots & \cdots & \\ x_{n-1} & x_{n-2} & \cdots & x_1\end{pmatrix}\begin{pmatrix} y_2 & y_3 & \cdots & y_n \\ y_3 & \cdots & \cdots & \\ \cdots & \cdots & & \\ 0 & & & \end{pmatrix}\Bigg\}.\end{aligned} \tag{9}$$

したがって，H_n^{-1} は計算でき，2 つの線形方程式を解くための計算量は $O(n \log n)$，Hankel 行列と行列の積の計算量はなので全体の計算量は $O(c_1 n^2)$ である．ただし，実際は下三角行列である Hankel 行列と上三角行列である Hankel 行列の積のため，実際の計算量は $O(n^2)$ 以下で押さえることができる．

いま求めたい値は $||H_n^{-1}||_2$ であり定義より，

$$||H_n^{-1}||_2 = \max_{\boldsymbol{x} \neq 0} \frac{||H_n^{-1}\boldsymbol{x}||_2}{||\boldsymbol{x}||_2} \tag{10}$$

であるが計算が大変なので，フロベニウスノルム $||*||_F$ で近似する．

$$||H_n||_F = \sqrt{\sum_{h \in H_n} |h|^2} = \sqrt{H_n H_n^*} = \sqrt{\sum_i \sigma_i^2}$$

このとき，

$$||H_n||_2 ||x|| < ||H_n||_F ||x|| \text{ for } x \in \mathbb{F}^n \ \{\mathbf{0}\}$$

の関係をみたす．フロベニウスノルムの場合，n 倍程度大きく見積もることになってしまうが，互いに素か否かを判定することを目的にしているので，σ_n が大きいか小さいかの判定ができればよく，$\sigma_n \ll 1$，すなわち，$||H_n^{-1}||_F \gg 1$ か否かだけわかれば良い．そのため，互いに素か否かの判定と，そのときの許容度について見積もることができる．

参　考　文　献

[1] A. V. Aho, J. E. Hopcroft and J. D. Ullman. *The design and analysis of computer algorithms.* Addison-Wesley, 1974.

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

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

[4] 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.

[5] Benjamin and Bennet, *The probability of relatively prime polynomials*, Mathematics Magagine, vol. 80, no. 3, 2007, 196–202.

[6] Beckermann and Labahn, *When are Two Numerical Polynomials Relatively Prime?*, J. of Symb. Comp., vol. 26, 6, 1998, 677–689.

[7] Corteel, Savage, Wilf and Zeilberger, *A pentagonal number sieve*, J. of Combinatorial Theory, Series A, 82(2), 1998, 186–192.

[8] J. Glasa, *On explicite formulae for Hankel matrix inversion*, WSEAS Trans. Math., **1**, 2002, 142–146.

[9] G. Heinig and K. Rost, *Algebraic method for Toeplitz-like matrices and operators*, Birkhäuser, 1984.

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

[11] Sederberg and Chang, *Best linear common divisors for approximate degree reduction*, Computer-Aided Design, Vol. 25(3), 1993, 163–168.

[12] M. Sanuki. *Challenge to fast and stable computation of approximate univariate GCD, based on displacement structures*, Proc. of SNC2011, ACM Press, 2011, 178–186.

[13] M. Sanuki and T. Sasaki, *Computing approximate GCDs in ill-conditioned cases*, Proc. of SNC 2007, 2007, 170–179.