数理解析研究所講究録
915巻 1995年 1-11

数値的に安定な一変数多項式剰余列の生成法

大迫 尚行* 鳥居 達生* 杉浦 洋* 櫻井 鉄也**
*名古屋大学工学部情報工学科 **筑波大学電子情報系

A Stably Generating Method for Complex Coefficient Polynomial Remainder Sequences

Naoyuki OHSAKO* Tatsuo TORII* Hiroshi SUGIURA*
Tetsuya SAKURAI**

*Department of Information Engineering, Faculty of Engineering
Nagoya University, Nagoya 464-01, Japan
**Institute of Information Sciences and Electronics
University of Tsukuba, Tsukuba, 305, Japan

Abstract

From the viewpoint of numerical stability, Euclidean algorithm has still a problem even when we generate the univariate polynomial remainder sequences. As we have to determine whether the remainder polynomial is zero or not to get the GCD (greatest common divisor) of two polynomials $f(z)$ and $g(z)$, it is difficult to distinguish the zero under the floating point arithmetic. In order to overcome this difficulty, we propose a stable algorithm to evaluate the subresultant by introducing pivoting in the process of elimination of leading coefficients of the polynomials. By our method, we can stably calculate a subsequence of polynomial remainder sequence.

1 はじめに

ユークリッド互除法は古くから広く知られている算法の1つで, 2つの多項式の最大公約因子を求める問題 [1] や関数の有理関数近似 [5] , あるいは代数方程式の解法 [6, 7, 12, 11] 等に用いられている. しかしながらユークリッド互除法には次の克服すべき問題点がある. 有理係数の多項式を対象にすると数式処理では計算の中間結果が莫大になる中間膨張と呼ばれる現象によって計算量が多くなる点にあり, 浮動小数点演算では桁溢れや丸め誤差の影響を受けやすい点にある.

我々は浮動小数点演算の立場から一変数多項式を対象に, 数値的不安定性を克服するために多項式剰余列の安定な算法を提案する.

まず最初に多項式に関する術語と記号を導入する.
一変数 z の複素係数多項式 $F(z)$ を

$$F(z) = f_m z^m + f_{m-1} z^{m-1} + \ldots + f_0$$

とする.

$\mathrm{lc}(F(z))$	z の最高巾係数 f_m を $F(z)$ の主係数 (leading coefficient) といい $\mathrm{lc}(F(z))$ で表す.
$\|\|F(z)\|\|$	$F(z)$ のノルムを表す. $F(z)$ の係数の絶対値の最大値で定義する.
$\deg(F(z))$	$\mathrm{lc}(F(z)) \neq 0$ のとき $F(z)$ は m 次式であるという. m を $F(z)$ の次数 (degree) といい $\deg(F(z))$ で表す. $\mathrm{lc}(F(z)) \neq 0$ であるか明記されてないとき $F(z)$ は高々 m 次であるという. $F(z)$ の係数が全て零であるとき, 即ち $F(z) \equiv 0$ のとき, $\deg(F(z)) = -\infty$ と定義する.
mod	2 つの多項式 $F(z)$, $G(z)$, に対して $F(z)$ を $G(z)$ で割った剰余多項式を $F(z) \bmod G(z)$ で表す.
$\sim$	2 つの多項式 $F(z)$, $G(z)$ が定数倍を除いて等しいとき, $F(z)$ と $G(z)$ は互いに相似であるといい $F(z) \sim G(z)$ で表す.
枢軸 (pivot)	同じ次数の多項式列において, 絶対値の一番大きい主係数を枢軸 (pivot) という. 枢軸を選ぶ操作を枢軸選び (pivoting) という.
$\mathrm{Elim}(G_0, G_1)$	2 つの同じ次数の多項式 G_0, G_1 に対して主係数が枢軸となる多項式で他方の多項式を割った剰余多項式を与える関数.
$\mathrm{Piv}\{G_i\}_{i=0}^{k}$	同じ次数の多項式列 $\{G_i\}_{i=0}^{k}$ に対して主係数が枢軸となる多項式と G_0 とを交換する操作.

定義 1.1 (多項式剰余列) 次のユークリッド互除法で与えられる多項式列 $P_0, P_1, \ldots, P_k(\neq 0)$ を多項式剰余列という [9].

[入力] 2 つの多項式 $F(z), G(z)$, $\deg(F(z)) \geq \deg(G(z))$.

[出力] 多項式剰余列, 及び $F(z)$ と $G(z)$ の最大公約因子.

[初期設定] $P_0 \leftarrow F(z)$, $P_1 \leftarrow G(z)$, $i \leftarrow 0$.

[反復計算] [1] $i \leftarrow i+1$,
$P_{i+1} \leftarrow P_{i-1} \bmod P_i$.

[2] $\deg(P_{i+1}) > 0$ ならば [1] へ.
$\deg(P_{i+1}) \leq 0$ ならば $k \leftarrow i+1$ として停止する.
$P_k \equiv 0$ ならば $k \leftarrow k-1$ とする. このとき P_k が $F(z)$ と $G(z)$ の最大公約因子である.

定義 1.2 (部分終結式) 2 つの多項式

$$\begin{aligned} F &= f_m z^m + f_{m-1} z^{m-1} + \ldots + f_0, \\ G &= g_n z^n + g_{n-1} z^{n-1} + \ldots + g_0, \\ &\quad \text{但し, } m \geq n. \end{aligned}$$

に対して F と G の部分終結式 $S_j(F,G)$ を次のように定義する [2, 3].

$$S_j(F,G) := \begin{vmatrix} f_m & f_{m-1} & \cdots & \cdots & \cdots & f_{2j+2-n} & Fz^{n-j-1} \\ & f_m & \cdots & \cdots & \cdots & f_{2j+3-n} & Fz^{n-j-2} \\ & & \ddots & & & \vdots & \vdots \\ 0 & & & f_m & \cdots & f_{j+1} & Fz^0 \\ g_n & g_{n-1} & \cdots & \cdots & \cdots & g_{2j+2-m} & Gz^{m-j-1} \\ & g_n & \cdots & \cdots & \cdots & g_{2j+3-m} & Gz^{m-j-2} \\ & & \ddots & & & \vdots & \vdots \\ 0 & & & g_n & \cdots & g_{j+1} & Gz^0 \end{vmatrix}, \quad 0 \le j \le n-1.$$

但し, $i < 0$ のときは $f_i = g_i = 0$ とする.

特に $j = 0$ のときは単に終結式という. $S_j(F,G)$ を定義する右辺は見かけ上 $m+n-j-1$ 次の多項式であるが, 実際は高々 j 次の多項式である.

- 部分終結式の代数的意味.

多項式の次数を 1 次下げるにはもう 1 つ同じ次数の多項式が必要である. 同じ次数の 2 つの多項式から主係数消去により 1 つ次数の低い多項式が 1 つ得られる. このことを踏まえて定義 1.2 の 2 つの多項式 F, G において $n = m-1$ とし, G の次数より 1 つ次数の低い多項式を求めてみる. それには G と同じ次数の多項式が 1 つ必要である. そのような多項式は F と zG とで主係数消去して得られる. さらにこの多項式と G とで主係数消去することにより求めるべき多項式が得られる. F, zG, G をそれぞれ G の次数より低次の項は括弧で括って次のように列記する.

$$\begin{aligned} F &= f_m z^m + f_{m-1} z^{m-1} + \{f_{m-2} z^{m-2} + \ldots + f_0\}, \\ zG &= g_{m-1} z^m + g_{m-2} z^{m-1} + \{g_{m-3} z^{m-2} + \ldots + g_0 z\}, \\ G &= g_{m-1} z^{m-1} + \{g_{m-2} z^{m-2} + \ldots + g_0\}. \end{aligned}$$

これを次のように行列表現する.

$$\begin{bmatrix} F \\ zG \\ G \end{bmatrix} = \begin{bmatrix} f_m & f_{m-1} & f_{m-2} z^{m-2} + \ldots + f_0 \\ g_{m-1} & g_{m-2} & g_{m-3} z^{m-2} + \ldots + g_0 z \\ 0 & g_{m-1} & g_{m-2} z^{m-2} + \ldots + g_0 \end{bmatrix} \begin{bmatrix} z^m \\ z^{m-1} \\ 1 \end{bmatrix}$$

右辺の係数行列の行列式において 1 列 $\times z^m$, 2 列 $\times z^{m-1}$ を 3 列に加えても行列式の値は変わらない. このときの行列式は $S_{m-2}(F,G)$ である.

一般に $S_j(F,G)$ は, F と G から G より $n-j$ 次低い多項式を得るのに要する多項式 Fz^{n-j-1}, Fz^{n-j-2}, ..., Fz, F, Gz^{m-j-1}, Gz^{m-j-2}, ..., Gz, G を j 次以下の項を括弧で括って上の要領で行列表現したときの係数行列の行列式である.

次に部分終結式と多項式剰余列との関係を表す定理を挙げる.

定理 1.1 (多項式剰余列と部分終結式に関する定理) 多項式 $F(z)$ と $G(z)$ から生成される多項式剰余列を $P_0, P_1, \ldots, P_k (\neq 0)$ とし $n_i := \deg(P_i)$ $(0 \le i \le k)$ とする. このとき

$$S_j(F,G) = 0, \quad 0 \le j < n_k. \tag{1.1}$$

さらに各 $i=2,3,\ldots,k$ について

$$\begin{aligned} S_{n_i}(F,G) &\sim P_i, && (1.2)\\ S_j(F,G) &= 0,\ \ n_i<j<n_{i-1}-1, && (1.3)\\ S_{n_{i-1}-1}(F,G) &\sim P_i. && (1.4)\end{aligned}$$

が成り立つ [2, 3].

定理 1.1 の多項式剰余列 $P_0,P_1,\ldots,P_k$ において P_0,P_1 以外の多項式の次数が 1 次ずつ減少するとき, 即ち

$$n_{i-1}-n_i=1,\ \ i=2,3,\ldots,k$$

のとき多項式剰余列は正規 (Normal) であるといい, そうでないとき不正規 (Abnormal) であるという. 多項式剰余列が正規であるとき (1.3) はない. またこのとき (1.2) と (1.4) は同一である. 部分終結式は次の定理より有理関数近似に応用される.

定理 1.2 2 つの多項式

$$\begin{aligned} F &= f_mz^m+f_{m-1}z^{m-1}+\ldots+f_0,\\ G &= g_nz^n+g_{n-1}z^{n-1}+\ldots+g_0,\\ &\quad \text{但し,}\ \ m\geq n.\end{aligned}$$

の各部分終結式 $S_j(F,G)$ は 2 つの多項式 A,B で一意に表現される [2].

$$\begin{aligned} S_j(F,G) &= AF+BG && (1.5)\\ \text{但し, } \deg(S_j(F,G)) &\leq \deg(G)-\deg(A_j)-1. && (1.6)\end{aligned}$$

ここで A, B はそれぞれ

$$A = \begin{vmatrix} f_m & f_{m-1} & \cdots & \cdots & \cdots & f_{2j+2-n} & z^{n-j-1}\\ & f_m & \cdots & \cdots & \cdots & f_{2j+3-n} & z^{n-j-2}\\ & & \ddots & & & \vdots & \vdots\\ 0 & & & f_m & \cdots & f_{j+1} & z^0\\ g_n & g_{n-1} & \cdots & \cdots & \cdots & g_{2j+2-m} & 0\\ & g_n & \cdots & \cdots & \cdots & g_{2j+3-m} & 0\\ & & \ddots & & & \vdots & \vdots\\ 0 & & & g_n & \cdots & g_{j+1} & 0 \end{vmatrix}, \qquad (1.7)$$

$$B = \begin{vmatrix} f_m & f_{m-1} & \cdots & \cdots & \cdots & f_{2j+2-n} & 0\\ & f_m & \cdots & \cdots & \cdots & f_{2j+3-n} & 0\\ & & \ddots & & & \vdots & \vdots\\ 0 & & & f_m & \cdots & f_{j+1} & 0\\ g_n & g_{n-1} & \cdots & \cdots & \cdots & g_{2j+2-m} & z^{m-j-1}\\ & g_n & \cdots & \cdots & \cdots & g_{2j+3-m} & z^{m-j-2}\\ & & \ddots & & & \vdots & \vdots\\ 0 & & & g_n & \cdots & g_{j+1} & z^0 \end{vmatrix}. \qquad (1.8)$$

である.

補助定理 1.1 多項式 F と G より生成される多項式剰余列の隣合う 2 つの要素を P_{j-1}, P_j とすると P_{j-1} と P_j より生成される多項式剰余列は F と G より生成される多項式剰余列の部分列である.

[証明] 多項式剰余列の定義より明らかである. ■

補助定理 1.2 2 つの多項式 F, G ($\deg(F) \geq \deg(G)$) と定数倍の違いを除いて等しい多項式をそれぞれ $\hat{F}$, $\hat{G}$ とすれば各部分終結式 $S_j(F,G)$ もまた $S_j(\hat{F},\hat{G})$ と定数倍の違いを除いて等しい.

[証明] $\hat{F} = \alpha F$, $\hat{G} = \beta G$ とすると, $S_j(\hat{F},\hat{G}) = S_j(\alpha F, \beta G)$ である. $S_j(\alpha F, \beta G)$ の各行を α あるいは β で括れば行列式の多重線形性より $S_j(\hat{F},\hat{G}) \sim S_j(F,G)$ がいえる. ■

補助定理 1.3 2 つの同じ次数の多項式 S_0, T とで主係数消去した多項式を S_1 とすると

$$S_0 \bmod S_1 \sim T \bmod S_1$$

が成り立つ.

[証明] S_0 と T とで主係数消去して得られる S_1 は 2 つの定数 α と β とで次のように書ける.

$$S_1 = \alpha S_0 + \beta T \tag{1.9}$$

(1.9) の両辺を S_1 で割ると

$$0 = \alpha S_0 \bmod S_1 + \beta T \bmod S_1$$

である. ゆえに

$$S_0 \bmod S_1 \sim T \bmod S_1 \ ■$$

系 1.1 補助定理 1.3 の条件の下で, S_0 と S_1 で生成される多項式剰余列の各要素は T と S_1 とで生成される多項式剰余列の各要素と定数倍の違いを除いて等しい.

2 ユークリッド互除法の数値的不安定性

2 つの多項式から多項式剰余列を生成するユークリッド互除法において多項式除算は主係数消去過程より構成される. ここでは剰余多項式を部分終結式を用いて導出し, 主係数消去の過程をみる.

多項式 F, G ($\deg(F) = m$, $\deg(G) = n$) の剰余多項式 $F \bmod G$ は定理 2.1 より $S_{n-1}(F,G)$ と相似である. 従って定数倍の違いを除けば多項式剰余列は部分終結式を用いて定義できる.

さて 2 つの多項式を F, G, $\deg(F) = m$, $\deg(G) = m-1$ として 多項式剰余列の要素 $P_2 (= F \bmod G)$ を $S_{m-2}(F,G)$ の行列を三角化して求めてみる. ここで主係数消去の際の枢軸を形式的に G の主係数とすると, 三角化の過程は次の通りである.

$$\begin{bmatrix} f_m & f_{m-1} & F \\ g_{m-1} & g_{m-2} & zG \\ 0 & g_{m-1} & G \end{bmatrix} \xrightarrow{(1)} \begin{bmatrix} g_{m-1} & g_{m-2} & zG \\ f_m & f_{m-1} & F \\ 0 & g_{m-1} & G \end{bmatrix} \xrightarrow{(2)} \begin{bmatrix} g_{m-1} & g_{m-2} & zG \\ 0 & f_{m-1}^{(1)} & F \bmod zG \\ 0 & g_{m-1} & G \end{bmatrix}$$

$$\xrightarrow{(3)} \begin{bmatrix} g_{m-1} & g_{m-2} & zG \\ 0 & g_{m-1} & G \\ 0 & f_{m-1}^{(1)} & F \bmod zG \end{bmatrix} \xrightarrow{(4)} \begin{bmatrix} g_{m-1} & g_{m-2} & zG \\ 0 & g_{m-1} & G \\ 0 & 0 & (F \bmod zG) \bmod G \end{bmatrix}$$

(1): 1行と2行を交換.
(2): 1行×$(-f_m/g_{m-1})$ を2行に加える.
(3): 2行と3行を交換.
(4): 2行×$(-f_{m-1}^{(1)}/g_{m-1})$ を3行に加える.

ここで三角化後の最下位の対角成分は $(F \bmod zG) \bmod G = F \bmod G$ である.

つまり F を G で割った剰余多項式 $F \bmod G$ は $S_{m-2}(F,G)$ の行列を形式的に G の主係数を常に枢軸として三角化したときの最下位の対角成分と一致する. G の主係数が相対的に非常に小さいときには, 精度低下や桁溢れが起こり得る. 定数倍の違いを除けば $S_{m-2}(F,G)$ は三角化のしかたによらず剰余多項式と等しいので主係数消去において形式的に常に G を枢軸にするよりも絶対値の大きい方の主係数を枢軸にする方が, 数値的に安定である.

今度は G の主係数 g_{m-1} を ϵ $(0 < \epsilon \ll 1)$ で置き代えて 多項式剰余列の要素 P_2, P_3 とそれぞれ相似である部分終結式を枢軸選び付きで三角化して求めてみる.

- $S_{m-2}(F,G)$ $(\sim P_2)$ の三角化

$$\begin{bmatrix} f_m & f_{m-1} & F \\ \epsilon & g_{m-2} & zG \\ 0 & \epsilon & G \end{bmatrix} \xrightarrow{(1)} \begin{bmatrix} f_m & f_{m-1} & F \\ 0 & g_{m-1}^{(1)} & G^{(1)} \\ 0 & \epsilon & G \end{bmatrix} \xrightarrow{(2)} \begin{bmatrix} f_m & f_{m-1} & F \\ 0 & g_{m-1}^{(1)} & G^{(1)} \\ 0 & 0 & G^{(2)} \end{bmatrix}$$

(1): 1行×$(-\epsilon/f_m)$ を2行に加える.
(2): 2行×$(-\epsilon/g_{m-1}^{(1)})$ を3行に加える.

ここで

$$G^{(1)} := zG - \frac{\epsilon}{f_m}F \tag{2.1}$$

$$G^{(2)} := G - \frac{\epsilon}{\mathrm{lc}(G^{(1)})}G^{(1)} \tag{2.2}$$

である. (2.2) より $G \approx G^{(2)}$ であるから次の多項式剰余列の要素を求めるのに $S_{m-3}(G, G^{(2)})$ $(\sim P_3)$ を三角化すると多項式の係数全体が桁落ちする. ここで補助定理 1.3 の結果を使うと (2.2) 式より $S_{m-3}(G, G^{(2)}) \sim S_{m-3}(G^{(1)}, G^{(2)})$ であるから $S_{m-3}(G^{(1)}, G^{(2)})$ を三角化することで上のような桁落ちが避けられる.

主係数消去過程の枢軸ができるだけ大きくなるようにして枢軸選びを徹底させたものが次の我々の提案する数値的に安定な多項式剰余列の生成法である.

3 数値的に安定な多項式剰余列の生成法

次に述べる多項式剰余列の生成法は基本的には部分終結式の反復計算であるから先の定理 2.1 よりユークリッド互除法によって生成される多項式剰余列のある要素と定数倍を除いて等しい. この算法の特徴は多項式剰余列のうちで比較的数値的に安定に求まる多項式を選択的に計算するところにある. 本算法を部分終結式を用いて説明する.

さて本算法は 2 つの多項式

$$\begin{aligned} F &= f_m z^m + f_{m-1} z^{m-1} + \ldots + f_0, \\ G &= g_n z^n + g_{n-1} z^{n-1} + \ldots + g_0. \\ & \quad \text{但し, } m \geq n. \end{aligned}$$

に対して, 次の 2 通りに分類して計算を行なう.

場合 1　$m = n$ 又は $|\mathrm{lc}(G)| \geq |\mathrm{lc}(F)|$
$\Longrightarrow S_{n-1}(F, G)$ $(\sim F \bmod G)$ を計算.

場合 2　$m > n$ 且つ $|\mathrm{lc}(G)| < |\mathrm{lc}(F)|$
$\Longrightarrow$ 多項式剰余列のうちのある 2 つの隣合う要素と相似な部分終結式を計算.

場合 1 での計算は次の通りである.

[1] $i = m-n, m-n-1, \ldots, 1$ について,
$\cdot F \leftarrow \mathrm{Elim}(F, z^i G)$.

[2] $\cdot \mathrm{Piv}(F, G)$,
$\cdot G \leftarrow \mathrm{Elim}(F, G)$.
G が多項式剰余列の要素である.

[3] $\deg(G) > 0$ ならば次の多項式剰余列の要素を計算する.
$\deg(G) \leq 0$ ならば 停止する.
このとき $G \equiv 0$ ならば F が最大公約因子である.

場合 1 での計算は部分終結式 $S_{n-1}(F, G)$ の行列成分を枢軸選び付きで三角化していることに対応している. なお $m = n$ のとき [1] の計算はない. 次に 場合 2 での計算を部分終結式を用いて説明する. 場合 2 での計算は 場合 1 での計算に比べて複雑である.

• 場合 2 での計算.

[1] $i = m-n, m-n+1, \ldots, m-2$ について,
$G^{(i)} := z^i G \bmod F$ を $|\mathrm{lc}(G^{(i)})| \geq |\mathrm{lc}(F)|$ を満足するまで計算し, 満足しなければ $G^{(m-2)}$ まで $n-1$ 回多項式除算を行なう.
ここで $G^{(i)} = z^i G \bmod F$ は

$$\begin{aligned} G^{(i)} &= z^i G \bmod F \\ &= \{z(z^{i-1} G \bmod F)\} \bmod F \\ &= z G^{(i-1)} \bmod F. \end{aligned}$$

より順次計算される. $G^{(m-n+l-l)}$ まで多項式除算を l 回計算したとき, 対応する 2 つの部分終結式は $S_{n-l}(F, G)$ と $S_{n-l-1}(F, G)$ である. 各多項式 $G^{(i)}$ の係数を

$$G^{(i)} = \sum_{j=0}^{m-1} g_j^{(i)} z^j, \ (i = m-n, m-n+1, \ldots, m-n+l-1)$$

とすると

$$S_{n-l-1}(F,G)$$

$$\sim \begin{vmatrix} f_m & f_{m-1} & \cdots & \cdots & \cdots & \cdots & F \\ g_{m-1}^{(m-n+l-1)} & g_{m-2}^{(m-n+l-1)} & \cdots & \cdots & \cdots & \cdots & zG^{(m-n+l-1)} \\ & g_{m-1}^{(m-n+l-1)} & \cdots & \cdots & \cdots & \cdots & G^{(m-n+l-1)} \\ & g_{m-1}^{(m-n+l-2)} & \cdots & \cdots & \cdots & \cdots & G^{(m-n+l-2)} \\ & \vdots & & & & & \vdots \\ & g_{m-1}^{(m-n)} & \cdots & \cdots & \cdots & \cdots & G^{(m-n)} \\ & g_n & \cdots & \cdots & \cdots & \cdots & z^{m-n-1}G \\ & & g_n & \cdots & \cdots & \cdots & z^{m-n-2}G \\ & & & \ddots & & & \vdots \\ \mathbf{0} & & & & g_n & \cdots & G \end{vmatrix} \tag{3.1}$$

又 (3.1) 式の行列成分の 1 列目と後ろから 2 列目及び 1 行目と 2 行目を除いて得られる小行列式は部分終結式 $S_{n-l}(F,G)$ と相似である.

[2] (3.1) 式の 3 行目以下を枢軸選び付きで三角化する.

(3.1) 式

$$\sim \begin{vmatrix} f_m & f_{m-1} & \cdots & \cdots & \cdots & F \\ g_{m-1}^{(m-n+l-1)} & g_{m-2}^{(m-n+l-1)} & \cdots & \cdots & \cdots & zG^{(m-n+l-1)} \\ & \hat{g}_{m-1}^{(m-n+l-1)} & \cdots & \cdots & \cdots & \hat{G}^{(m-n+l-1)} \\ & & \ddots & & & \vdots \\ & & & \hat{g}_{n-l+1}^{(1)} & \hat{g}_{n-l}^{(1)} & \hat{G}^{(1)} \\ \mathbf{0} & & & & \hat{g}_{n-l}^{(0)} & \hat{G}^{(0)} \end{vmatrix} \tag{3.2}$$

(3.2) 式の 3 行目以下の対角成分には主係数消去の際の枢軸が並ぶ. 又

$$\hat{G}^{(0)} \sim S_{n-l}(F,G)$$

である.

[3] (3.2) を上から順に主係数消去する.

$$(3.2)\text{ 式} \sim \begin{vmatrix} g_{m-1}^{(m-n+l)} & \cdots & \cdots & \cdots & G^{(m-n+l)} \\ \hat{g}_{m-1}^{(m-n+l-1)} & \cdots & \cdots & \cdots & \hat{G}^{(m-n+l-1)} \\ & \ddots & & & \vdots \\ & & \hat{g}_{n-l+1}^{(1)} & \hat{g}_{n-l}^{(1)} & \hat{G}^{(1)} \\ \mathbf{0} & & & \hat{g}_{n-l}^{(0)} & \hat{G}^{(0)} \end{vmatrix} \tag{3.3}$$

$$\sim \begin{vmatrix} \hat{g}_{m-1}^{(m-n+l)} & \hat{g}_{m-2}^{(m-n+1)} & \cdots & \cdots & \hat{G}^{(m-n+l)} \\ & \hat{g}_{m-2}^{(m-n+l-1)} & \cdots & \cdots & \hat{G}^{(m-n+l-1)} \\ & & \ddots & & \vdots \\ & & & \hat{g}_{n-l}^{(1)} & \hat{G}^{(1)} \\ \mathbf{0} & & & \hat{g}_{n-l}^{(0)} & \hat{G}^{(0)} \end{vmatrix} \tag{3.4}$$

$$\sim \begin{vmatrix} \hat{g}_{m-l}^{(1)} & \hat{G}^{(1)} \\ \hat{g}_{m-l}^{(0)} & \hat{G}^{(0)} \end{vmatrix} \sim \hat{G}$$

$\hat{G}^{(0)}$, $\hat{G}$ が求めるべき多項式である. それぞれ隣合う 2 つの多項式剰余列の要素と相似である.

[4] $\hat{G}^{(1)}$, $\hat{G}^{(0)}$ のうち主係数が枢軸となる多項式と $\hat{G}$ とで次の隣合う多項式剰余列の要素を求める.

• 零判定

多項式 F と G の部分終結式を計算する際の多項式及び主係数の零判定を次のように行なう. ここでは倍精度計算での零判定を与える.

零判定するのに必要な 定数 ϵ, γ を

$$\epsilon := 10^{-12},\ \gamma := \max\left(||F||, ||G||\right)$$

とする. 2 つの同じ次数の多項式 P, Q より主係数消去して得られた多項式を R とし, 主係数消去の際の枢軸を $\mathrm{lc}(P)$ とすると

$$R = Q - \frac{\mathrm{lc}(Q)}{\mathrm{lc}(P)} P$$

である. $R, \mathrm{lc}(R)$ が次の零判定を満たすとき それぞれを零とみなす.

- 多項式 R の零判定

$$\frac{|\mathrm{lc}(P)|}{\gamma} \times \frac{||R||}{\gamma} \leq \epsilon$$

- 多項式 R の主係数 $\mathrm{lc}(R)$ の零判定

$$\frac{|\mathrm{lc}(P)|}{\gamma} \times \frac{|\mathrm{lc}(R)|}{\gamma} \leq \epsilon$$

• 数値例

次の不正規に近い多項式剰余列を生成する 2 つの多項式 F と G について ユークリッド互除法と比較した結果を挙げる. 倍精度計算し下線部は 4 倍精度計算した値と異なる部分である.

$$\begin{aligned} F(z) &= z^6 + \frac{11}{12}(1+\delta)z^5 + \frac{10}{11}z^4 + \frac{9}{10}z^3 + \frac{8}{9}z^2 + \frac{7}{8}z + \frac{6}{7}, \\ G(z) &= z^5 + \frac{11}{12}z^4 + \frac{10}{11}(1+\delta)z^3 + \frac{5}{6}z^2 + \frac{4}{5}z + \frac{3}{4}, \\ \delta &= 10^{-7}. \end{aligned}$$

Table 3.1: Comparison of Euclidean algorithm and Our method.

	ユークリッド互除法	本算法
P_2	$-1.749368687316\underline{8} \times 10^{-7}z^4$ $+6.6666583333325 \times 10^{-2}z^3$ $+8.888881250000\underline{0} \times 10^{-2}z^2$ $+0.12499992666667z$ $+0.85714278839286$	$1.749368687316\underline{8} \times 10^{-7}z^4$ $-6.6666583333325 \times 10^{-2}z^3$ $-8.888881250000\underline{0} \times 10^{-2}z^2$ $-0.12499992666667z$ -0.85714278839286
P_3	$145229975132.5\underline{2}z^3$ $+193640079534.01z^2$ $+272310331004.51z$ $+1867238188723.8$	
P_4	$4.9096560150730 \times 10^{-12}z^2$ $-3.1795399646484 \times 10^{-12}z$ $-2.7660096435511 \times 10^{-12}$	
P_5	$540442552695.10z$ $+2029318777042.0$	$-0.23056649210443z$ -0.86574944736120
P_6	$7.8396248252327 \times 10^{-11}$	-0.86223029085074

	ユークリッド互除法	本算法
$P_5/\|\|P_5\|\|$	$0.26631722862332z + 1$	$-0.26632011467891z - 1$

4 おわりに

不正規もしくは不正規に近い多項式剰余列に対して比較的安定に求まる要素及び多項式の最大公約因子を選択的に計算する算法を設計した. 多項式剰余列の各要素を部分終結式の行列成分を枢軸選び付きで三角化して計算することでユークリッド互除法で起こる数値的不安定性を克服した. 尚本方法は関数の有理関数近似や代数方程式の解法に応用されるのでこれを今度の課題としたい.

参考文献

[1] Akritas, A.G., A New Method for Computing Polynomial Greatest Common Divisors and Polynomial Remainder Sequences, *Mumer. Math.* 52. 119-127 (1988).

[2] Brown, W.S.,Traub, J.F., On Euclid's Algorithm and the Theory of Subresultants, J.ACM, 18(1971), 505-514.

[3] Collins, G.E., Subresultants and Reduced Polynomial Remainder Sequences, *Journal of the ACM*, Vol.14, No.1, (Jan. 1967), 128-142.

[4] Cuyt, A., Wuytack, L., Nonlinear Methods in Numerical Analysis, Amsterdam, North-Holland 1989.

[5] 宮広栄一, 野田松太郎., 新しい有理関数近似によるハイブリッド積分の拡張について, 日本応用数理学会論文誌, Vol.2, No.4, (1992), pp.193-206

[6] Sakurai, T.,Torii, T.and Sugiura, H., An Iterative Method for Algebraic Equation by Padè Approximation, Computing 46 (1991) 131-141.

[7] Sakurai, T.,Sugiura, H.and Torii, T., Numerical factorization of a polynomial by rational Hermite interpolation, Numerical Algorithms 3 (1992) 411-418.

[8] Sasaki, T.and Sasaki, M., Analysis of Accuracy Decreasing in Polynomial Remainder Sequence with Floating-point Number Coefficients, *J. Inf. Process*, Vol.12, No.4, (1989), 384-403.

[9] 佐々木建昭, 計算代数, 岩波講座応用数学, 岩波書店 1993.

[10] 佐々木建昭, 数式処理, 情報処理叢書 7, 情報処理学会, 1981.

[11] 園田信吾, 櫻井鉄也, 杉浦洋, 鳥居達生., 分割統治法による多項式の数値的因数分解, 日本応用数理学会論文誌, Vol.1, No.4, (1991), pp.277-290

[12] Torii, T.and Sakurai, T.and Sugiura, H., An application of Sunzi's theorem for solving algebraic equations, *Proceedings of the First China-Japan Seminar on Numerical Mathematics, Beijing* (1992) (1993) 155-167.