数理解析研究所講究録
第1927巻 2014年 106-114

複数個の1変数多項式に対する部分終結式行列の構成に向けて

Towards reduced construction of subresultant matrix of multiple univariate polynomials

照井 章*
Akira Terui
筑波大学 数理物質系
Faculty of Pure and Applied Sciences, University of Tsukuba

Abstract

我々は，3個以上の実係数1変数多項式に対し，それらの最大公約子 (GCD) の次数を見積もることができるような行列（部分終結式行列，もしくはそれらに類似する行列）の新たな構成法を示唆する．この構成法は，筆者が知る限り，これまでに提案された同種の行列の構成法と比較して，次元がより小さく抑えられ，行列の rank をはじめとする計算の効率の向上が期待される．本稿では，ある計算例に対し，新たな構成法によって構成される行列の rank から入力多項式の GCD の次数を見積もる計算例を示す．

Abstract

For more than three real univariate polynomials as an input, we suggest a new construction of subresultant-like matrix which enable us to estimate the degree of the greatest common divisor (GCD) of the input polynomials from its rank. To the best of the author's knowledge, the dimension of the matrix with our definition is smaller than those with previously known definitions, thus we expect more efficient computation from subresultant-like matrices, such as matrix rank, by our definition. We demonstrate estimating the degree of the GCD from the rank of the matrix by our definition with an example.

1 はじめに

本稿では，3個以上の1変数多項式に対し，それらの最大公約子 (Greatest Common Divisor; GCD) の次数を見積もることができるような行列（部分終結式行列，もしくはそれらに類似する行列）の構成について論ずる．

f, g をともに実係数1変数多項式とする．f と g に対し，それらの係数を成分にもつ Sylvester 行列を構成するとき，その行列式を f と g の終結式 [6] といい，ここに $R(f,g)$ で表す．f と g が共通零点をもつための必要十分条件として $R(f,g)=0$ が知られている．なお，f と g が共通零点をもつことは，f と g が自明でない GCD をもつことと同値であることに注意する．

また，f と g で生成される多項式剰余列 (Polynomial Remainder Sequence; PRS) に対し，Sylvester 行列の小行列式により，PRS の各要素の係数を表すことが可能である．このような行列は "部分終結式行列"

*terui@math.tsukuba.ac.jp

とも呼ばれている．部分終結式の理論により，f と g の Sylvester 行列や部分終結式行列の rank から，f と g の GCD の次数を見積もることが可能である [1].

入力多項式の個数が 3 個以上の場合，部分終結式行列として，いくつかの行列の構成法 ([2], [3]) が知られているが，それらの構造はより複雑さを増し，次元もより大きくなる．よって，このような場合に，部分終結式行列，もしくはそれに類似する行列で，次元がより小さな行列を用いることができれば，入力多項式の GCD の次数を見積もるための rank の計算もより効率的に行えるようになることが期待される．

本稿では，3 個以上の入力多項式のある例題に対し，筆者が知る範囲において，部分終結式行列と同等な行列として，既知のものよりも次元がより小さな行列で，GCD の次数の見積もりが可能な行列を構成し，実際にその行列の rank を求めることにより，GCD の次数を見積もる．

以下では次の事項について述べる．第 2 章では，2 個の入力多項式に対し，部分終結式行列を用いた GCD の次数の見積もりを復習する．第 3 章では，3 個以上の入力多項式に対する既知の部分終結式行列の表現を紹介し，計算効率の観点から課題を示す．第 4 章では，ある例題に対し，部分終結式行列に類似の行列として，次元がより小さな行列を構成し，その行列の rank から入力多項式の GCD の次数の見積もりが可能であることを示す．

2 部分終結式行列と 1 変数多項式の GCD の見積もり

以下では，1 変数多項式 f, g に対し，f の次数を $\deg(f)$ で表し，$\deg(f) \geq \deg(g)$ のとき，f を g で割った剰余を $\mathrm{rem}(f, g)$ で表す．また，1 変数多項式 $f, g, \ldots, h$ に対し，それらの GCD を $\gcd(f, g, \ldots, h)$ で表す．

1 変数多項式 $P(x) = p_n x^n + \cdots + p_0 x^0$ に対し，$C_k(P)$ を次式で定義される $(n+k, k+1)$ 行列（“たたみこみ” 行列）とする．

$$C_k(P) = \begin{pmatrix} p_n & & \\ \vdots & \ddots & \\ p_0 & & p_n \\ & \ddots & \vdots \\ & & p_0 \end{pmatrix}.$$

その上で，多項式

$$P_1(x) = p_{d_1}^{(1)} x^{d_1} + \cdots p_1^{(1)} x + p_0^{(1)}, \quad P_2(x) = p_{d_1}^{(2)} x^{d_2} + \cdots p_1^{(2)} x + p_0^{(2)} \tag{1}$$

$(d_1 \geq d_2)$ に対し，k 次 $(0 \leq k < d_2)$ の部分終結式行列 (subresultant matrix) を次式で定義する．

$$N_k(P_1, P_2) = \begin{pmatrix} p_{d_1}^{(1)} & & & p_{d_1}^{(2)} & & \\ \vdots & \ddots & & \vdots & \ddots & \\ p_0^{(1)} & & p_{d_1}^{(1)} & p_0^{(2)} & & p_{d_1}^{(2)} \\ & \ddots & \vdots & & \ddots & \vdots \\ & & p_0^{(1)} & & & p_0^{(2)} \end{pmatrix}. \tag{2}$$

$d_2 - k$ 列 $\quad$ $d_1 - k$ 列

$k = 0$ のとき，$\det(N_0(P_1, P_2)$ は古典的な終結式 (resultant) [6] に等しい．

P_1 と P_2 によって定まる k 次の部分終結式行列の特異性は，P_1 と P_2 の GCD およびその次数と関連があることが知られている [1].

命題 1
P_1, P_2 を式 (1) で与えられたものとする．$N_k(P_1, P_2)$ が正則ならば，またその時に限り，$\deg(\gcd(P_1, P_2)) \leq k$ が成り立つ．∎

部分終結式の理論より，$N_k(P_1, P_2)$ が，$k \geq d$ のときに非特異かつ $k = 0, 1, \ldots, d-1$ のときに特異ならば $\deg(\gcd(P_1, P_2)) = d$ であることがわかる．このとき，$N_0(P_1, P_2)$ の rank が full-rank から d だけ減少する．よって，$N_0(P_1, P_2)$ の rank を調べることにより，$\deg(\gcd(P_1, P_2))$ を見積もることができる．

$N_0(P_1, P_2)$ の rank と $\deg(\gcd(P_1, P_2))$ の関係は，近似 GCD の算法においても，たとえば筆者が提案する算法 ([4], [5]) の中では，制約つき最適化の制約条件を導くのに用いられている．

3　3個以上の入力多項式に対する部分終結式行列とその課題

入力多項式の個数が 3 個以上の場合に，Rupprecht [2] は，部分終結式行列の一つとして，以下の形の行列を提案している．

$$N_k(P_1, \ldots, P_n) = \begin{pmatrix} C_{d_1-1-k}(P_2) & C_{d_2-1-k}(P_1) & \mathbf{0} & \cdots & \mathbf{0} \\ C_{d_1-1-k}(P_3) & \mathbf{0} & C_{d_3-1-k}(P_1) & \cdots & \mathbf{0} \\ \vdots & \vdots & & \ddots & \vdots \\ C_{d_1-1-k}(P_n) & \mathbf{0} & \cdots & \mathbf{0} & C_{d_n-1-k}(P_1) \end{pmatrix}. \tag{3}$$

この形の部分終結式行列は，筆者も 3 個以上の入力多項式に対する近似 GCD 算法 ([4], [5]) で用いており，効果を挙げている．

しかしながら，式 (3) による部分終結式行列は，入力多項式の個数に比例して次元が大きくなる（行数: $r_k = d_1 + d_2 + \cdots + d_n - (n-1)k + (n-2)d_1$, 列数: $c_k = d_1 + d_2 + \cdots + d_n - n \cdot k$）．筆者の近似 GCD 算法では，反復計算に用いる連立 1 次方程式の係数行列に，式 (3) と同様の形の行列がブロックとして埋め込まれており，部分終結式行列の次元は算法の効率にも影響する．よって，3 個以上の入力多項式に対しては，より小さな次元をもち，それらの rank から入力多項式の GCD の次数を見積もることが可能な（部分終結式行列に類似する）行列を用いることが望ましい．

3 個以上の入力多項式に対する部分終結式行列の構成法では，上記の Rupprecht の方法の他に，筆者が知る限り，佐々木・古川による多重多項式剰余列と，それらに対する部分終結式の理論がある [3]．この理論は，入力多項式の組 $(P_1, \ldots, P_n)$ に対し，ある P_i で残りの P_j $(j \neq i)$ を割った剰余を求める計算の繰り返しによって生成される多項式の組（多重多項式剰余列）について，各多項式の係数を，入力多項式の係数を成分とする行列式で表現するための行列式の具体的な構成法を与えている点で興味深い．しかしながら，本論においては，PRS の各係数の具体的な表現よりもむしろ，入力多項式の GCD の見積もりの方により興味があり，かつ，そのような情報を，より簡潔な行列表現で得たいという要望がある．

そこで，次章では，3 個の入力多項式に対し，2 個の入力多項式に対する部分終結式行列 $N_k(P_1, P_2)$ に類似し，かつ表現がより簡潔で次元がより小さな行列を構成し，その rank から入力多項式の GCD の次数を見積もる例を示す．

4 より簡潔な部分終結式行列によるGCDの次数の見積もり（計算例）

本章では，次式で与えられる多項式 $P_{1,1}(x), P_{2,1}(x), P_{3,1}(x)$ に対し，$\deg(\gcd(P_{1,1}, P_{2,1}, P_{3,1}))$ を見積もる．

$$
\begin{aligned}
P_{1,1}(x) &= p_4^{(1,1)}x^4 + p_3^{(1,1)}x^4 + p_2^{(1,1)}x^4 + p_1^{(1,1)}x + p_0^{(1,1)}, \quad p_4^{(1,1)} \neq 0, \\
P_{2,1}(x) &= p_4^{(2,1)}x^4 + p_3^{(2,1)}x^4 + p_2^{(2,1)}x^4 + p_1^{(2,1)}x + p_0^{(2,1)}, \quad p_4^{(2,1)} \neq 0, \\
P_{3,1}(x) &= p_4^{(3,1)}x^4 + p_3^{(3,1)}x^4 + p_2^{(3,1)}x^4 + p_1^{(3,1)}x + p_0^{(3,1)}, \quad p_4^{(3,1)} \neq 0, \qquad (4) \\
\gcd(P_{1,1}, P_{1,2}, P_{1,3}) &= \gcd(P_{1,1}, P_{2,1}), \quad \deg(\gcd(P_{1,1}, P_{1,2}, P_{1,3})) = \deg(\gcd(P_{1,1}, P_{2,1})) = 2, \\
\deg(\gcd(P_{1,1}, P_{3,1})) &= 3.
\end{aligned}
$$

さらに，本稿では，$P_{1,1}, P_{1,2}, P_{1,3}$ によって生成されるPRSは非特異，すなわち，多重PRSの各要素（剰余）を求める際の次数の減少はすべて1と仮定する．

入力多項式 (4) に対し，部分終結式行列に類似する行列として，次の行列を定義する．

$$
\bar{N}_0(P_{1,1}, P_{2,1}, P_{3,1}) = \Big(C_3(P_{1,1})|C_3(P_{2,1})|C_3(P_{3,1})\Big)
$$

$$
= \begin{pmatrix}
p_4^{(1,1)} & & & & p_4^{(2,1)} & & & & p_4^{(3,1)} & & & \\
p_3^{(1,1)} & p_4^{(1,1)} & & & p_3^{(2,1)} & p_4^{(2,1)} & & & p_3^{(3,1)} & p_4^{(3,1)} & & \\
p_2^{(1,1)} & p_3^{(1,1)} & p_4^{(1,1)} & & p_2^{(2,1)} & p_3^{(2,1)} & p_4^{(2,1)} & & p_2^{(3,1)} & p_3^{(3,1)} & p_4^{(3,1)} & \\
p_1^{(1,1)} & p_2^{(1,1)} & p_3^{(1,1)} & p_4^{(1,1)} & p_1^{(2,1)} & p_2^{(2,1)} & p_3^{(2,1)} & p_4^{(2,1)} & p_1^{(3,1)} & p_2^{(3,1)} & p_3^{(3,1)} & p_4^{(3,1)} \\
p_0^{(1,1)} & p_1^{(1,1)} & p_2^{(1,1)} & p_3^{(1,1)} & p_0^{(2,1)} & p_1^{(2,1)} & p_2^{(2,1)} & p_3^{(2,1)} & p_0^{(3,1)} & p_1^{(3,1)} & p_2^{(3,1)} & p_3^{(3,1)} \\
 & p_0^{(1,1)} & p_1^{(1,1)} & p_2^{(1,1)} & & p_0^{(2,1)} & p_1^{(2,1)} & p_2^{(2,1)} & & p_0^{(3,1)} & p_1^{(3,1)} & p_2^{(3,1)} \\
 & & p_0^{(1,1)} & p_1^{(1,1)} & & & p_0^{(2,1)} & p_1^{(2,1)} & & & p_0^{(3,1)} & p_1^{(3,1)} \\
 & & & p_0^{(1,1)} & & & & p_0^{(2,1)} & & & & p_0^{(3,1)}
\end{pmatrix}. \qquad (5)
$$

式 (5) の $\bar{N}_0$ の次元は8行12列のため，$\bar{N}_0$ のrankは高々8である．そこで，本例題では $\bar{N}_0$ に列変形を施すことにより，

$$
\mathrm{rank}(\bar{N}_0) = 6 = 8 - \deg(\gcd(P_{1,1}, P_{2,1}, P_{3,1})) \qquad (6)
$$

を示す．以下では

1. 列ブロック $C_3(P_{1,1})$ と $C_3(P_{2,1})$ の間での列変形
2. 列ブロック $C_3(P_{1,1})$ と $C_3(P_{3,1})$ の間での列変形

を独立して行い，その後，両者の結果を統合して $\mathrm{rank}(\bar{N}_0)$ を求める．

4.1 列ブロック $C_3(P_{1,1})$ と $C_3(P_{2,1})$ の間での列変形

本節に挙げる列ブロックでの列変形は，$P_{1,1}$ と $P_{2,1}$ によって生成されるPRSに対応する．

1. $P_{1,1}$ で $P_{2,1}$ を消去: $\mathrm{rem}(P_{2,1}, P_{1,1}) = P_{2,2}(x) = p_3^{(2,2)}x^3 + p_2^{(2,2)}x^2 + p_1^{(2,2)}x + p_0^{(2,2)}$ とおく．$P_{1,1}$ と $P_{2,1}$ はともに4次の多項式なので，$P_{2,2}$ の各項の係数の導出は，式 (5) の $\bar{N}_0$ において，$j = 1, \ldots, 4$ に対し，第 j 列の $-\dfrac{p_4^{(2,1)}}{p_4^{(1,1)}}$ 倍を第 $j+4$ 列に加え，第 $j+4$ 列の最上部の成分を消去する列変形に対

応する．この列変形により，$\bar{N}_0$ の列ブロック $\left(C_3(P_{1,1})|C_3(P_{2,1})\right)$ は

$$\begin{pmatrix}
p_4^{(1,2)} & & & & & & & \\
p_3^{(1,2)} & p_4^{(1,2)} & & & p_3^{(2,2)} & & & \\
p_2^{(1,2)} & p_3^{(1,2)} & p_4^{(1,2)} & & p_2^{(2,2)} & p_3^{(2,2)} & & \\
p_1^{(1,2)} & p_2^{(1,2)} & p_3^{(1,2)} & p_4^{(1,2)} & p_1^{(2,2)} & p_2^{(2,2)} & p_3^{(2,2)} & \\
p_0^{(1,2)} & p_1^{(1,2)} & p_2^{(1,2)} & p_3^{(1,2)} & p_0^{(2,2)} & p_1^{(2,2)} & p_2^{(2,2)} & p_3^{(2,2)} \\
 & p_0^{(1,2)} & p_1^{(1,2)} & p_2^{(1,2)} & & p_0^{(2,2)} & p_1^{(2,2)} & p_2^{(2,2)} \\
 & & p_0^{(1,2)} & p_1^{(1,2)} & & & p_0^{(2,2)} & p_1^{(2,2)} \\
 & & & p_0^{(1,2)} & & & & p_0^{(2,2)}
\end{pmatrix} \tag{7}$$

となる（ここに，$\bar{N}_0$ の列ブロック $C_3(P_{1,1})$ に対応する多項式 $P_{1,1}$ を，式 (7) の左側の列ブロックでは $P_{1,2}$ とおき，$j=0,\ldots,4$ に対し，$p_j^{(1,2)}=p_j^{(1,1)}$ とおいた）．このとき，第 5 列から第 8 列まで，最上部の成分が消去されたことに注意する．

2. $P_{2,2}$ で $P_{1,2}$ を消去: $\mathrm{rem}(P_{1,2},P_{2,2})=P_{1,3}(x)=p_2^{(1,3)}x^2+p_1^{(1,3)}x+p_0^{(1,3)}$ とおく．$\deg(P_{1,2})=4$, $\deg(P_{2,2})=3$ より，$P_{1,3}$ の各項の係数の導出は，式 (7) の列ブロックにおいて，$j=2,\ldots,4$ に対し，以下の列変形により，第 j 列の $p_4^{(1,2)}$ および $p_3^{(1,2)}$ の成分を消去する計算に対応する．

   (a) 第 j 列に第 $j+3$ 列の $-\dfrac{p_4^{(1,2)}}{p_3^{(2,2)}}$ 倍を加える．この結果の第 $(j,j+1)$ 成分を $\bar{p}_3^{(1,2)}$ とおく．

   (b) 第 j 列に第 $j+4$ 列の $-\dfrac{\bar{p}_3^{(1,2)}}{p_3^{(2,2)}}$ 倍を加える．

   以上の列変形により，式 (7) の列ブロックは

$$\begin{pmatrix}
p_4^{(1,2)} & & & & & & & \\
p_3^{(1,2)} & & & & p_3^{(2,3)} & & & \\
p_2^{(1,2)} & & & & p_2^{(2,3)} & p_3^{(2,3)} & & \\
p_1^{(1,2)} & p_2^{(1,3)} & & & p_1^{(2,3)} & p_2^{(2,3)} & p_3^{(2,3)} & \\
p_0^{(1,2)} & p_1^{(1,3)} & p_2^{(1,3)} & & p_0^{(2,3)} & p_1^{(2,3)} & p_2^{(2,3)} & p_3^{(2,3)} \\
 & p_0^{(1,3)} & p_1^{(1,3)} & p_2^{(1,3)} & & p_0^{(2,3)} & p_1^{(2,3)} & p_2^{(2,3)} \\
 & & p_0^{(1,3)} & p_1^{(1,3)} & & & p_0^{(2,3)} & p_1^{(2,3)} \\
 & & & p_0^{(1,3)} & & & & p_0^{(2,3)}
\end{pmatrix} \tag{8}$$

となる（ここに，式 (7) の第 5 列から第 8 列に対応する多項式 $P_{2,2}$ を，式 (8) では $P_{2,3}$ とおき，$j=0,\ldots,3$ に対し，$p_j^{(2,3)}=p_j^{(2,2)}$ とおいた）．さらに，$P_{1,3}(x)$ は $P_{1,1}$ と $P_{2,1}$ によって生成される PRS の要素である 2 次の多項式であるが，仮定より $\deg(\gcd(P_{1,1},P_{2,1}))=2$ であることから，$P_{1,3}(x)=c_1\cdot\gcd(P_{1,1},P_{2,1})$ $(c_1\neq 0\in\mathbb{R})$ であることがわかる．

3. $P_{1,3}$ で $P_{2,3}$ を消去: $P_{1,3}=c_1\cdot\gcd(P_{1,1},P_{2,1})$ より，$\mathrm{rem}(P_{1,3},P_{2,3})=0$. ゆえに，このような列の導出は，式 (8) の列ブロックにおいて，$j=7,8$ に対し，以下の列変形により，第 j 列の成分を消去する計算に対応する．

   (a) 第 j 列に第 $j-5$ 列の $-\dfrac{p_3^{(2,3)}}{p_2^{(1,3)}}$ 倍を加える．この結果の第 $(j-2,j)$ 成分を $\bar{p}_2^{(2,3)}$ とおく．

(b) 第 j 列に第 $j-4$ 列の $-\dfrac{\bar{p}_2^{(2,3)}}{p_2^{(1,3)}}$ 倍を加える.

以上の列変形により，式 (8) の列ブロックは

$$\begin{pmatrix} p_4^{(1,2)} & & & & & & & \\ p_3^{(1,2)} & & & & p_3^{(2,3)} & & & \\ p_2^{(1,2)} & & & & p_2^{(2,3)} & p_3^{(2,3)} & & \\ p_1^{(1,2)} & p_2^{(1,4)} & & & p_1^{(2,3)} & p_2^{(2,3)} & 0 & \\ p_0^{(1,2)} & p_1^{(1,4)} & p_2^{(1,4)} & & p_0^{(2,3)} & p_1^{(2,3)} & 0 & 0 \\ & p_0^{(1,4)} & p_1^{(1,4)} & p_2^{(1,4)} & & p_0^{(2,3)} & 0 & 0 \\ & & p_0^{(1,4)} & p_1^{(1,4)} & & & 0 & 0 \\ & & & p_0^{(1,4)} & & & & 0 \end{pmatrix} \tag{9}$$

となる（ここに，式 (8) の第 2 列から第 4 列に対応する多項式 $P_{1,3}$ を，式 (9) では $P_{1,4}$ とおき，$j=0,1,2$ に対し，$p_j^{(1,4)}=p_j^{(1,3)}$ とおいた）．このとき，第 7 列と第 8 列が消去されたことに注意する．

ゆえに，列ブロック $C_3(P_{1,1})$ と $C_3(P_{2,1})$ の間の列変形により，列ブロック $C_3(P_{2,1})$ の rank を 2 下げられることがわかる．

4.2 列ブロック $C_3(P_{1,1})$ と $C_3(P_{3,1})$ の間での列変形

本節に挙げる列ブロックでの列変形は，$P_{1,1}$ と $P_{3,1}$ によって生成される PRS に対応する．

1. $P_{3,1}$ で $P_{1,1}$ を消去: $\mathrm{rem}(P_{1,1},P_{3,1})=P_{1,5}(x)=p_3^{(1,5)}x^3+p_2^{(1,5)}x^2+p_1^{(1,5)}x+p_0^{(1,5)}$ とおく．$P_{1,1}$ と $P_{3,1}$ はともに 4 次の多項式なので，$P_{1,5}$ の係数の導出は，$j=1,\ldots,4$ に対し，$\bar{N}_0$ の第 $j+8$ 列の $-\dfrac{P_4^{(1,1)}}{P_4^{(3,1)}}$ 倍を第 j 列に加え，第 $j+8$ 列の最上部の成分を消去する列変形に対応する．この列変形により，$\bar{N}_0$ の列ブロック $\left(C_3(P_{1,1})|C_3(P_{3,1})\right)$ は

$$\begin{pmatrix} & & & & p_4^{(3,5)} & & & \\ p_3^{(1,5)} & & & & p_3^{(3,5)} & p_4^{(3,5)} & & \\ p_2^{(1,5)} & p_3^{(1,5)} & & & p_2^{(3,5)} & p_3^{(3,5)} & p_4^{(3,5)} & \\ p_1^{(1,5)} & p_2^{(1,5)} & p_3^{(1,5)} & & p_1^{(3,5)} & p_2^{(3,5)} & p_3^{(3,5)} & p_4^{(3,5)} \\ p_0^{(1,5)} & p_1^{(1,5)} & p_2^{(1,5)} & p_3^{(1,5)} & p_0^{(3,5)} & p_1^{(3,5)} & p_2^{(3,5)} & p_3^{(3,5)} \\ & p_0^{(1,5)} & p_1^{(1,5)} & p_2^{(1,5)} & & p_0^{(3,5)} & p_1^{(3,5)} & p_2^{(3,5)} \\ & & p_0^{(1,5)} & p_1^{(1,5)} & & & p_0^{(3,5)} & p_1^{(3,5)} \\ & & & p_0^{(1,5)} & & & & p_0^{(3,5)} \end{pmatrix} \tag{10}$$

となる（ここに，$\bar{N}_0$ の列ブロック $C_3(P_{3,1})$ に対応する多項式 $P_{3,1}$ を，式 (10) の左側の列ブロックでは $P_{3,5}$ とおき，$j=0,\ldots,4$ に対し，$p_j^{(3,5)}=p_j^{(3,1)}$ とおいた）．さらに，$P_{1,5}(x)$ は $P_{1,1}$ と $P_{3,1}$ によって生成される PRS の要素である 3 次多項式であるが，仮定より $\deg(\gcd(P_{1,1},P_{3,1}))=3$ であることから，$P_{1,5}=c_2\cdot\gcd(P_{1,1},P_{3,1})$ $(c_2\neq 0\in\mathbb{R})$ であることがわかる．

2. $P_{1,5}$ で $P_{3,5}$ を消去: $P_{1,5}=c_2\cdot\gcd(P_{1,1},P_{3,1})$ より，$\mathrm{rem}(P_{1,1},P_{3,1})=0$. ゆえに，式 (10) において，これに対応する列変形は，$j=6,7,8$ に対し，以下の計算により行われる．

(a) 第 j 列に第 $j-5$ 列の $-\dfrac{p_4^{(3,5)}}{p_3^{(1,5)}}$ 倍を加える．この結果の第 $(j-3,j)$ 成分を $\bar{p}_3^{(3,5)}$ とおく．

(b) 第 j 列に第 $j-4$ 列の $-\dfrac{\bar{p}_3^{(3,5)}}{p_3^{(1,5)}}$ 倍を加える．

以上の列変形により，式 (10) の列ブロックは

$$\begin{pmatrix}
 & & & & p_4^{(3,5)} & \\
p_3^{(1,6)} & & & & p_3^{(3,5)} & 0 & \\
p_2^{(1,6)} & p_3^{(1,6)} & & & p_2^{(3,5)} & 0 & 0 & \\
p_1^{(1,6)} & p_2^{(1,6)} & p_3^{(1,6)} & & p_1^{(3,5)} & 0 & 0 & 0 \\
p_0^{(1,6)} & p_1^{(1,6)} & p_2^{(1,6)} & p_3^{(1,6)} & p_0^{(3,5)} & 0 & 0 & 0 \\
 & p_0^{(1,6)} & p_1^{(1,6)} & p_2^{(1,6)} & & 0 & 0 & 0 \\
 & & p_0^{(1,6)} & p_1^{(1,6)} & & & 0 & 0 \\
 & & & p_0^{(1,6)} & & & & 0
\end{pmatrix}. \tag{11}$$

となる（ここに，式 (10) の第 1 列から第 4 列に対応する多項式 $P_{1,5}$ を，式 (11) では $P_{1,6}$ とおき，$j=0,\ldots,3$ に対し，$p_j^{(1,6)}=p_j^{(1,5)}$ とおいた）．

ゆえに，列ブロック $C_3(P_{1,1})$ と $C_3(P_{3,1})$ の間の列変形により，列ブロック $C_3(P_{1,1})$ の rank を 3 下げられることがわかる．

4.3 行列 $\bar{N}_0(P_{1,1},P_{2,1},P_{3,1})$ の列変形のまとめ

第 4.1 節および第 4.2 節のブロック毎の列変形をまとめると，行列 $\bar{N}_0(P_{1,1},P_{2,1},P_{3,1})$ を次式の形に変換する列変形が存在することがわかる．

$$\begin{pmatrix}
p_4^{(1,2)} & & & & & & & & p_4^{(3,5)} & & & \\
p_3^{(1,2)} & & & & p_3^{(2,3)} & & & & p_3^{(3,5)} & 0 & & \\
p_2^{(1,2)} & & & & p_2^{(2,3)} & p_3^{(2,3)} & & & p_2^{(3,5)} & 0 & 0 & \\
p_1^{(1,2)} & p_2^{(1,4)} & & & p_1^{(2,3)} & p_2^{(2,3)} & 0 & & p_1^{(3,5)} & 0 & 0 & 0 \\
p_0^{(1,2)} & p_1^{(1,4)} & p_2^{(1,4)} & & p_0^{(2,3)} & p_1^{(2,3)} & 0 & 0 & p_0^{(3,5)} & 0 & 0 & 0 \\
 & p_0^{(1,4)} & p_1^{(1,4)} & p_2^{(1,4)} & & p_0^{(2,3)} & 0 & 0 & & 0 & 0 & 0 \\
 & & p_0^{(1,4)} & p_1^{(1,4)} & & & 0 & 0 & & & 0 & 0 \\
 & & & p_0^{(1,4)} & & & & 0 & & & & 0
\end{pmatrix}. \tag{12}$$

ここに，第 3, 4, 5 列の各成分は，$\gcd(P_{1,1},P_{2,1},P_{3,1})$ の各係数に対応することに注意する．

これに対し，以下の列変形を行うことにより，第 9 列を消去して式 (6) が成り立つことを示す．

1. 第 1 列の $-\dfrac{p_4^{(3,5)}}{p_4^{(1,2)}}$ 倍を第 9 列に加える．これにより，第 $(9,1)$ 成分が消去される．この列変形によって得られる第 $(9,2)$ 成分を $\bar{p}_3^{(3,5)}$ とおく．

2. 上で得られた第 9 列に，第 5 列の $-\dfrac{\bar{p}_3^{(3,5)}}{p_3^{(2,3)}}$ 倍を加える．これにより，第 $(9,2)$ 成分が消去される．この列変形によって得られる第 $(9,3)$ 成分を $\bar{p}_2^{(3,5)}$ とおく．

3. 上で得られた第9列に，第6列の $-\dfrac{p_2^{(3,5)}}{p_3^{(2,3)}}$ 倍を加える．これにより，第 $(9,3)$ 成分が消去される．新たに得られた第9列を

$$ {}^t(0,0,0,p_4^{(3,6)},p_3^{(3,6)},p_2^{(3,6)},0,0) \tag{13} $$

とおく．ゆえに，式 (12) の行列は

$$ \begin{pmatrix} p_4^{(1,2)} & & & & & & & 0 & & \\ p_3^{(1,2)} & & & & p_3^{(2,3)} & & & 0 & 0 & \\ p_2^{(1,2)} & & & & p_2^{(2,3)} & p_3^{(2,3)} & & 0 & 0 & 0 \\ p_1^{(1,2)} & p_2^{(1,4)} & & & p_1^{(2,3)} & p_2^{(2,3)} & 0 & p_4^{(3,6)} & 0 & 0 & 0 \\ p_0^{(1,2)} & p_1^{(1,4)} & p_2^{(1,4)} & & p_0^{(2,3)} & p_1^{(2,3)} & 0 & 0 \; p_3^{(3,6)} & 0 & 0 & 0 \\ & p_0^{(1,4)} & p_1^{(1,4)} & p_2^{(1,4)} & & p_0^{(2,3)} & 0 & 0 \; p_2^{(3,6)} & 0 & 0 & 0 \\ & & p_0^{(1,4)} & p_1^{(1,4)} & & & 0 & 0 & & 0 & 0 \\ & & & p_0^{(1,4)} & & & & 0 & & & 0 \end{pmatrix} \tag{14} $$

となる．

4. 式 (14) の行列の第9列は，多項式

$$ p_4^{(3,6)}x^4+p_3^{(3,6)}x^3+p_2^{(3,6)}x^2=x^2(p_4^{(3,6)}x^2+p_3^{(3,6)}x+p_2^{(3,6)}) \tag{15} $$

に対応する．一方，$P_{1,4}=\gcd(P_{1,1},P_{2,1},P_{3,1})=\gcd(P_{1,1},P_{2,1})$ より，$P_{1,1},P_{2,1},P_{3,1}$ の $\mathbb{R}[x]$-線形結合で次数が2次以上の多項式は $P_{1,4}$（またはその定数倍）を因子にもつ．ゆえに，上述のステップ $1,\ldots,3$ によって得られた多項式 (15) のうち，x^2 を除く因子は $P_{1,4}$ の定数倍である．一方，式 (14) の行列の第2列が表す多項式は

$$ p_2^{(1,4)}x^4+p_1^{(1,4)}x^3+p_0^{(1,4)}x^2=x^2\cdot P_{1,4}(x) $$

であり，式 (15) の定数倍である．ゆえに，式 (14) の行列の第9列は，同じ行列の第2列の定数倍によって消去されることがわかる．

以上の列変形により，式 (14) の行列の第9列は消去され，次式のようになる．

$$ \begin{pmatrix} p_4^{(1,2)} & & & & & & & 0 & & \\ p_3^{(1,2)} & & & & p_3^{(2,3)} & & & 0 & 0 & \\ p_2^{(1,2)} & & & & p_2^{(2,3)} & p_3^{(2,3)} & & 0 & 0 & 0 \\ p_1^{(1,2)} & p_2^{(1,4)} & & & p_1^{(2,3)} & p_2^{(2,3)} & 0 & 0 & 0 & 0 & 0 \\ p_0^{(1,2)} & p_1^{(1,4)} & p_2^{(1,4)} & & p_0^{(2,3)} & p_1^{(2,3)} & 0 & 0 \; 0 & 0 & 0 & 0 \\ & p_0^{(1,4)} & p_1^{(1,4)} & p_2^{(1,4)} & & p_0^{(2,3)} & 0 & 0 \; 0 & 0 & 0 & 0 \\ & & p_0^{(1,4)} & p_1^{(1,4)} & & & 0 & 0 & & 0 & 0 \\ & & & p_0^{(1,4)} & & & & 0 & & & 0 \end{pmatrix}. \tag{16} $$

また，式 (16) の行列の第 $1,\ldots,6$ 列は，適当な列の入れ替えにより，非零成分が下三角で，かつ対角成分が非零になるようにできるので，線型独立である．以上により，式 (6) が示された．

5 まとめ

本稿では，3個以上の1変数多項式に対し，rankからGCDの次数を見積もることができるような，部分終結式行列に類似する行列で，既知の同種の行列に比べて次元がより小さなものの存在を示唆し，一つの計算例を示した．

計算例においては，入力多項式の個数は3個でそれらの次数はすべて等しく（4次），それらから選んだ2つの多項式によって生成される（通常の）PRSはすべて非特異であることを仮定した．そして，この条件下で構成した行列のrankからGCDの次数を見積もることができることを示した．

本稿の計算例によって構成した行列は，同じ目的で用いることができる既知の部分終結式行列と比較して，次元がより小さく，近似GCDの次数の見積もりなどを目的とした数値計算において，時間計算量の面で計算の効率化が期待できる．

一方で，本稿の計算例を，より一般の入力多項式に適用させるためには，1) 入力多項式の個数が任意の$n > 2$の場合，2) 入力多項式の次数が任意に与えられた場合，そして3) 入力多項式から生成されるPRSが特異な場合（PRSの次数の減少が1を越えるような要素が存在する場合），に対する理論の正当性を示す必要がある．

今後は，これらの状況も含め，より一般の入力多項式に対し，本稿の計算例のような行列を構成できるよう，一般論の構築に結びつけたいと考えている．

参 考 文 献

[1] I. Z. Emiris, A. Galligo, and H. Lombardi. Certified approximate univariate GCDs. *J. Pure Appl. Algebra*, Vol. 117/118, pp. 229–251, 1997.

[2] D. Rupprecht. An algorithm for computing certified approximate GCD of n univariate polynomials. *J. Pure and Applied Algebra*, Vol. 139, pp. 255–284, 1999.

[3] Tateaki Sasaki and Akio Furukawa. Theory of multiple polynomial remainder sequence. *Publ. Res. Inst. Math. Sci.*, Vol. 20, pp. 367–399, 1984.

[4] A. Terui. GPGCD, an iterative method for calculating approximate GCD, for multiple univariate polynomials. In V.P. Gerdt, W. Koepf, E.W. Mayr, and E.H. Vorozhtsov, editors, *Computer Algebra in Scientific Computing (Proc. CASC 2010)*, Vol. 6244 of *Lecture Notes in Computer Science*, pp. 238–249. Springer, 2010.

[5] 照井章. 近似GCD算法GPGCDの複数入力多項式への拡張. 数式処理研究の新たな発展, 数理解析研究所講究録, 第1759巻, pp. 15–25. 京都大学数理解析研究所, 2011.

[6] 高木貞治. 代数学講義（改訂新版）. 共立出版, 東京, 1965.