多項式を要素に持つ行列の分解に基づく多変数近似GCDの最適化

Optimization of multivariate approximate GCD based on decomposition of matrices within polynomial entries

筑波大学医学医療系　　讃岐勝 [*1]
Masaru Sanuki
Institute of Medicine, University of Tsukuba

Abstract

The QRGCD method for univariate polynomials is known as an efficient algorithm for computing approximate greatest common divisor (GCD). However, it is well known that extending such numerically based algorithms to multivariate polynomials presents significant challenges. In this study, we revisit computational techniques for matrices whose entries are multivariate polynomials, aiming to improve the efficiency of approximate GCD algorithms based on linear equations. Furthermore, we investigate the QR decomposition for matrices with multivariate polynomial entries and explore the development of corresponding algorithms.

1　はじめに

浮動小数係数$\mathbb{F}$を数係数, 主変数x, 従変数$(\boldsymbol{t}) = (t_1, \ldots, t_\ell)$からなる多変数多項式環$\mathbb{F}[x, \boldsymbol{t}] = \mathbb{F}[x, t_1, \ldots, t_\ell]$の多項式$F(x, \boldsymbol{t}), G(x, \boldsymbol{t})$の近似GCDの計算法について本稿では議論する.

多変数多項式の近似GCDを求めるアルゴリズム開発に関する研究は1980年末から始まり，数多くの算法が提案されてきた．黎明期においては計算機の能力もそれほどではなかったため数式処理をベースにした方法も見られたが，計算機の能力があがり始めた2000年以降は数値計算をベースにした方法がではじめ，2010年以降は数値計算を主にした算法が精度がよく，しばし利用される．一方で数式処理を基にした算法は数値計算と合わせたハイブリッドアルゴリズムとして改良されて，精度の肝となる部分は数値計算，精度が落ちないことを保証できる場所は数式処理をテクニックを使うことで独自性を出している．本稿では後者について探求する.

数式処理をもとに多項式を扱うと数式膨張に起因する大きな桁落ち誤差の発生と丸め誤差の蓄積によってすぐに計算が不安定にあり，意味のない結果を返すことが多い．数式膨張を抑える有効な方法として，イデアル$I = \langle t_1 - s_1, \ldots, t_\ell - s_\ell \rangle$上で計算することである$(\boldsymbol{s} = (s_1, \ldots, s_\ell) \in \mathbb{F}^\ell)$．これらを適応した方法として次が知られる.

- 互除法の拡張：PC-PRS法の適応と有効浮動小数の組み合わせ [7]

[*1] 〒 305-8575 茨城県つくば市天王台 1-1-1　E-mail: sanuki@md.tsukuba.ac.jp

- QRGCD 法を Givens 回転のみで擬似的に実現 (上三角行列だけを計算) [7]

$$\begin{pmatrix} c(\boldsymbol{t}) & s(\boldsymbol{t}) \\ -s(\boldsymbol{t}) & c(\boldsymbol{t}) \end{pmatrix} \begin{pmatrix} F(x,\boldsymbol{t}) \\ G(x,\boldsymbol{t}) \end{pmatrix} \pmod{I^{w+1}}$$

これらは数式膨張は抑えたが，丸め誤差の蓄積による計算の不安定さの考慮をしていないため次数の小さな場合にしか有効ではない．

EZ-GCD 法，EEZ-GCD 法 (Hensel による方法) はリフティングに用いる初期因子が安定であれば計算精度がある程度良いことが知られている．このことは，精度が必要な部分は数値計算で，効率的に計算できる部分は数式処理で構成することが有効であることを示唆している．この点に注目して，Bezout 行列を用いる近似 GCD 計算法と知られる Barnetts の定理の拡張 [8]，部分終結式行列の零空間から近似 GCD を計算する方法の拡張 [9]，を実現した．本稿では，よく知られた方法でまだ拡張されていない QRGCD 法の多変数多項式への拡張をゴールに議論を行う．これを実現するためには，多変数多項式を要素に持つ行列の QR 法を構成する必要があり，線形代数でよく知られたアルゴリズムの拡張になっているのか注意深く議論することが必要となる．

以上の議論を進めるため，2 章では多項式を要素に持つ行列からなる線型方程式を逆行列で求めることから始める (LU 分解をするわけではない)．3 章以降で QR 分解に必要な直交行列の拡張などを検討してアルゴリズムを検討する．

2　逆行列による方法

行列 $\mathcal{M} \in \mathbb{F}[\boldsymbol{t}]^{m\times m}$ を考える．行列の各要素が同じ全次数 i の斉次多項式で構成されるよう，次のように表現する．

$$\begin{aligned} \mathcal{M} &= \mathcal{M}^{(0)} + \delta\mathcal{M}^{(1)} + \delta\mathcal{M}^{(1)} + \cdots + \delta\mathcal{M}^{(w)} + \ldots \\ &\equiv \mathcal{M}^{(w)} \pmod{I^{w+1}}. \end{aligned}$$

ここで，$\delta\mathcal{M}^{(i)} \in \mathbb{F}[\boldsymbol{t}]^{m\times m}$ の各要素は全次数 i の斉次多項式であり，とくに $\mathcal{M}^{(0)} \in \mathbb{F}^{m\times m}$ である．

以下，$\mathcal{M}^{(0)} \in \mathbb{F}^{m\times m}$ は正則であると仮定する (正則になるように $\boldsymbol{s} \in \mathbb{F}^{\ell}$ を選ぶ)．このとき，行列 $\mathcal{M}$ の右逆行列 $\mathcal{N} = \mathcal{M}^{-1} \pmod{I^{w+1}}$ を次の手順で構成される．

補題 1
$\mathcal{M}^{(0)} \in \mathbb{F}^{m\times m}$ が正則のとき，$\mathcal{M} \in \mathbb{F}[\boldsymbol{t}]^{m\times m} \pmod{I}^{(w+1)}$ の右逆行列 $\mathcal{N}^{(w)} \in \mathbb{F}[\boldsymbol{t}]^{m\times m}$ が存在する；

$$\mathcal{M}^{w}\mathcal{N}^{w} \equiv \mathcal{E} \pmod{I^{w+1}}$$

ここで，$\mathcal{E} \in \mathbb{F}^{m\times m}$ は単位行列である．

証明

- $w = 0$ のとき，$\mathcal{M}^{(0)}$ の (右) 逆行列 $N^{(0)} = \left(\mathcal{M}^{(0)}\right)^{-1}$ は数値計算で求める．
- $w = 1$ のとき，$(\mathcal{M}^{(0)} + \delta\mathcal{M}^{(1)})(\mathcal{N} + \delta\mathcal{N}^{(1)}) \equiv \mathcal{E} \pmod{I^2}$ を満たす $\delta\mathcal{N}^{(1)}$ は次の手順で構成される．全次数 1 の斉次部分のみ集めると次を得る ($\mathcal{O} \in \mathbb{F}^{m\times m}$ は零行列)．

$$\begin{aligned} \mathcal{M}^{(0)}\delta\mathcal{N}^{(1)} + \delta\mathcal{M}^{(1)}\mathcal{N}^{(0)} &= \mathcal{O} \\ \mathcal{M}^{(0)}\delta\mathcal{N}^{(1)} &= -\delta\mathcal{M}^{(1)}\mathcal{N}^{(0)} \end{aligned}$$

- w 次まで構成されたと仮定し，$w+1$ 次を行列 δN^{w+1} は次のように構成する．

$$(\mathcal{M}^{(0)} + \cdots + \delta\mathcal{M}^{(w)})(\mathcal{N}^{(0)} + \cdots + \delta\mathcal{N}^{(w)}) \equiv \mathcal{E} \pmod{I^{w+1}}$$

の全次数 w 次の部分を整理することによって $\delta\mathcal{N}^{(w)}$ は次のように構成される．

$$\mathcal{M}^{(0)}\delta\mathcal{N}^{(w)} + \delta\mathcal{M}^{(1)}\delta\mathcal{N}^{(w-1)} + \cdots + \delta\mathcal{M}^{(w)}\mathcal{N}^{(0)} = \mathcal{O} \tag{1}$$

$$\mathcal{M}^{(0)}\delta\mathcal{N}^{(w)} = -\sum_{i=1}^{w} \delta\mathcal{M}^{(i)}\delta\mathcal{N}^{(w-i)} \tag{2}$$

$\mathcal{M}^{(0)}$ は正則なので，$w+1$ 次の項 $\delta\mathcal{N}^{(w+1)} = -\mathcal{N}^{(0)} \sum_{i=1}^{w} \delta\mathcal{M}^{(i)}\delta\mathcal{N}^{(w-i)}$ と表される．

∎

命題 2

補題 *1* で構成した右逆行列は左逆行列にもなる．

証明

式 (2) の $i = w, w-1, \ldots$ の場合についてそれぞれ右側から $\mathcal{M}^{w-i}$ を乗ずる．

$$\begin{aligned}
\mathcal{M}^{(0)}\delta\mathcal{N}^{(w)} \cdot \mathcal{M}^{(0)} &= -\delta\mathcal{M}^{(1)}\delta\mathcal{N}^{(w-1)} \cdot \mathcal{M}^{(0)} - \delta\mathcal{M}^{(2)}\delta\mathcal{N}^{(w-2)} \cdot \mathcal{M}^{(0)} - \cdots \\
\mathcal{M}^{(0)}\delta\mathcal{N}^{(w-1)} \cdot \delta\mathcal{M}^{(1)} &= -\delta\mathcal{M}^{(1)}\delta\mathcal{N}^{(w-2)} \cdot \delta\mathcal{M}^{(1)} - \delta\mathcal{M}^{(2)}\delta\mathcal{N}^{(w-3)} \cdot \delta\mathcal{M}^{(1)} - \cdots \\
&\vdots
\end{aligned}$$

右辺を足し合わせて整理すると，式 (1) より

$$-\delta\mathcal{M}^{(1)} \cdot \mathcal{O} - \delta\mathcal{M}^{(2)} \cdot \mathcal{O} - \cdots - \delta\mathcal{M}^{(w)} \cdot \mathcal{O} = \mathcal{O}$$

次に左辺を足し合わせると，

$$\mathcal{M}^{(0)}\left(\delta\mathcal{N}^{(w)}\mathcal{M}^{(0)} + \cdots + \delta\mathcal{N}^{(0)}\delta\mathcal{N}^{(w)}\right) = \mathcal{O}$$

を得るので，$\mathcal{M}^{(0)}$ が正則より

$$\delta\mathcal{N}^{(w)}\mathcal{M}^{(0)} + \cdots + \delta\mathcal{N}^{(0)}\delta\mathcal{N}^{(w)} = \mathcal{O}$$

を得る．それゆえ，$\mathcal{N}^{(w)}\mathcal{M}^{(w)} \equiv \mathcal{E} \pmod{I^{w+1}}$ であり，構成した右逆行列は左逆行列にもなる． ∎

2.1 既存の方法との比較

[8] では，逆行列を直接計算しないアプローチで線型方程式を解いた．実際のアプローチは次のとおりである．

アルゴリズム 1 (線型方程式の解法：解をリフティングする方法)

- 入力：線型方程式 $\mathcal{M}\boldsymbol{x} = \boldsymbol{b}$ *with* $\boldsymbol{b} \in \mathbb{F}[\boldsymbol{t}]^{m\times m}$．ただし，$\mathcal{M}^{(0)}$ は正則.
- 出力：$x \equiv c^{w} \in \mathbb{F}[\boldsymbol{t}]^{m\times m} \pmod{I^{w+1}}$

  次の手順で実行する．

  - $w = 0$ のとき：数値計算手法で解く．$\boldsymbol{c}^{(0)} = \mathcal{N}^{(0)}\boldsymbol{b}^{(0)}$

- $w = 1$ のとき：$\delta \boldsymbol{c}^{(1)} = \delta \boldsymbol{b}^1 - \mathcal{N}^{(0)} \left(\delta \mathcal{M}^{(1)} \boldsymbol{c}^{(0)} \right)$
- $w - 1$ 次まで構成されたとき；

$$\delta \boldsymbol{c}^{(w)} = \delta \boldsymbol{b}^{(w)} - \mathcal{N}^{(0)} \times \sum_{i=0}^{w-1} \delta \mathcal{M}^{w-i} \delta \boldsymbol{c}^{(i)}$$

今回提案した方法は，行列と行列の積の繰り返し，既存の方法 (アルゴリズム 1) は行列とベクトルの積の繰り返しであるため今回の提案手法は計算効率は良くないように見える．実際，計算量は $O(m)$ 倍だけ異なる (行列と行列の積を複数行うため)．

しかし，次の節で述べる refinement を検討すると今回の提案手法が悪くないことがわかる．

2.2 解の refinement

$\mathcal{M}\boldsymbol{x} = \boldsymbol{b}$ の解の refinement について数値計算でよく知られた次のルーチンの場合で検討を行う．

$\boldsymbol{z}_0$ を初期解とするときに，逆行列 $M^{-1} = \mathcal{N}^w$ を用いる方法は次の手順で動く．

アルゴリズム 2

- $\boldsymbol{r}_0 = \mathcal{M}\boldsymbol{z}_0 - \boldsymbol{b}$
- $\boldsymbol{z}_1 = \boldsymbol{z}_0 + \mathcal{M}^{-1}\boldsymbol{r}_0 \pmod{I^{w+1}}$
- $\vdots$
- $\boldsymbol{r}_i = \mathcal{M}\boldsymbol{z}_i - \boldsymbol{b}$
- $\boldsymbol{z}_{i+1} = \boldsymbol{z}_i + \mathcal{M}^{-1}\boldsymbol{r}_i \pmod{I^{w+1}}$
  - $||\boldsymbol{z}_i|| < ||\boldsymbol{z}_{i+1}||$ のとき終了

計算を見ると，1 つのステップは 1 回の行列とベクトルの積と 1 回のベクトルの同士の差の計算になる．

アルゴリズム 1 について，$\mathcal{M}^{-1} = \mathcal{N}^{(w)}$ を計算していないため，refinement のたびに線型方程式を解く必要がある．結果として計算量を比較すると，m 回 refinement を実行したとき同様の計算量になるため，単純に線型方程式を解くと行った場合には，本稿で提案した方法は全く効率的はない．

2.3 近似 GCD の計算に限った場合

Barnett の定理をでは線型方程式を解くこととなっているが，近似 GCD の計算で必要なのは解のある 1 つの要素のみである (第 1 要素か最後の要素のみ)．アルゴリズム 2 の

- $\boldsymbol{r}_i = \mathcal{M}\boldsymbol{z}_i - \boldsymbol{b}$
- $\boldsymbol{z}_{i+1} = \boldsymbol{z}_i + \mathcal{M}^{-1}\boldsymbol{r}_i \pmod{I^{w+1}}$

の部分に着目すると，逆行列 $\mathcal{N}^{(w)}$ がわかっていると Jacobi 法のような並列化が可能であり，実装の部分では効率化が期待できることがわかる．

3　多変数多項式による QRGCD 法

この章では，多項式を要素にもつ行列に対する QR 法について検討する．数値行列の場合，直行行列と上三角行列の積に分解する方法であるが，多項式を要素にもつ行列が直行するとは？ということから検討する必要がある．

本稿では，リフティング法によるアルゴリズムに着目しているため，次の分解が可能か検討する．

問題 1 (直行行列の拡張案：その 1)
$\mathcal{S} \in \mathbb{F}[\boldsymbol{t}]^{m\times m}$ に対して、次の分解が一般的に構築できるのか検討する．

$$\mathcal{S} \equiv \mathcal{Q}\mathcal{R} \equiv \mathcal{Q}^{(w)}\mathcal{R}^{(w)} \pmod{I^{w+1}}$$

where $\mathcal{Q}, \mathcal{R} \in \mathbb{F}[\boldsymbol{u}]^{m\times m}$ *with* $\mathcal{Q}\mathcal{Q}^T, \mathcal{Q}^T\mathcal{Q} \equiv \mathcal{E} \pmod{I^{w+1}}$ *and* $\mathcal{R}$ *is upper-trianguler* ∎

低次の部分からみる．

- $w = 0$: QR 分解

  $$\mathcal{S}^{(0)} = \mathcal{Q}^{(0)}\mathcal{R}^{(0)}$$

  Q は直交変換の積でかける．

- $w = 1$
  $\mathcal{Q}\mathcal{Q}^T, \mathcal{Q}^T\mathcal{Q} \equiv \mathcal{E} \pmod{I^2}$ を満たすには $\mathcal{Q}^{(1)} = \mathcal{Q}^{(0)} + \delta\mathcal{Q}^{(1)}$ について次の 3 条件を満たす必要がある．
  1. $\left(\mathcal{Q}^{(1)}\right)^T\mathcal{Q}^{(1)} \equiv \mathcal{Q}^{(1)}\left(\mathcal{Q}^{(1)}\right)^T \equiv \mathcal{E} \pmod{I^2}$
  2. $\left(\delta\mathcal{Q}^{(1)}\right)^T\mathcal{Q}^{(0)} + \left(\delta\mathcal{Q}^{(0)}\right)^T\delta\mathcal{Q}^{(1)} = \mathcal{O}$
  3. $\left(\delta\mathcal{Q}^{(1)}\right)^T\delta\mathcal{Q}^{(1)} \equiv \mathcal{O} \pmod{I^2}$

- ⋮

ここで，$\left(\delta\mathcal{Q}^{(1)}\right)^T\mathcal{Q}^{(0)} + \left(\delta\mathcal{Q}^{(0)}\right)^T\delta\mathcal{Q}^{(1)} = \mathcal{O}$ について，$\left(\delta\mathcal{Q}^{(0)}\right)^T\delta\mathcal{Q}^{(1)}$ は交代行列[1)]を満たすことが条件となる．このとき，次がすぐに言える．

補題 3
$\delta\mathcal{Q}^{(0)}$ は直交行列とする．$\delta\mathcal{Q}^{(1)}$ のある (i,j) 要素が 0 でないとき，$\left(\delta\mathcal{Q}^{(1)}\right)^T\mathcal{Q}^{(0)} + \left(\delta\mathcal{Q}^{(0)}\right)^T\delta\mathcal{Q}^{(1)}$ に対角要素が 0 でない要素が存在する．

証明
$\left(\delta\mathcal{Q}^{(0)}\right)^T\delta\mathcal{Q}^{(1)}$ は交代行列なので，$\delta\mathcal{Q}^{(1)}$ の i 列は $\sum_{j\neq i}\alpha_{i,j}\boldsymbol{q}_j^{(0)}$ でかける．このとき，$\left(\delta\mathcal{Q}^{(0)}\right)^T\delta\mathcal{Q}^{(1)}$ の (i,j) 要素は $\alpha_{i,j}$ であり $(i \neq j)$,

$$\alpha_{i,j} = -\alpha_{j,i} \neq 0$$

となる $i \neq j$ がある．一方で，$\left(\delta\mathcal{Q}^{(1)}\right)^T\mathcal{Q}^{(0)}$ について，(i,i) は $\alpha_{i,j}$ になる． ∎

ゆえに次がいえる．

[1)] $\mathcal{M}$ が交代行列 $\Leftrightarrow m_{i,j} = -m_{i,j}(i \neq j)$ and $m_{i,i} = 0$

命題 4
任意に与えられた行列 $\mathcal{S} \in \mathbb{F}[\boldsymbol{t}]^{m\times m}$ の分解について，$\mathcal{Q}^T\mathcal{Q}, \mathcal{Q}\mathcal{Q}^T \equiv \mathcal{E}$ をみたす $\mathcal{Q} \in \mathbb{F}[\boldsymbol{t}]\backslash\mathbb{F}$ は存在しない∎

次の例 1 は補題 3 を具体的に示す例になる．

例 1
$\left(\delta\mathcal{Q}^{(1)}\right)^T\mathcal{Q}^{(0)} + \left(\delta\mathcal{Q}^{(0)}\right)^T\delta\mathcal{Q}^{(1)}$ の対角要素含めて 0 にならないことを示す例になる．

- サンプル *1*

$$\begin{pmatrix} & 1 & \\ & & 1 \\ 1 & & \end{pmatrix} \cdot \begin{pmatrix} -2 & & \\ & & 2 \\ & 2 & \end{pmatrix} t_i = \begin{pmatrix} & & 2 \\ & 2 & \\ -2 & & \end{pmatrix} t_i$$
$$\begin{pmatrix} -2 & & \\ & & 2 \\ & 2 & \end{pmatrix} t_i \cdot \begin{pmatrix} & & 1 \\ 1 & & \\ & 1 & \end{pmatrix} = \begin{pmatrix} & & -2 \\ & 2 & \\ 2 & & \end{pmatrix} t_i$$

- サンプル *2*

$$\begin{pmatrix} & 1 & \\ & & 1 \\ 1 & & \end{pmatrix} \cdot \begin{pmatrix} & -5 & \\ -5 & & \\ & & 5 \end{pmatrix} t_i = \begin{pmatrix} -5 & & \\ & & 5 \\ & -5 & \end{pmatrix} t_i$$
$$\begin{pmatrix} & -5 & \\ -5 & & \\ & & 5 \end{pmatrix} t_i \cdot \begin{pmatrix} & & 1 \\ 1 & & \\ & 1 & \end{pmatrix} = \begin{pmatrix} -5 & & \\ & & -5 \\ & 5 & \end{pmatrix} t_i$$

対角要素以外は *0* にできることを示す例になっていることに注意する．この事実は定義を拡張する上で重要な気付きとなる．

問題 2 (直行行列の拡張案：その 2)
$\mathcal{S} \in \mathbb{F}[\boldsymbol{t}]^{m\times m}$ に対して、次の分解を考える

$$\mathcal{S} \equiv \mathcal{Q}\mathcal{R} \equiv \mathcal{Q}^{(w)}\mathcal{R}^{(w)} \pmod{I^{w+1}}$$

where $\mathcal{Q}, \mathcal{R} \in \mathbb{F}[\boldsymbol{t}]^{m\times m}$ *with* $\mathcal{Q}\mathcal{Q}^T, \mathcal{Q}^T\mathcal{Q} \equiv \mathcal{U}$ *and* $\mathcal{R}$ *is upper-trianguler.* ここで、

$$\mathcal{U} = \begin{pmatrix} u_1 & 0 & \cdots \\ \vdots & \ddots & \vdots \\ 0 & \ddots & u_m \end{pmatrix} = \mathrm{diag}(u_i) \in \mathbb{F}\{\boldsymbol{t}\}^{m\times m}$$

whwre each $u_i = 1 + u_{i,1}(\boldsymbol{t}) + u_{i,2}(\boldsymbol{t}) + \cdots \in \mathbb{F}\{\boldsymbol{t}\}$ *is unit.* ∎

上三角行列は次のように構築される．

$$\mathcal{Q}^{(0)^T}\delta\mathcal{S}^{(1)} \quad = \quad \left(\mathcal{Q}^{(0)^T}\delta\mathcal{Q}^{(1)}\right)\mathcal{R}^{(0)} + \delta\mathcal{R}^{(1)}$$

各行列は $\delta\mathcal{Q}^{(1)}$ から構成する (除算をする感覚である)．
まず，$\mathcal{Q}^{(1)} = \mathcal{Q})^0 + \delta\mathcal{Q}^{(1)}$ について定義に従うのであれば，次を満たす必要がある．

1. $\left(\mathcal{Q}^{(1)}\right)^T\mathcal{Q}^{(1)} \equiv \mathcal{Q}^{(1)}\left(\mathcal{Q}^{(1)}\right)^T \equiv \mathcal{U} \pmod{I^2}$
2. $\left(\delta\mathcal{Q}^{(1)}\right)^T\mathcal{Q}^{(0)} + \left(\delta\mathcal{Q}^{(0)}\right)^T\delta\mathcal{Q}^{(1)} = \mathrm{diag}(u_1, \ldots, u_\ell)$
3. $\left(\delta\mathcal{Q}^{(1)}\right)^T\delta\mathcal{Q}^{(1)} \equiv \mathcal{O} \pmod{I^2}$

であり，$\delta\mathcal{Q}^{(1)}$ について ${\mathcal{Q}^{(0)}}^T\delta\mathcal{S}^{(1)} = \sum_{w_1+\ldots+w_\ell=1} \boldsymbol{u}^{\boldsymbol{\alpha}}{\tilde{\mathcal{Q}^{(0)}}}^T\delta\tilde{\mathcal{S}}^{(1)}$ with $\delta\tilde{\mathcal{S}}^{(1)} \in \mathbb{F}^{m\times m}$ と見ることで，数値行列で計算を扱うことができる．それぞれで対角要素にだけ値が並ぶようになることを示せば良い．前述の例 1 と次の例 2 は実際にそのようにできることを示す例になっている．

例 2
$\left(\delta\mathcal{Q}^{(1)}\right)^T\mathcal{Q}^{(0)} + \left(\delta\mathcal{Q}^{(0)}\right)^T\delta\mathcal{Q}^{(1)} = \mathrm{diag}(u_1, \ldots, u_\ell)$ となることはサンプル *1*, サンプル *2* で確認済みである．

- サンプル *3*

$$\begin{pmatrix} -2 & -5 & \\ -5 & & 2 \\ & 2 & 5 \end{pmatrix} t_i \cdot \begin{pmatrix} & & 1 \\ 1 & & \\ & 1 & \end{pmatrix} = \begin{pmatrix} -5 & & -2 \\ & 2 & -5 \\ 2 & 5 & \end{pmatrix} t_i$$

$$\begin{pmatrix} & 1 & \\ & & 1 \\ 1 & & \end{pmatrix} \cdot \begin{pmatrix} -2 & -5 & \\ -5 & & 2 \\ & 2 & 5 \end{pmatrix} t_i = \begin{pmatrix} -5 & & 2 \\ & 2 & 5 \\ -2 & -5 & \end{pmatrix} t_i$$

∎

このことは，任意の行列に対して拡張された直交分解ができることを示している．実際，

$${\mathcal{Q}^{(0)}}^T\mathcal{Q}^{(0)} = \begin{pmatrix} {\boldsymbol{q}_1^{(0)}}^T \\ \vdots \\ {\boldsymbol{q}_m^{(0)}}^T \end{pmatrix} (\boldsymbol{q}_1^{(0)} \cdots \boldsymbol{q}_m^{(0)}) = \mathcal{E}$$

に注目すると

$$\begin{pmatrix} {\boldsymbol{q}_1^{(0)}}^T \\ \vdots \\ {\boldsymbol{q}_m^{(0)}}^T \end{pmatrix} (\boldsymbol{q}_2^{(0)}\ \boldsymbol{q}_1^{(0)}\ \boldsymbol{q}_3^{(0)} \cdots \boldsymbol{q}_m^{(0)})$$

は (1,1),(2,2) 要素が (1,2), (2,1) に移動

$$\begin{pmatrix} {\boldsymbol{q}_1^{(0)}}^T \\ \vdots \\ {\boldsymbol{q}_m^{(0)}}^T \end{pmatrix} (\alpha\boldsymbol{q}_2^{(0)}\ -\alpha\boldsymbol{q}_1^{(0)}\ \alpha\boldsymbol{q}_3^{(0)} \cdots \alpha\boldsymbol{q}_m^{(0)})$$

は (1,2) が α, (2,1) が $-\alpha$ となる。加えて (i,i) が α となる

$$\begin{pmatrix} {\boldsymbol{q}_1^{(0)}}^T \\ \vdots \\ {\boldsymbol{q}_m^{(0)}}^T \end{pmatrix} (\boldsymbol{q}_2^{(0)}\ \boldsymbol{q}_1^{(0)}\ \boldsymbol{q}_3^{(0)} \cdots \boldsymbol{q}_m^{(0)})$$

は (1,1),(2,2) 要素が (1,2), (2,1) に移動

$$\begin{pmatrix} {\boldsymbol{q}_1}^{(0)^T} \\ \vdots \\ {\boldsymbol{q}_m}^{(0)^T} \end{pmatrix} (\alpha {\boldsymbol{q}_2}^{(0)} + \beta {\boldsymbol{q}_3}^{(0)} \ -\alpha {\boldsymbol{q}_1}^{(0)} + \beta {\boldsymbol{q}_2}^{(0)} \ \alpha {\boldsymbol{q}_3}^{(0)} + \beta {\boldsymbol{q}_1}^{(0)} \cdots \ \alpha {\boldsymbol{q}_m}^{(0)} + \beta {\boldsymbol{q}_m}^{(0)})$$

は

- (1,2) が α, (2,1) が $-\alpha$ となる。
- (1,3) が $-\beta$, (3,1) が $-\beta$ となる。
- 加えて (i,i) が $\alpha+\beta$ となる

命題 5
直交行列 Q と行列 A について，$Q^TA + A^TQ$ は次を満たす

1. 行列 $\mathcal{A}$ が対称かつ直行基底の定数倍，に加えて、基底の変換 (変換した方の片方は符号を変える) ことによって、対称行列になる。

ゆえに、

- $\mathcal{Q}^{(1)} = \mathcal{Q})0 + \delta\mathcal{Q}^{(1)}$ について
  1. $\left(\mathcal{Q}^{(1)}\right)^T \mathcal{Q}^{(1)} \equiv \mathcal{Q}^{(1)}\left(\mathcal{Q}^{(1)}\right)^T \equiv \mathcal{U} \pmod{I^2}$
  2. $\left(\delta\mathcal{Q}^{(1)}\right)^T \mathcal{Q}^{(0)} + \left(\delta\mathcal{Q}^{(0)}\right)^T \delta\mathcal{Q}^{(1)} = \mathrm{diag}(u_1, \ldots, u_\ell)$
  3. $\left(\delta\mathcal{Q}^{(1)}\right)^T \delta\mathcal{Q}^{(1)} \equiv \mathcal{O} \pmod{I^2}$

の存在性を示した。

- $w = 2$ のとき、 $\mathcal{Q}^{(2)} = \mathcal{Q}^{(1)} + \delta\mathcal{Q}^{(2)}$ について
  1. $\left(\mathcal{Q}^{(1)}\right)^T \mathcal{Q}^{(1)} \equiv \mathcal{Q}^{(1)}\left(\mathcal{Q}^{(1)}\right)^T \equiv \mathcal{U} \pmod{I^3}$
  2. $\left(\delta\mathcal{Q}^{(2)}\right)^T \mathcal{Q}^{(0)} + \left(\delta\mathcal{Q}^{(1)}\right)^T \delta\mathcal{Q}^{(1)} + \left(\delta\mathcal{Q}^{(0)}\right)^T \delta\mathcal{Q}^{(2)} = \mathrm{diag}(u_1, \ldots, u_\ell)$

  である。$\delta\mathcal{Q}^{(1)}$ は直交行列のため、$\left(\delta\mathcal{Q}^{(2)}\right)^T \mathcal{Q}^{(0)} + \left(\delta\mathcal{Q}^{(0)}\right)^T \delta\mathcal{Q}^{(2)} = \mathrm{diag}(u_1, \ldots, u_\ell)$ について確認すればよい ($w = 1$ と一緒の議論)

- $w = 2n - 1$ は同様の議論
- $w = 2n$ も同様の議論 ($\delta\mathcal{Q}^{(n)}$ は直交行列が追加)

多項式を要素に持つ行列の QR 分解: $w = 1$

以上をまとめることで，$\mathcal{S}$ を多項式 F, G からなる Sylvester 行列とするとき，

$$ {\mathcal{Q}^{(0)}}^T \delta\mathcal{S}^{(1)} \quad = \quad \left({\mathcal{Q}^{(0)}}^T \delta\mathcal{Q}^{(1)} \right) \mathcal{R}^{(0)} + \delta\mathcal{R}^{(1)} $$

の計算は次のように行うことができる

- ${\mathcal{Q}^{(0)}}^T \delta\mathcal{S}^{(1)} = \sum_{w_1+\ldots+w_\ell=1} \boldsymbol{u}^{\boldsymbol{\alpha}} {\mathcal{Q}^{(0)}}^T \delta\tilde{\mathcal{S}}^{(1)}$ with $\delta\tilde{\mathcal{S}}^{(1)} \in \mathbb{F}^{m\times m}$ を $\mathcal{R}^{(0)}$ で消去するようなことを考える．$\delta\mathcal{R}^{(1)}$ は残った部分
- $\mathcal{R}^{(0)}$ による消去を次のように実現
  - $\mathcal{R}^{(0)}$ を利用して、右辺を上三角行列にする。
    - 直交行列の定数倍によって削除 $\delta\tilde{\mathcal{Q}}^{(1)}$ を得る。
    - $\mathcal{Q}^{(0)}$ で基底変換
- w のとき，同様の考えによって計算を進めることが可能である．

$$ \begin{aligned} \mathcal{S} &\equiv \left(\mathcal{Q}^{(w-1)} + \delta\mathcal{Q}^{(w)} \right) \left(\mathcal{R}^{(w-1)} + \delta\mathcal{R}^{(w)} \right) \pmod{I^{w+1}} \\ \delta\mathcal{S}^{(w)} &= \mathcal{Q}^{(0)} \delta\mathcal{R}^{(w)} + \sum_i \delta\mathcal{Q}^{(i)} \delta\mathcal{R}^{(w-i)} + \delta\mathcal{Q}^{(w)} \mathcal{R}^{(0)} \\ \delta\mathcal{S}^{(w)} - \sum_i \delta\mathcal{Q}^{(i)} \delta\mathcal{R}^{(w-i)} &= \mathcal{Q}^{(0)} \delta\mathcal{R}^{(w)} + \delta\mathcal{Q}^{(w)} \mathcal{R}^{(0)} \end{aligned} $$

より

$$ {\mathcal{Q}^{(0)}}^T \left(\delta\mathcal{S}^{(w)} - \sum_i \delta\mathcal{Q}^{(i)} \delta\mathcal{R}^{(w-i)} \right) \quad = \quad \left({\mathcal{Q}^{(0)}}^T \delta\mathcal{Q}^{(w)} \right) \mathcal{R}^{(0)} + \delta\mathcal{R}^{(w)} $$

  - (左辺) を $\mathcal{R}^{(0)}$ で消去することで $\delta\mathcal{R}^{(w)}$ と $\delta\mathcal{Q}^{(w)}$ が得られる．

多項式を要素に持つ行列の QR 分解: w

次の手順で計算が可能であることが示唆される．

- F, G の Sylvester 行列を構成
- $\mathcal{S} = \mathcal{Q}^{(0)} \mathcal{R}^{(0)}$
- for 全次数 from 1 to w do

$$ {\mathcal{Q}^{(0)}}^T \left(\delta\mathcal{S}^{(w)} - \sum_i \delta\mathcal{Q}^{(i)} \delta\mathcal{R}^{(w-i)} \right) \quad = \quad \left({\mathcal{Q}^{(0)}}^T \delta\mathcal{Q}^{(w)} \right) \mathcal{R}^{(0)} + \delta\mathcal{R}^{(w)} $$

  - 主要素の消去 $\left({\mathcal{Q}^{(0)}}^T \delta\mathcal{Q}^{(w)} \right) \to \delta\mathcal{R}^{(0)}$
  - $\delta\mathcal{Q}^{(w)}$ の計算

4 まとめ

本稿では，QR 分解の拡張を行った．拡張によって近似 GCD の計算ができる可能性を示したが，アルゴリズムとなっていない．アルゴリズム示し，計算例，実行時間を提示することが今後の課題である．h

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] 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.

[4] S. Gao, E. Kaltofen, J. P. May, Z. Yang and L. Zhi, *Approximate factorization of multivariate polynomials via differential equations*, Proc. of ISSAC'04, ACM Press, 2004, 167–174.

[5] 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.

[6] M. Sanuki. *Computing multivariate approximate GCD based on Barnett's theorem*, Proc. of Symbolic-Numeric Computation 2009 (SNC 2009), 2009, 149–157.

[7] M. Sanuki and T. Sasaki, *Computing approximate GCDs in ill-conditioned cases*, International Workshop of Symbolic-Numeric Computation 2007 (SNC2007), ACM Press, 2007, 170-179, 25–27.

[8] M. Sanuki. *Computing multivariate approximate GCD based on Barnett's theorem*, Proc. of Symbolic-Numeric Computation 2009 (SNC 2009), 2009, 149-157, 2009.

[9] M. Sanuki, A Stable Computation of Multivariarte Apporximate GCD Based on SVD and Lifting Technique, SCSS2024 (10th International Symposium on Symbolic Computation in Software Science), 2024. (electronic publishing)

[10] T. Sasaki and S. Yamaguchi, *An analysis of cancellation error in multivariate Hensel construction with floating-point number arithmetic*, Proc. of ISSAC' 98, ACM Press, 1998, 1 – 8.

[11] Z. Zeng and B. H. Dayton, *The approximate GCD of inexact polynomials part II: A multivariate algorithm*, Proc. of ISSAC'04, ACM Press, 2004, 320–327.

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