数理解析研究所講究録
1138巻 2000年 1-12

二変数多項式の近似因数分解 ～許容度の下限と既約判定～

筑波大学数学研究科　長坂　耕作(Kosaku Nagasaka) *

概　要

二変数多項式の近似因数分解において，許容度内で出来る限り分解したことを保証することは難しい．一方，一変数の近似 GCD 計算においては，許容度内での GCD の最大次数を保証するアルゴリズムが (条件はあるものの) 提案されている．本稿では，それらのアプローチを踏襲し数値的に近似因数分解の可能性について，分解に必要な許容度を，佐々木ら [SSKS91, SSH92, SS93] そして筆者ら [NS98] により改良されたベキ級数展開した根の線形従属性を利用したアルゴリズムから導くと共に，根の係数行列の特異値分解 (SVD) により与えられた許容度内での根の摂動上限を導き，その可能性について議論する．

1　はじめに

多くの係数体上の多項式の因数分解について，これまでに多くの研究がされている．しかしながら，入力多項式の係数が不正確である場合に有用な近似因数分解についての研究は余り進んでいない．近年の研究では，厳密な多項式の既約判定の自然な拡張として，入力多項式の係数の近傍での既約性の研究 [Kal95] や，近似 GCD の様に最適化を使用した近似因数分解 [HK99] などは行われているものの，効果的な近似因数分解アルゴリズムの研究はほとんど行われていない．一方，もう一つの重要な代数計算である GCD については，近年の研究により様々なアルゴリズムが提案 [CGTW95, EGL97, P98] されている．本稿では，近似 GCD 計算で使われる特異値分解 (SVD) に注目し，二変数多項式の根のベキ級数展開における係数の摂動上限を導き，近似因数分解を意識した因数分解アルゴリズムである [SSKS91, SSH92, SS93, NS98] の自然な拡張として，与えられた許容度内での既約判定について述べる．

まず，本稿で使用する記号について定義しておく．

- $\|P\|$: 多項式 P の 2 ノルム;
  $\|P\| = (\sum_{i=0}^{n}\sum_{j=0}^{d}|c_{i,j}|^2)^{\frac{1}{2}}$, $P(x,y)=\sum_{i=0}^{n}\sum_{j=0}^{d}c_{i,j}y^jx^i$.

*nagasaka@math.tsukuba.ac.jp

- $\|A\|_2$: 行列 $A(\in \mathbb{C}^{n\times m})$ の 2 ノルム;
  $\|A\|_2 = \sup_{x\neq 0} \|Ax\|_2 \,/\, \|x\|_2,\ x \in \mathbb{C}^n,\ \|x\|_2 = (\sum_{k=1}^{n} |x_i|^2)^{\frac{1}{2}}$.
- $\sigma_i(M)$: 行列 M の i 番目に大きい特異値.
- E_i : [NS98] で与えられた因子多項式の y に関する次数上限.
- $\lfloor F \rfloor_e$: F の各単項式のうち，y の次数が e 以上の項の和.
- $\lceil F \rceil^{e'}$: F の各単項式のうち，y の次数が e' 以下の項の和.
- $[F]_e^{e'}$: $\lceil \lfloor F \rfloor_e \rceil^{e'}$ を表す.

なお，全ての数値例は C 版 GAL に CLAPACK-D をリンクしたシステム上で求めたものであり，各数値は 16 桁の精度を持つ．紙面の都合上その全ての桁は掲載していないため，各数値は実際のものとは多少異なる.

1.1 近似因数分解

定義 1 F, G, H を $\mathbb{C}$ 上の多変数多項式，ε を微小正数とする．F が許容度 ε で近似因数分解可能であるとは，次のような多項式 Δ_F が存在することと定義する.

$$F = GH + \Delta_F,\ \ \|\Delta_F\| \,/\, \|F\| = \varepsilon \ll 1. \tag{1}$$

定義 2 $\mathbf{v}_1, \ldots, \mathbf{v}_n \in \mathbb{C}^l,\ l \geq n$ とし，$R_1 : a_1\mathbf{v}_{i_1} + \cdots + a_r\mathbf{v}_{i_r} = 0$ と $R_2 : b_1\mathbf{v}_{j_1} + \cdots + b_s\mathbf{v}_{j_s} = 0$ を $\mathbf{v}_1, \ldots, \mathbf{v}_n$ の間の線形従属関係 *(*ここで，$a_i, b_j \in \mathbb{C}$ である*)* とする．このとき，$\{i_1, \ldots, i_r\} \bigcap \{j_1, \ldots, j_s\} = \emptyset$ であれば R_1 と R_2 は ***disjoint*** であると言う.

近似因数分解を考慮したアルゴリズム [SSKS91, SSH92, SS93, NS98] について，次の F に関して説明する.

$$F = x^n + f_{n-1}x^{n-1} + \cdots + f_0,\ \ f_i \in \mathbb{C}[y, \ldots, z]\ (i = n-1, \ldots, 0). \tag{2}$$

アルゴリズム **3** (因数分解アルゴリズム)

Step 1 $F(x, c_y, \ldots, c_z)$ が無平方であるような数 $c_y, \ldots, c_z$ を定める.

Step 2 何らかの数値算法にて $F(x, c_y, \ldots, c_z)$ の根 $\zeta_1, \ldots, \zeta_n$ を求める.

Step 3 以下を満たす $F(x, y, \ldots, z)$ の根に関するベキ級数展開を行う.

$$F(x, y, \ldots, z) \equiv (x - \varphi_1(y, \ldots, z)) \cdots (x - \varphi_n(y, \ldots, z)) \pmod{S^{E_n+1}}.$$

Step 4 各根のベキ乗 $\lceil\varphi_1^i\rceil^{E_n},\ldots,\lceil\varphi_n^i\rceil^{E_n},\ i=1,\ldots,n$ を求める.

Step 5 $M_i\ (1\le i\le n)$ を j 番目の行が $[\varphi_j^i]_{E_i+1}^{E_n}$ の係数ベクトルである行列と定義し，パラメータ $\lambda_2,\ldots,\lambda_n$ を含む行列 $M(\lambda_2,\ldots,\lambda_n)=M_1+\lambda_2M_2+\cdots+\lambda_nM_n$ の次のような線形関係を求め，*disjoint* な関係に変換する.

$$[\varphi_{j_1}^i+\cdots+\varphi_{j_r}^i]_{E_i+1}^{E_n}=0,\ \ i=1,\ldots,n.$$

Step 6 各々の *disjoint* な線形関係に対応する既約因子 $G\equiv(x-\varphi_{j_1})\cdots(x-\varphi_{j_r})\pmod{S^{E_n+1}}$ を一次因子の積として求める.

上記アルゴリズムは次の定理に基づいている.

定理 4 $F=(x-\varphi_1)\cdots(x-\varphi_n)$ とし，G,H を次式のようにおく.

$$\begin{cases} G^{(k)}=\lceil(x-\varphi_1)\cdots(x-\varphi_m)\rceil^k, \\ H^{(k)}=\lceil(x-\varphi_{m+1})\cdots(x-\varphi_n)\rceil^k, \end{cases} \tag{3}$$

このとき，次の A,B は同値である.

$$A\ :\ [\varphi_1^i+\cdots+\varphi_m^i]_{E_i+1}^{E_n}=0\ \ (i=1,\ldots,m), \tag{4}$$

$$B\ :\ F=G^{(E_n)}H^{(E_n)}. \tag{5}$$

上記アルゴリズムでは因数分解すべき多項式をモニックと仮定しているが，モニックでない多項式に対しても同様の因数分解が可能である [NS98].

1.2 近似因数分解に必要な許容度の下限

定義 5 F,G,H を $\mathbb{C}$ 上の多変数多項式，ε を微小正数とする．F が許容度 ε で近似因数分解不可能であるとは，次のような多項式 Δ_F が存在しないことと定義する.

$$F=GH+\Delta_F,\ \ \|\Delta_F\|\ /\ \|F\|=\varepsilon\ll 1, \tag{6}$$

上記アルゴリズム 3 と定理 4 より次の系が導かれる.

系 6 $M(\lambda_2,\ldots,\lambda_n)$ のランクが $n-1$ であるとき，F は既約である．また，逆も成り立つ.

注意 7 系 *6* では，パラメータを伴った行列 M のランクと与式 F の既約性についてのみ述べているが，行列 M の線形独立な n 個の行列のうち一つでもランクが $n-1$ であれば F は既約と判定出来る．本稿では根との関係が最も単純な M_1 にのみ注目する.

さらに次の補題を紹介しておく．

補題 8 行列 $A, B \in \mathbb{C}^{m\times n}$ に対して次が成り立つ．*[GC96, Theorem 2.5.3]*

$$k < r = \mathrm{rank}(A),\ \sigma_{k+1} = \min_{\mathrm{rank}(B)=k} \|A - B\|_2 .$$

これらの系と補題より，既約多項式が近似因数分解により分解されるには，そのベキ級数展開された根が，係数行列 M の最小特異値以上のノルム程度の摂動を必要とすることがわかる．このことを次の例で示す．

例 1 既約な多項式 $F = (x^2 + yx + 2y - 1)(x^3 + y^2x - y + 7) + 0.2x$ の因数分解を考える．本稿で紹介したアルゴリズムに基づき根のベキ級数展開を行うと，次の 5 つの根を得る．(紙面の都合上、桁は短くしてある)

$$\begin{aligned}
\varphi_1 = {} & -1.8996 + 0.0930y + 0.1818y^2 + 0.0085y^3 + 0.0011y^4 - 0.0002y^5 - 0.0005y^6, \\
\varphi_2 = {} & -1.0170 + 0.4930y + 0.3653y^2 + 0.3652y^3 + 0.4292y^4 + 0.5600y^5 + 0.7788y^6, \\
\varphi_3 = {} & 0.9645 - 1.6550i - (0.0420 - 0.0732i)y - (0.0938 + 0.1503i)y^2 - (0.0076 + \\
& 0.0033i)y^3 + (0.0023 + 0.0027i)y^4 + (0.0032 - 0.0020i)y^5 - (0.001 + 0.004i)y^6, \\
\varphi_4 = {} & 0.9645 + 1.6550i - (0.0420 + 0.0732i)y - (0.0938 - 0.1503i)y^2 - (0.0076 - \\
& 0.0033i)y^3 + (0.0023 - 0.0027i)y^4 + (0.0032 + 0.0020i)y^5 - (0.001 - 0.004i)y^6, \\
\varphi_5 = {} & 0.9875 - 1.5020y - 0.3596y^2 - 0.3584y^3 - 0.4349y^4 - 0.5661y^5 - 0.7762y^6.
\end{aligned}$$

次式は，この根に対応する行列 M_1 を表す．(即ち，y の次数が 2 次から 6 次の部分)

$$\begin{pmatrix}
0.1818 & 0.0085 & 0.0011 & -0.0002 & -0.0005 \\
0.3653 & 0.3652 & 0.4292 & 0.5600 & 0.7788 \\
-0.094 - 0.150i & -0.008 - 0.003i & 0.002 + 0.003i & 0.003 - 0.002i & -0.001 - 0.004i \\
-0.094 + 0.150i & -0.008 + 0.003i & 0.002 - 0.003i & 0.003 + 0.002i & -0.001 + 0.004i \\
-0.3596 & -0.3584 & -0.4349 & -0.5661 & -0.7762
\end{pmatrix}$$

そこで，この行列の特異値を計算すると，大きい順に $1.65877, 0.29241, 0.01091, 0.00624$ となり，F が既約なことからもわかるように行列のランクは 4 である．補題 8 より，与式 F が可約となるためには行列 M_1 のランクが 4 未満になるように，行列に変化を加える必要がある．つまり，最低でも行列のノルムが 0.00624 程度になる摂動を根はしなくてはならない． ◁

上記例からわかるように，与えられた許容度内での保証付き近似因数分解を行うことは難しいものの，根の摂動上限を計算することにより，与式が許容度内で既約であることを示すことは可能である．以下の章では根の摂動上限について議論し，許容度内での近似因数分解可能性について述べる．

実際に F の既約因子を求めるには，M_1 だけでなくパラメータを含む行列 M に関しての計算を必要とするが，M_i の要素は M_1 の要素に複雑に依存しているため，根の摂動と $i>1$ なる行列 M_i の特異値との関係は現在のところ明らかでない部分が多く，今後の課題である．(安易な拡張を行っても，M_1 単独の利用に比べて良い結果は得られないことが定理 4 よりわかる．実際の実験例もそれを示唆している)

2 根の摂動上限

この章では，二変数多項式のベキ級数展開された根の摂動について論ずる．与式の係数の変化が，ベキ級数展開された根にどの程度影響するかを見積もるため，Hensel 構成により展開された根を次のように定義する．

$$
\begin{aligned}
&F(x,y)=x^n+\textstyle\sum_{j=0}^{d}\sum_{l=0}^{n-1} f_{j,l}y^jx^l, n=\deg(F),\ F\in\mathbb{C}[x,y],\\
&G(x,y)=x^{n-1}+\textstyle\sum_{j=0}^{d}\sum_{l=0}^{n-2} g_{j,l}y^jx^l, H(x,y)=x+\sum_{j=0}^{d} h_{j,0}y^j,\\
&G,H\in\mathbb{C}\{y\}[x], F(x,y)\equiv G(x,y)H(x,y) \pmod{y^{k+1}}.
\end{aligned}
$$

ここで，便宜上摂動上限を見積もる根を $H(x,y)$ と一次因子の形で表していることに注意されたい．$G(x,y)$ は，H に含まる根以外の根に対応する一次因子の積である．この注目する根および両因子 H と G は，y に関して k 次までベキ級数展開されていることを上記定義は示している．

問題 9 与えられた微小正数 $\varepsilon\ll 1$ に対する下記を満たす上限 B を見積もりたい．

$$
\begin{aligned}
&\tilde{F}(x,y)\equiv\tilde{G}(x,y)\tilde{H}(x,y) \pmod{y^{k+1}},\ \tilde{F}=F+\Delta_F,\\
&\|\Delta_F\| \,/\, \|F\|\leq\varepsilon,\ \deg(\Delta_F)<\deg(F),\ B=\max\{\|H-\tilde{H}\|\}.
\end{aligned}
$$

この B は，許容度 ε での多項式 F のベキ級数展開された根の摂動上限である．

なお，根の入れ替わりを避け，根の摂動先を唯一なものに限定するため，与式 $F(x,y)$ および $F(x,0)$ は，許容度 ε で近似無平方であると仮定する．

2.1 Hensel 構成による上限

Hensel 構成による上限の見積もりは，余り良い値を与えない．このことを示すために，根のベキ級数展開 $\varphi_i(y,\ldots,z)$ $(i=1,\ldots,n)$ に与式の係数の変化がどの程度影響を与えるかを Hensel 構成の手順に沿って計算する．まず，次のように初期因子をおく．

$$
F_1^{(0)}=x-\zeta_1,\ \ldots,\ F_n^{(0)}=x-\zeta_n. \tag{7}
$$

各構成で使用する Moses-Young の補間式 $w_1^{(l)},\ldots,w_n^{(l)}$ $(l=0,\ldots,n-1)$ を求める．

$$w_i^{(l)}=\frac{\zeta_i^l}{\prod_{j=1,\neq i}^{n}(\zeta_i-\zeta_j)}. \tag{8}$$

これらの $w_i^{(l)}$ $(i=1,\ldots,n)$ は，次式を満たす．

$$w_1^{(l)}\frac{F_1^{(0)}\cdots F_n^{(0)}}{F_1^{(0)}}+\cdots+w_n^{(l)}\frac{F_1^{(0)}\cdots F_n^{(0)}}{F_n^{(0)}}=x^l. \tag{9}$$

$k-1$ 次まで Hensel 構成を行ったと仮定し，$F\equiv F_1^{(k')}\cdots F_n^{(k')}(\mathrm{mod}\ y^{k'+1})$ かつ $F_i^{(k')}\equiv F_i^{(0)}$ $(\mathrm{mod}\ y)$ を満たす真の因子を $F_1^{(k')},\ldots,F_n^{(k')}$, $k'=0,\ldots,k-1$ とおき，それぞれの k' 回目の因子に含まれる摂動を $e_{k'}$ とする．このとき，k 次の因子 $F_1^{(k)},\ldots,F_n^{(k)}$ は次式で計算される．

$$F_i^{(k)}=F_i^{(k-1)}+\sum_{l=0}^{n-1}w_i^{(l)}\tilde{f}_l^{(k)},\quad i=1,\ldots,n. \tag{10}$$

ここで，$\tilde{f}_0^{(k)},\ldots,\tilde{f}_{n-1}^{(k)}$ は次を満たす．

$$F-F_1^{(k-1)}\cdots F_n^{(k-1)}\equiv\tilde{f}_{n-1}^{(k)}x^{n-1}+\cdots+\tilde{f}_0^{(k)}\pmod{y^{k+1}}. \tag{11}$$

よって，k 回目の因子に含まれる摂動は次のようになる．

$$e_k\equiv\varepsilon F-\sum_{i=1}^{n}\binom{n}{i}e_{k-1}^i\,\|F^{(k-1)}\|^{n-i}\pmod{y^{k+1}}. \tag{12}$$

以上により単純に見積もっても $e_k=\varepsilon+ne_{k-1}$, $e_0=\varepsilon$ より，$e_k=\frac{\varepsilon(n^{k+1}-1)}{n-1}$ なる関係を得る．

例 2 では，この Hensel 構成による摂動上限が過大な見積もりを与える上，y の次数が上がるにつれ急速に膨張するため実用的でないことを示す．

例 2 例 1 の多項式 $F=(x^2+yx+2y-1)(x^3+y^2x-y+7)+0.2x$ に上記摂動上限を適用してみる．仮に許容度を $\varepsilon=0.000001$ とすれば，$(e_2,e_3,e_4,e_5,e_6)=(0.000031, 0.000156, 0.000781, 0.003906, 0.019531)$ と見積もられる．この値の意味するところは，上記許容度内で例 1 の行列 M_1 は最大でノルムが 0.0445731 程度の摂動をするということであり，F の近似因数分解可能性を否めない，ということだ．しかしながら，以下の章で述べるようにこの許容度内で F は既約である．このように上記上限では F を近似因数分解不可能と判定出来ないため，より良い摂動上限を求める必要がある． ◁

2.2 反復計算による摂動上限

Hensel 構成では初期因子に含まれる摂動が，次数を上げるにつれ大きく響いて来る．これは，その構成手法からは避けられないことであるが，実用的な摂動上限からは程遠い．そこで，既に求めた $F \equiv GH$ なる関係から $F+\Delta_F \equiv (G+\Delta_G)(H+\Delta_H)$ を満たす各々の摂動項 Δ_G, Δ_H を求めることを考える．

上記関係式より $\Delta_F \equiv G\Delta_H + H\Delta_G + \Delta_G\Delta_H$ を得るが，$\varepsilon \ll 1$ であり，ほとんどの場合 $\Delta_G\Delta_H \ll G\Delta_H + H\Delta_G$ が成り立つ．よって，$\tilde{G} = G+\Delta_G$, $\tilde{H} = H+\Delta_H$ を $\tilde{F}, G, H$ から求める，次のような反復計算が導き出される．

反復計算の初期因子として，$G^{(0)}(x,y) = G(x,y)$ と $H^{(0)}(x,y) = H(x,y)$ をおく．$G^{(i)}(x,y), H^{(i)}(x,y)$ は，次式を満たす $\tilde{G}, \tilde{H}$ それぞれの i 番目の近似因子を表す．

$$
\begin{aligned}
&\tilde{F}(x,y) - G^{(i)}H^{(i)} \equiv \textstyle\sum_{j=0}^{k}\sum_{l=0}^{n-1} \Delta_{f_{j,l}}^{(i)} y^j x^l \pmod{y^{k+1}},\\
&G^{(i)}(x,y) = G^{(i-1)}(x,y) + \Delta_G^{(i)} = x^{n-1} + \textstyle\sum_{j=0}^{k}\sum_{l=0}^{n-2} g_{j,l}^{(i)} y^j x^l,\\
&H^{(i)}(x,y) = H^{(i-1)}(x,y) + \Delta_H^{(i)} = x + \textstyle\sum_{j=0}^{k} h_{j,0}^{(i)} y^j,\\
&\Delta_G^{(i)} = \textstyle\sum_{j=0}^{k}\sum_{l=0}^{n-2} \Delta_{g_{j,l}}^{(i)} y^j x^l, \quad \Delta_H^{(i)} = \textstyle\sum_{j=0}^{k} \Delta_{h_{j,0}}^{(i)} y^j.
\end{aligned}
$$

定義 10 行列 $\Delta_F^{(i)}$, $\Delta^{(i)}$ を次のように定義する．

$$
\begin{aligned}
\Delta_F^{(i)} &= (\Delta_{f_{0,0}}^{(i)}, \Delta_{f_{0,1}}^{(i)}, \cdots, \Delta_{f_{k,n-1}}^{(i)})^t,\\
\Delta^{(i)} &= (\Delta_{h_{0,0}}^{(i)}, \cdots, \Delta_{h_{k,0}}^{(i)}, \Delta_{g_{0,0}}^{(i)}, \Delta_{g_{0,1}}^{(i)}, \cdots, \Delta_{g_{k,n-2}}^{(i)})^t.
\end{aligned}
$$

定義 11 ブロック行列 $M^{(i)}$ を次のように定義する．

$$
M^{(i)} = \begin{pmatrix}
G_0^{(i)} & & & & & H_0^{(i)} & & & & \\
G_1^{(i)} & G_0^{(i)} & & & & H_1^{(i)} & H_0^{(i)} & & & \\
\vdots & G_1^{(i)} & \ddots & & & \vdots & H_1^{(i)} & \ddots & & \\
G_{k-1}^{(i)} & \vdots & \ddots & G_0^{(i)} & & H_{k-1}^{(i)} & \vdots & \ddots & H_0^{(i)} & \\
G_k^{(i)} & G_{k-1}^{(i)} & \cdots & G_1^{(i)} & G_0^{(i)} & H_k^{(i)} & H_{k-1}^{(i)} & \cdots & H_1^{(i)} & H_0^{(i)}
\end{pmatrix}.
$$

ここで，$G_j^{(i)}$ と $H_j^{(i)}$ は，$\lambda = 1\ (j=0)$, $\lambda = 0\ (j \neq 0)$ なる次式のブロック因子である．

$$
G_j^{(i)} = \begin{pmatrix}
g_{j,0}^{(i)}\\ g_{j,1}^{(i)}\\ \vdots\\ g_{j,n-3}^{(i)}\\ g_{j,n-2}^{(i)}\\ \lambda
\end{pmatrix}, \quad
H_j^{(i)} = \begin{pmatrix}
h_{j,0}^{(i)} & & & \\
\lambda & h_{j,0}^{(i)} & & \\
 & \lambda & \ddots & \\
 & & \ddots & h_{j,0}^{(i)}\\
 & & & \lambda
\end{pmatrix}.
$$

なお，行列 $M^{(i)}$ の大きさは $n(k+1) \times n(k+1)$ となる．

行列 $M^{(i)}$ は，大抵の多項式に対し特異な行列とならないことが簡単に証明出来るため，本稿では簡単のため，行列 $M^{(i)}$ は特異でないと仮定する．よって，特異値分解を用いて次のように $M^{(i)}$ の逆行列を表現出来る．

$$M^{(i)^+} = V^{(i)}\Sigma^{(i)^+}U^{(i)^T}, \quad M^{(i)} = U^{(i)}\Sigma^{(i)}V^{(i)^T}. \tag{13}$$

定義より，

$$M^{(i-1)}\Delta^{(i)} = \Delta_F^{(i-1)} \ (i = 1, 2, \cdots). \tag{14}$$

つまり，$i-1$ 番目の近似因子より i 番目の因子を次式で計算できる．

$$\Delta^{(i)} = M^{(i-1)^+}\Delta_F^{(i-1)}. \tag{15}$$

以下で議論する条件のもとで，$\tilde{G}$ と $\tilde{H}$ は式 (15) の反復計算を無限に繰り返すことで表現可能である．

補題 12 任意の行列 A, E $(\in \mathbb{C}^{n\times m})$ に対し，以下が成り立つ．[1)]

$$|\sigma_\kappa(A+E) - \sigma_\kappa(A)| \leq \|E\|_2 . \tag{16}$$

補題 13 行列の 2 ノルムは次の性質を持つ．[2)]

$$A \in \mathbb{C}^{n\times m}, B \in \mathbb{C}^{n\times r}, C \in \mathbb{C}^{r\times m},\ A = BC,\ \|A\|_2 = \|BC\|_2 \leq \|B\|_2\|C\|_2 . \tag{17}$$

定義 14 新たに以下の記号を導入する．

$$s_i = c\,\|\Delta_F^{(i)}\|_2\,/\sigma_{(i)}^2,\ \ t_i = \sigma_{(i+1)}/\sigma_{(i)},\ \ c = \sqrt{k+1},\ \ \sigma_{(i)} = \sigma_{n(k+1)}(M^{(i)}). \tag{18}$$

補題 15 $\Delta_F^{(i)}, \Delta^{(i)}, c$ は次式を満たす．

$$\|\Delta_F^{(i)}\|_2 \leq c\,\|\Delta^{(i)}\|_2^2 . \tag{19}$$

[1)] see [GC96, Corollary 8.6.2].

[2)] see [GC96, 2.3.1].

証明 $\delta G^{(i)}$ と $\delta H^{(i)}$ を次のような行列とする．

$$\delta G^{(i)} = \begin{pmatrix} \delta G_0^{(i)} & & & & \\ \delta G_1^{(i)} & \delta G_0^{(i)} & & & \\ \vdots & \delta G_1^{(i)} & \ddots & & \\ \delta G_{k-1}^{(i)} & \vdots & \ddots & \delta G_0^{(i)} & \\ \delta G_k^{(i)} & \delta G_{k-1}^{(i)} & \cdots & \delta G_1^{(i)} & G_0^{(i)} \end{pmatrix}, \tag{20}$$

$$\delta G_j^{(i)} = \begin{pmatrix} \Delta_{g_{j,0}}^{(i)} \\ \Delta_{g_{j,1}}^{(i)} \\ \vdots \\ \Delta_{g_{j,n-3}}^{(i)} \\ \Delta_{g_{j,n-2}}^{(i)} \end{pmatrix}, \quad \delta H^{(i)} = \begin{pmatrix} \Delta_{h_{0,0}}^{(i)} \\ \Delta_{h_{1,0}}^{(i)} \\ \vdots \\ \Delta_{h_{k-1,0}}^{(i)} \\ \Delta_{h_{k,0}}^{(i)} \end{pmatrix}. \tag{21}$$

ここで，それぞれの行列の大きさは $(n-1)(k+1)\times(k+1)$ と $(k+1)\times 1$ である．よって，補題 13 より

$$\begin{aligned} \|\Delta_F^{(i)}\|_2 &= \|\delta G^{(i)}\delta H^{(i)}\|_2 \\ &\le \|\delta G^{(i)}\|_2 \|\delta H^{(i)}\|_2 \\ &\le \sqrt{k+1}\,\|\Delta^{(i)}\|_2 \|\Delta^{(i)}\|_2 \\ &= c\,\|\Delta^{(i)}\|_2^2 . \end{aligned} \tag{22}$$

∎

補題 16 $\Delta_F^{(i)}$ と s_i は次式を満たす．

$$\|\Delta_F^{(i)}\|_2 \le \Pi_{j=0}^{i-1} s_j \,\|\Delta_F^{(0)}\|_2 \quad (i>0). \tag{23}$$

証明 式 (15) と補題 15 の関係を用いることで，数学的帰納法により証明される．そこで，$i=1,2,\cdots,\kappa$ に関して補題は成り立つと仮定し，$i=\kappa+1$ について証明する．($i=1$ の場合は明らかである)

$$\begin{aligned} \|\Delta_F^{(\kappa+1)}\|_2 &\le c\,\|\Delta^{(\kappa+1)}\|_2^2 \\ &\le c\,\|\Delta_F^{(\kappa)}\|_2^2 / \sigma_{(\kappa)}^2 \\ &= s_\kappa\,\|\Delta_F^{(\kappa)}\|_2 \\ &\le s_\kappa(\Pi_{j=0}^{\kappa-1} s_j\,\|\Delta_F^{(0)}\|_2) \\ &= \Pi_{j=0}^{\kappa} s_j\,\|\Delta_F^{(0)}\|_2 . \end{aligned}$$

∎

補題 17 $s_i<1$ ならば $\|\Delta_F^{(i+1)}\|_2 < \|\Delta_F^{(i)}\|_2$ が成り立つ．

証明 補題 16 の証明より明らか. ∎

定理 18 $0 \leq s_0 \leq \frac{3-\sqrt{5}}{2}$ (<1) ならば $0 \leq s_i \leq s_j$ $(i \geq j \geq 0)$ が成り立つ.

証明 単調減少を示すため, $i = 0, 1, 2, \cdots, \kappa$ に対して定理が成り立つと仮定し, $0 \leq s_{\kappa+1} \leq s_\kappa$ を示す.

仮定より $0 \leq s_\kappa \leq \frac{3-\sqrt{5}}{2}$ (<1), つまり $0 \leq s_\kappa \leq (1-s_\kappa)^2$ が成り立つ. これは, $z = \frac{3-\sqrt{5}}{2}, \frac{3+\sqrt{5}}{2}$ が $z = (1-z)^2$ を満たすからである. さらに, 補題 12 より t_κ は次のように変形出来る.

$$\begin{aligned} t_\kappa &= \sigma_{(\kappa+1)}/\sigma_{(\kappa)} \\ &= (\sigma_{(\kappa+1)} - \sigma_{(\kappa)})/\sigma_{(\kappa)} + 1 \\ &\geq 1 - c \left\|\Delta^{(\kappa+1)}\right\|_2 / \sigma_{(\kappa)} \\ &\geq 1 - c \left\|\Delta_F^{(\kappa)}\right\|_2 / \sigma_{(\kappa)}^2 \\ &= 1 - s_\kappa \ (>0). \end{aligned}$$

よって, $0 \leq s_\kappa \leq (1-s_\kappa)^2 \leq t_\kappa^2$ かつ $0 \leq s_\kappa^2/t_\kappa^2 \leq s_\kappa$ が成り立つので, 補題 16 の証明のように $s_{\kappa+1}$ を次のように変形出来る.

$$\begin{aligned} 0 \leq s_{\kappa+1} &= c \left\|\Delta_F^{(\kappa+1)}\right\|_2 / \sigma_{(\kappa+1)}^2 \\ &\leq c s_\kappa \left\|\Delta_F^{(\kappa)}\right\|_2 / \sigma_{(\kappa+1)}^2 \\ &= c s_\kappa \left\|\Delta_F^{(\kappa)}\right\|_2 / (t_\kappa^2 \sigma_{(\kappa)}^2) \\ &= s_\kappa^2/t_\kappa^2 \\ &\leq s_\kappa. \end{aligned}$$

以上により, $0 \leq s_i \leq s_j$ $(i \geq j \geq 0)$ を得る. ∎

系 19 $s_0 \leq \frac{3-\sqrt{5}}{2}$ (<1) ならば, 上記の反復アルゴリズムは収束する.

定理 20 $s_0 \leq \frac{3-\sqrt{5}}{2}$ (<1) ならば, $B \leq \sum_{k=1}^{\infty} s_0^{k-1}/(1-s_0)^{k-1} \left\|\Delta_F^{(0)}\right\|_2 / \sigma_{(0)}$ が成り立つ.

証明 補題 16 と定理 18 より以下のように変形し, 残差項の和を取ることで B の上限を得る.

$$\begin{aligned} \left\|\Delta^{(k)}\right\|_2 &\leq \left\|\Delta_F^{(k-1)}\right\|_2 / \sigma_{(k-1)} \\ &= \left\|\Delta_F^{(k-1)}\right\|_2 / t_{k-2}\sigma_{(k-2)} \\ &= \left\|\Delta_F^{(k-1)}\right\|_2 / \Pi_{i=0}^{k-2} t_i \sigma_{(0)} \\ &\leq \Pi_{i=0}^{k-2} s_i \left\|\Delta_F^{(0)}\right\|_2 / \Pi_{i=0}^{k-2} t_i \sigma_{(0)} \\ &\leq \Pi_{i=0}^{k-2} s_i/(1-s_i) \left\|\Delta_F^{(0)}\right\|_2 / \sigma_{(0)} \\ &\leq s_0^{k-1}/(1-s_0)^{k-1} \left\|\Delta_F^{(0)}\right\|_2 / \sigma_{(0)}. \end{aligned}$$

さらに定理 20 より次の系が導かれる．

系 21 許容度を ε としたとき，$M_1 = M(0,\ldots,0)$ の摂動の上限は $\sqrt{\sum_{i=1}^{n} B_i^2}$ で与えられる．ここで，B_i は F の i 番目の根の y に関して E_n 次までの摂動の上限を表す．

例 3 例 1 の多項式 $F = (x^2+yx+2y-1)(x^3+y^2x-y+7)+0.2x$ を許容度 0.000001 で変化させたときに，上述の定理を用いて根の摂動の上限を求める．$\|\Delta_F\| \,/\, \|F\| \leq 0.000001$ より初期の残差 $\|\Delta_F^{(0)}\| \leq 0.000001\ \|F\| = 0.0000198504$ となり，それぞれの根の摂動上限は，$0.00009333, 0.00017111, 0.00013391, 0.00013391, 0.00017974$ となる．つまり，系 3 より M_1 の摂動上限は 0.00020869 となり，F が近似因数分解されるのに必要な変化 0.00624 には届かないことがわかる．よって，F は許容度 0.000001 で近似因数分解不可能である．
◁

注意 22 以上により，根のベキ級数展開から近似因数分解に必要な許容度の下限 $\tilde{\varepsilon}$ が求まる．

$$\tilde{\varepsilon} \to \frac{\sigma'_{(0)}\left(\sqrt{n}\,\sigma'_{(0)} + 2\,\sigma_{n-1}(M_1)\,c - \sqrt{n{\sigma'_{(0)}}^2 + 4\,\sigma_{n-1}(M_1)^2\,c^2}\right)}{2\,c\sqrt{n}\,\|F\|_2}$$

ここで，$\sigma'_{(0)} = \min_{\varphi}(\sigma_{(0)})$ である．*(例：例 1 の多項式の許容度の下限は，0.000014558 となる)*

参 考 文 献

[CGTW95] R. M. Corless, P. M. Gianni, B. M. Trager and S. M. Watt. The singular value decomposition for polynomial systems. *Proc. ACM Internat. Symp. on Symbolic and Algebraic Computation* (1995), 195–207.

[EGL97] Ioannis Z. Emiris, André Galligo and Henri Lombardi. Certified approximate univariate GCDs. *J. Pure Appl. Algebra*, **117&118** (1997), 229–251.

[GC96] Gene H. Golub and Charles F. Van Loan. Matrix Computations Third Edition. (*Johns Hopkins Series in the Mathematical Sciences*, The Johns Hopkins University Press, 1996).

[HK99] Markus A. Hitz and Erich Kaltofen. Efficient Algorithms for Computing the Nearest Polynomial with a Real Root and Related Problems. *Proc. ACM Internat. Symp. on Symbolic and Algebraic Computation* (1999), 205–212.

[Kal95] Erich Kaltofen. Effective Noether Irreducibility Forms and Applications. *J. Computer and System Sciences*, **50** (1995), 274–295.

[NS98] K. Nagasaka and T. Sasaki. Approximate Multivariate Factorization and Its Time Complexity. `http://math.unm.edu/ACA/1998/proceedings.html`, *IMACS ACA '98 Electorical Proceedings*, 1998.

[P98] Victor Y. Pan. Approximate polynomial gcds, Padé approximation, polynomial zeros and bipartite graphs. *Proc. Ninth Annual ACM-SIAM Symp. on Discrete Algorithms* (1998), 68–77.

[SSH92] T. Sasaki, T. Saito and T. Hilano. Analysis of approximate factorization algorithm I. *Japan J. Indust. Appl. Math.*, **9** (1992), 351–368.

[SS93] T. Sasaki and M. Sasaki. A unified method for multivariate polynomial factorizations. *Japan J. Indust. Appl. Math.*, **10** (1993), 21–39.

[SSKS91] T. Sasaki, M. Suzuki, M. Kolář and M. Sasaki. Approximate factorization of multivariate polynomials and absolute irreducibility testing. *Japan J. Indust. Appl. Math.*, **8** (1991), 357–375.