数理解析研究所講究録
1038巻 1998年 111-118

多変数多項式の近似因数分解とその計算量

筑波大学 大学院 数学研究科 長坂 耕作 (Kosaku Nagasaka)
筑波大学 数学系 佐々木建昭 (Tateaki Sasaki)

1. はじめに

近似無平方分解や近似GCDなどの近似的代数計算は、数式処理分野の世界的トピックになりつつある。(これら近似的代数計算については、参考文献[1]に入門的事項が載っている)。近似因数分解も同様に、今後の発展が期待される分野である。多項式Fの精度εでの近似因数分解とは、

$$F = GH + \Delta_F \tag{1}$$

なる多項式GとHを見つけることである。ここで、Δ_Fはその数係数の絶対値がε以下である**微小**多項式である。これから分かるように、近似因数分解は唯一には定まらないが、与えられた精度の範囲でできる限り分解するものとする(εを無限小と定めれば、通常の因数分解となる)。

多変数多項式の因数分解は、Kronecker や Wang-Rothschild([WR75]) のアルゴリズムを用いた場合、多項式時間では終了しないことが知られている。論文[Kal85]では、根の最小多項式を構成して既約因子を求めるアルゴリズムが提案されており、これは多項式時間で終了する。近似因数分解に対するアルゴリズムとしては、論文[SSKS91]で提案された、ベキ級数展開された根の線形的な性質を利用したアルゴリズムがあり、論文[SSH92, SS93]ではその解析も行なわれている。しかしながら、そのアルゴリズムでは、根を**十分大きい次数までベキ級数展開する**と述べられているのみで、具体的にどの次数まで展開すればよいのか不明であった。そこで、本稿ではまず級数根の打ち切り次数の上限を決定する。また上記の論文では共通して、因数分解すべき多項式をモニックであると仮定している。モニックでない場合、古典的な方法でモニックな多項式へ変換する必要がある。しかし、多項式の数係数に誤差が含まれる場合、このモニック化は多項式の係数に含まれる誤差を著しく大きくするのが普通で、因数分解の精度が悪くなる。そこで本稿では、論文[SSKS91]の方法をモニック化を必要としないアルゴリズムに改変する。そして、このアルゴリズムが主変数の次数に関して多項式時間で終了することを示す。なお、精度に関する議論は今後の研究課題とし、本稿では精度εを無限小とした厳密な因数分解のみを扱う。数値計算は、桁落ちなどの誤差を含まず理想的な結果を返すものとする。

まず、本稿で用いる記号と述語の定義を2章で行ない、論文[SSKS91]で示されたアルゴリズムを3章で紹介する。多変数多項式の多項式因子の従変数に関する次数上限を4章で定め、5章では、モニックでない多項式の根に対する線形関係を用いた既約因子の決定法を提案する。その計算量については6章で議論し、最後に今後の課題を述べる。

2. 記号と述語

本稿では、浮動小数で表される複素数係数の単項式どうしの乗除算を計算量の単位とする。$\mathbf{C}$ を複素数体とし、多項式 $F(x,y,\ldots,z) \in \mathbf{C}[x,y,\ldots,z]$ の主変数 x に関する次数を $\deg(F)$、従変数に関する全次数を $\mathrm{tdeg}(F)$、主変数に関する主係数を $\mathrm{lc}(F)$ と表す。特に断らない限り全次数は従変数に関するものとする。F の各単項式のうち、全次数が e 以上の項の和を $\lfloor F \rfloor_e$ と表し、全次数が e' 以下の項の和を $\lceil F \rceil^{e'}$ で表す。$[F]_e^{e'}$ は $\lceil \lfloor F \rfloor_e \rceil^{e'}$ を表すとする。また、行列 M の階数を $\mathrm{rank}(M)$ と表す。

本稿では、因数分解すべき多項式を $\deg(F) = n, \mathrm{tdeg}(F) = d$ なる

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

とし、従変数の個数を v とする。各係数多項式の全次数は次のように定義する。

$$\mathrm{tdeg}(f_i) = e_i, \quad i = 0,1,\ldots,n$$

一般性を失わず多項式 $F(x,y,\ldots,z)$ と $F(x,0,\ldots,0)$ は原始的かつ無平方であるとする。なお、以下の章では F の次数 n の半分を越えない最大の整数を $\hat{n}$ と定める。

3. 既存の近似因数分解アルゴリズム

論文 [SSKS91] で提案された因数分解のアルゴリズムの概略を次の多項式 F について説明する。

$$F(x,y) = x^4 + (y-2)x^3 - (y+1)x^2 + (y^2+2)x - y$$

1 変数多項式 $F(x,0)$ の根を数値算法で求め、多変数 Hensel 構成を行なうと、$F(x,y)$ の x に関する 1 次因子として次のような 4 つのベキ級数が得られる。

$$\begin{aligned}
F_1 &= x - \varphi_1 = (x-0) - y/2 - y^2/8 - y^3/16 - 5y^4/128 + \cdots, \\
F_2 &= x - \varphi_2 = (x-1) + y/2 - y^2/8 + 0 + y^4/128 + \cdots, \\
F_3 &= x - \varphi_3 = (x-2) + y/2 + y^2/8 + y^3/16 + 5y^4/128 + \cdots, \\
F_4 &= x - \varphi_4 = (x+1) + y/2 + y^2/8 + 0 - y^4/128 + \cdots
\end{aligned}$$

これらのベキ級数の組合せで F の既約因子が求まる。この例では F_1F_3, F_2F_4 なる組合せが既約因子となっている。ここで、F_1 と F_3(あるいは F_2 と F_4) に注目してみると、y について 2 次以上の項同士の和がゼロになることがわかる。

さて、$F_1,\ldots,F_4$ のいくつかの積を A とする。

$$A = F_{m_1} \cdots F_{m_r} = x^r + a_{r-1}x^{r-1} + \cdots + a_0$$

もしも A が多項式ならば、当然、各係数 $a_i, (i = 0,\ldots,r-1)$ も多項式であり、論文 [SSH92] の Theorem 4.2 より $\mathrm{tdeg}(a_{r-1}) \leq 1$ であることがわかる。ここで、

$$a_{r-1} = -(\varphi_{m_1} + \cdots + \varphi_{m_r})$$

であることに注意すれば、$\varphi_{m_1},\ldots,\varphi_{m_r}$ の高次項は加えると互いに消去し合う必要がある。このことを利用して組合せを決定するのが、論文 [SSH92] にある既約因子の決定法である。

3.1. 因数分解アルゴリズム

論文 [SSKS91] で提案されたアルゴリズムの概略は以下のようなものである。

1. 多項式イデアル $S = (y - \hat{y}, \ldots, z - \hat{z})$, $\hat{y}, \ldots, \hat{z} \in \mathbf{C}$ を、F が S を法として無平方になるように定める。(一般性を失うことなく、$S = (y, \ldots, z)$ とする。このとき $F(x, y, \ldots, z) \equiv F(x, 0, \ldots, 0) \pmod{S}$ となる。)
2. 数値算法にて $F(x, 0, \ldots, 0)$ の根を求める。
3. 多変数 Hensel 構成により $F(x, y, \ldots, z)$ の x に関する根のベキ級数展開を求める。
4. ベキ級数根の係数に関する線形関係を用いて既約因子を求める。

このアルゴリズムの基礎となっているのは次の定理である。

定理 3.2 $\hat{E}$ を F の多項式因子の全次数上限とする。$L \geq \hat{E}$ なる任意の正整数 L に対し、

$$\lfloor \varphi_{m_1}^j + \cdots + \varphi_{m_r}^j \rfloor_{\hat{E}} \equiv 0 \pmod{S^{L+1}}, \quad (j = 1, 2, \ldots, n)$$

ならば、$F_{m_1}, \ldots, F_{m_r}$ の S^{L+1} を法とする積が F の多項式因子である。[1)]

定理 3.2 は論文 [SSKS91, SSH92] の主要定理であり、上記関係を求めることで既約因子を決定出来る。実際に上記関係を求めるには、論文 [SSKS91] の **Find-Relations** アルゴリズムを用いる。

定義 3.6 $j = 1, 2, \ldots, n$ に対し、M_j を第 i 行 $(i = 1, 2, \ldots, n)$ が $\lfloor \varphi_i^j \rfloor_{\hat{E}}$ の数係数の列からなる行列と定義する。ただし、数係数が 0 である項も省略しないものとする。

Find-Relations アルゴリズムは次のような行列に対して Gauss の消去法などの行列演算を行なうものである。

$$M(t_1, \ldots, t_k) = t_1 M_1 + \cdots + t_k M_k \tag{3}$$

ここで、$t_1, \ldots, t_k$ はパラメータとする。$k = n$ とすれば、**Find-Relations** により検出されたベキ級数の組合せの積は、定理 3.2 より F の多項式因子となる。しかし、論文 [SSH92] によれば、実際には $k = 1, 2$ 程度の小さい行列に対する計算で F の全ての既約因子を決定できる場合が多い。

3.2. 改善すべき点

上記算法の問題点として、1) ベキ級数の打ち切り上限 L の値が定まっていないこと、2) パラメータ $t_1, \ldots, t_k$ を含んだ行列計算を必要とすること、3) モニックでない多項式の場合にモニックな多項式への変換を必要とすること、があげられる。これらは以後の章で提案する本稿のアルゴリズムで解決する。

4. 多項式因子の係数部の次数上限

本章では、多項式 F の多項式因子の従変数に関する次数上限を求める。この次数上限は線形関係による既約因子の決定において重要な役割をはたす。論文 [SSH92] の次数上限に

[1)] cf. [SSH92, Theorem 5.3]

関する定理をモニックでない多項式に拡張することも可能だが、本稿では別のアプローチでより精緻な次数上限を決定する。紙面の都合上、証明は割愛する。

以下、$A, B \in \mathbf{C}[x, y, \ldots, z]$ なる多項式 A と B を次のように定める。

$$\begin{aligned} A &= a_m x^m + a_{m-1} x^{m-1} + \cdots + a_0, \ (m < n) \\ B &= b_{n-m} x^{n-m} + b_{n-m-1} x^{n-m-1} + \cdots + b_0 \end{aligned} \tag{4}$$

補題 4.1 $F = AB$ ならば $\mathrm{tdeg}(F) = \mathrm{tdeg}(A) + \mathrm{tdeg}(B)$ である。

補題 4.2 $F = AB$ のとき、$\mathrm{tdeg}(a_i) + \mathrm{tdeg}(b_j) > \mathrm{tdeg}(f_{i+j})$ ならば、$\mathrm{tdeg}(a_{i'}) + \mathrm{tdeg}(b_{j'}) > \mathrm{tdeg}(f_{i'+j'})$, $i \neq i', j \neq j'$ なる非零項 $a_{i'}x^{i'}$ と $b_{j'}x^{j'}$ が、それぞれ A と B に存在する。

定義 4.1 原点 $(0,0)$、点 $(0, e_0)$、点 (n, e_n)、および点 $(n, 0)$ は凸包上にあり、各点 (i, e_i), $0 < i < n$, は凸包の外側にプロットされない。そのような凸包のうち最小のものを $\mathcal{D}$ とする。（図1は $\mathcal{D}$ を図に表したものである。）

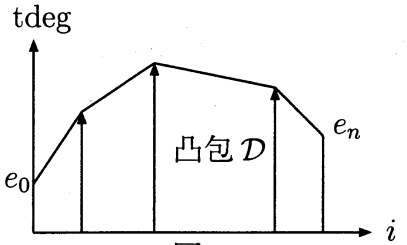

図1

このとき、従変数の次数上限に関して次の定理と系が成り立つ。

定理 4.1 $F = AB$ ならば、$i + j \leq n$ を満たす任意の正整数 i と j に対して、点 $(i + j, \mathrm{tdeg}(a_i \times b_j))$ が凸包 $\mathcal{D}$ の外側にプロットされることはない。

定義 4.2 図1において、横軸 i の値 $0, 1, \ldots, n$ のそれぞれに対して、対応する縦座標値のうち、凸包 $\mathcal{D}$ を越えない最大の整数値を E_i とする。（すなわち、各点 (i, E_i) は $\mathcal{D}$ の内部あるいは $\mathcal{D}$ の境界上にある）

系 4.1 式 (4) の多項式 A が F の多項式因子ならば、A の係数の次数上限として次が成立する。

$$\mathrm{tdeg}(a_i) \leq \min\{E_i, E_{n-m+i}\} \ \ (i = 0, 1, \ldots, m)$$

この系4.1による次数上限は論文 [SSH92] の次数上限よりも良い上限を与える。さらに、モニックでない多項式へも適用が可能である点でもすぐれている。

5. 一般の多変数多項式の因数分解

本章では3章で紹介した因数分解アルゴリズムの補完と修正を行なう。即ち、ベキ級数根の打ち切り次数の上限などを決定する。なお、本章では F をモニックと仮定しない。

定義 5.1 $k = 1, \ldots, \hat{n}$ に対し、E'_k を

$$E'_k = \max\{\min\{E_k, E_{n-\hat{n}+k}\}, E'_i + E'_j \ (i > 0, j > 0, i + j = k)\}$$

と定め、数値 $\tilde{E}_i$ を次のように定義する。

$$\tilde{E}_0 = e_n, \ \ \tilde{E}_i = ie_n + E'_i + 1, \ i = 1, 2, \ldots, \hat{n} \tag{5}$$

さて、3.1 のアルゴリズムにおいて、Step 3 で多変数 Hensel 構成を $k = 2\tilde{E}_{\hat{n}}$ まで行ない、次を満たす F の x に関するベキ級数根を求めたとしよう。

$$F(x, y, \ldots, z) \equiv \mathrm{lc}(F) F_1^{(2\tilde{E}_{\hat{n}})} \cdots F_n^{(2\tilde{E}_{\hat{n}})} \pmod{S^{2\tilde{E}_{\hat{n}}+1}} \tag{6}$$

ここで、各 F_i はモニックとする。以後、全次数が $2\tilde{E}_{\hat{n}}$ 次までの F の根のベキ級数展開をそれぞれ $\varphi_1, \ldots, \varphi_n$ とし、ベキ級数 F_i を $F_i = x - \varphi_i = F_i^{(2\tilde{E}_{\hat{n}})}$ $(i = 1, 2, \ldots, n)$ とする。

5.1. 線形関係を用いた既約因子の決定

Step 4 では線形関係を用いた既約因子の決定を行なう。モニックとは限らない多項式を扱うため、論文 [SSKS91, SSH92] の方法とは少し異なる。以下では G を次式で定める。

$$G = F_{m_1} \cdots F_{m_r} = x^r + g_{r-1} x^{r-1} + \cdots + g_0$$

補題 5.1 $j = 1, 2, \ldots, r$ に対し

$$\lfloor (\mathrm{lc}(F)\varphi_{m_1})^j + \cdots + (\mathrm{lc}(F)\varphi_{m_r})^j \rfloor_{\tilde{E}_j} \equiv 0 \pmod{S^{2\tilde{E}_r+1}}$$

ならば、$\mathrm{lc}(F)^i g_{r-i}$ を $S^{2\tilde{E}_r+1}$ を法として計算すれば、次が成り立つ。

$$\mathrm{tdeg}(\mathrm{lc}(F)^i g_{r-i}) < \tilde{E}_i$$

また、逆も成り立つ。

補題 5.2 $r \geq \hat{n}$ であるとき、$j = 1, 2, \ldots, r$ に対し

$$\lfloor (\mathrm{lc}(F)\varphi_{m_1})^j + \cdots + (\mathrm{lc}(F)\varphi_{m_r})^j \rfloor_{\tilde{E}_j} \equiv 0 \pmod{S^{2\tilde{E}_r+1}}$$

ならば、$\tilde{G} = \mathrm{lc}(F)^r F_{m_1} \cdots F_{m_r}$ は $\mathrm{lc}(F)^{n-1} F$ の多項式因子である。

証明 多項式 $\tilde{H}$ を $\tilde{H} = \mathrm{lc}(F)^{n-r} F_{m_{r+1}} \cdots F_{m_n}$ と定める。このとき補題5.1 より $S^{2\tilde{E}_r+1}$ を法として、$\mathrm{tdeg}(\tilde{G}) < \tilde{E}_r$ かつ $\mathrm{tdeg}(H) < \tilde{E}_r$ が成り立つ。次に、$\tilde{G}, \tilde{H}$ を $\mathrm{lc}(F)^{n-1} F$ で Hensel 構成すると、仮定より $2\tilde{E}_r + 1 > (n-1)e_n + d$, $[\tilde{G}]_{\tilde{E}_r}^{2\tilde{E}_r} = 0, [\tilde{H}]_{\tilde{E}_r}^{2\tilde{E}_r} = 0$ であるから、残差 $\Delta \equiv \mathrm{lc}(F)^{n-1} F - \tilde{G}\tilde{H} \pmod{S^{2\tilde{E}_r+2}}$ は 0 となる。明らかに、$S^{2\tilde{E}_r+3} \Rightarrow S^{2\tilde{E}_r+4} \Rightarrow \cdots$ と Hensel 構成を繰り返しても同様である。よって、$\tilde{G}$ は $\mathrm{lc}(F)^{n-1} F$ の多項式因子である。 □

系 5.1 $j = 1, 2, \ldots, \hat{n}$ に対し

$$\lfloor (\mathrm{lc}(F)\varphi_{m_1})^j + \cdots + (\mathrm{lc}(F)\varphi_{m_r})^j \rfloor_{\tilde{E}_j} \equiv 0 \pmod{S^{2\tilde{E}_{\hat{n}}+1}}$$

ならば、$\tilde{G} = \mathrm{lc}(F) F_{m_1} \cdots F_{m_r}$ の原始部分は F を割り切る。

これらの補題と系により定理 3.2 は次のように一般化される。

定理 5.1 $j=1,2,\ldots,\hat{n}$ に対し

$$\lfloor(\mathrm{lc}(F)\varphi_{m_1})^j+\cdots+(\mathrm{lc}(F)\varphi_{m_r})^j\rfloor_{\tilde{E}_j}\equiv 0 \pmod{S^{2\tilde{E}_{\hat{n}}+1}}$$

となり、かつ $\{\varphi_{m_1},\ldots,\varphi_{m_r}\}$ の任意の部分集合に対しては同様の関係式が成立しないならば、$\mathrm{lc}(F)F_{m_i}\cdots F_{m_r}$ の原始多項式部分が F の既約因子である。

以上より、既約因子の組合せを求めるためには定理 5.1 の関係を求めればよいことが分かる。この関係は論文 [SSKS91] の **Find-Relations** アルゴリズムで求められる。なお、論文 [SSKS91] では定理 3.2 の関係を求めるために、$t_1,t_2,\ldots,t_n$ をパラメータとした行列 $M(t_1,t_2,\ldots,t_n)$ に **Find-Relations** アルゴリズムを適用した。しかし、パラメータを多く含む行列演算は計算量を増大させるので、本稿では以下のように改善する。

補題 5.3 t をパラメータとする行列 $tM+M'$ において、

$$\mathrm{rank}(t'M+M')=\mathrm{rank}(tM+M'),\quad t'\in\mathbf{R}$$

ならば、$t'M+M'$ と $tM+M'$ に成り立つ線形関係は同値である。

補題 5.4 M,M' を n 行の行列とする。このとき、$\mathrm{rank}(t'M+M')<\mathrm{rank}(tM+M')$ となる $t'\in\mathbf{R}$ は高々 n 個である。

定義 5.2 $j=1,2,\ldots,\hat{n}$ に対し、M_j を第 i 行 $(i=1,2,\ldots,n)$ が $\lfloor(\mathrm{lc}(F)\varphi_i)^j\rfloor_{\tilde{E}_j}$ の数係数の列からなる行列と定義する。ただし、数係数が 0 の項も省略しないものとする。

これらの補題により、行列 $M(t_1,t_2,\ldots,t_{\hat{n}})=t_1M_1+t_2M_2+\cdots+t_{\hat{n}}M_{\hat{n}}$ のかわりに、1 つのパラメータのみを含む行列に対して **Find-Relations** アルゴリズムを何回か適用することで、既約因子となる組合せを決定することが出来る。

6. 計算量

本章では、前章で提案した因数分解アルゴリズムが主変数の次数 n に関して多項式時間となっていることを示す。

[Kal85, Lemma 1] より、Step 1 の多項式イデアル S の計算量は、最悪の場合 $2^vn^vd^v$ であることがわかる。よって Step 1 での計算量は、1 変数多項式 $F(x,\hat{y},\ldots,\hat{z})$ の計算量が $O(d^{v+1}n)$ であり、無平方性をチェックする $\gcd(F(x,\hat{y},\ldots,\hat{z}),F'(x,\hat{y},\ldots,\hat{z}))$ の計算量が $O(n^2)$ であることから、$O(2^vd^vn^{v+2})+O(2^vd^{2v+1}n^{v+1})$ となる。

Step 2 の数値算法にかかる時間は、数式処理に比べれば無視できる。

Step 3 の Hensel 構成について考察する。Lagrange の補間式の計算は、n 次未満の 1 変数多項式に対し互除法を各 l について n 回行なう必要があるので、全体では $O(n^4)$ の計算量となる。v 変数の多項式で全次数が K 以下の項の数は K^v を越えることはない。これは、1 つの変数に関する次数が K を越えることはないためである。[Kal85, §6] によれば、二項係数を用いてより良い上限を与えることが出来るが、簡単のため K^v を用いる。よって Step 3 の Hensel 構成において残差の計算量は $O(k^{2v}n^2)$ である。残差からの次の近似因子を計

算するとき、$k+1$ 回目では Lagrange の補間式と残差の積の計算量が $O(2(k^v-(k-1)^v)n)$ であり、残差の計算に比べて問題とならない。定理 5.1 によれば、Hensel 構成は $k=2\tilde{E}_{\hat{n}}$ 次まで行なえば十分である。よって、Hensel 構成全体の計算量は、

$$\begin{aligned} 2^{2v}n^2+\cdots+(2\tilde{E}_{\hat{n}})^{2v}n^2 &< (1+\cdots+2\tilde{E}_{\hat{n}})^{2v}n^2 \\ &= (2\tilde{E}_{\hat{n}}^2+\tilde{E}_{\hat{n}})^{2v}n^2 \\ &\approx 2^{6v}d^{4v}n^{4v+2} \end{aligned}$$

であり、$O(2^{6v}d^{4v}n^{4v+2})$ となる。

次に Step 4(既約因子決定アルゴリズム) を考察する。この Step は、$\mathrm{lc}(F)\varphi$ の累乗計算と **Find-Relations** による行列演算の 2 つにわけることが出来る。前者の計算はある k 冪に対しては、$\mathrm{lc}(F)\times\varphi$ とその k 乗までを全次数に関して $2\tilde{E}_k$ 次まで各々 n 個を計算すればよい。よって、累乗計算全体は

$$\begin{aligned} \textstyle\sum_{k=1}^{\hat{n}}(nd^v(2\tilde{E}_k)^v+n(k-1)(2\tilde{E}_k)^{2v}) &\le \textstyle\sum_{k=1}^{\hat{n}}(nd^v(4kd+1)^v+n(k-1)(4kd+1)^{2v}) \\ &\le n\textstyle\sum_{k=1}^{\hat{n}}k(4kd+1)^{2v} \\ &\le 2^{4v}d^{2v}n(\textstyle\sum_{k=1}^{\hat{n}}k^{2v+1}\le 2^{6v}d^{2v}n^{2v+3} \end{aligned}$$

となって、$O(2^{6v}d^{2v}n^{2v+3})$ の計算量であることが分かる。後者は、各要素がパラメータ t に関する 1 次多項式である $n\times((2\tilde{E}_{\hat{n}})^v-\tilde{E}_k^v)$ の行列に Gauss の消去を行なう前半部分と、$n\times n$ の行列に Gauss の消去を行なう後半部分に分けられる。前半部分の行列を次のように定め、消去法の概略を説明する。

$$\begin{pmatrix} m_{1,1} & \cdots & m_{1,q'} \\ \vdots & \ddots & \vdots \\ m_{q,1} & \cdots & m_{q,q'} \end{pmatrix},\ \deg_t(m_{i,j})\le 1,\ m_{i,j}\in\mathbf{C}[t]$$

1. $i=2$ とする。
2. $j=i,\ldots,q$ について次の行列操作を行なう。
   第 j 行に $m_{i-1,i-1}$ をかけ、第 $i-1$ 行に $m_{j,i-1}$ をかけたものをひく。
3. i が $n-1$ でなければ、i を 1 増やして Step 1 に戻る。

第 j 行に $m_{i-1,i-1}$ をかける部分は、$m_{i-1,i-1}$ の次数が $i-1$ 次であることから i^2q' 回の乗算を必要とし、第 $i-1$ 行に $m_{j,i-1}$ をかける部分は、第 $i-1$ 行の各項の次数が $i-1$ 次で $m_{j,i-1}$ の次数は $i-1$ であるから i^2q' 回の乗算を必要とする。これを $q-i+1$ 回行なうので、多めに見積もって $2i^2qq'$ 回の乗算となる。そして、i について 2 から q まで行なうので

$$2qq'(2^2+\cdots+q^2)<2q^4q'$$

より、計算量は $O(q^4q')$ となる。よって、$n\times((2\tilde{E}_{\hat{n}})^v-\tilde{E}_k^v)$ の行列の場合は、

$$n^4((2\tilde{E}_{\hat{n}})^v-\tilde{E}_k^v) = n^4((2nd+2)^v-(2kd+1)^v) \approx 2^{2v}n^{v+4}d^v$$

であるから、$O(2^{2v}n^{v+4}d^v)$ の計算量となる。この計算を k の値を 1 から順次 $\hat{n}$ まで増やしていく度に行なう必要があるものの、Hensel 構成の計算量に比べ問題とはならない。既約

因子決定アルゴリズムのStep 3については、適当な値tについて行列の各項を計算するのに$n\times((2\tilde{E}_{\hat{n}})^v-\tilde{E}_k^v)$回の乗算を必要とし、階数の計算はGaussの消去法を用いるので、計算量が$O(n^2((2\tilde{E}_{\hat{n}})^v-\tilde{E}_k^v))$となる。この適切な$t$の決定は最悪の場合でも$n$回で済むことを補題5.4が保証するため、Step 3の計算量もHensel構成に比べ問題とならない。

よって、全体を通しての計算量は$O(2^{6v}d^{4v}n^{4v+2})$となる。

7. 今後の課題と議論

本稿で示した近似因数分解の計算量は$O(2^{6v}d^{4v}n^{4v+2})$であり、主変数の次数nについて多項式時間となっている。試し割りのステップを含む因数分解が多項式時間とならないのに比べ、本稿のアルゴリズムは高次多項式に対しては効率の良いことが分かる。

確かに今回示した計算量は多項式時間となったが、この計算量は実際にははるかに大きい見積もりとなっている。その主な理由として、定理5.1はjについて$\hat{n}$まで条件を満たすときに既約因子を決定するとあるが、実際にはほとんどの多項式に対して$j=2,3$程度で既約因子を決定することが出来る。これは、Hensel構成と$\mathrm{lc}(F)\varphi$の累乗計算を著しく減らせることを意味する。今後は、どのような多項式が早い段階で既約因子を決定でき、どのような多項式がjについて$\hat{n}$まで行なわないと決定できないのかを調べたい。また、実際に本稿で提案したアルゴリズムで多項式を因数分解した場合、論文[SSH92]のアルゴリズムに比べてどの程度改善されたかについて実験を行ないたい。なお、実際に近似因数分解を行なう場合は精度を考慮した既約因子の決定を行なわなければならず、本稿の定理5.1もより複雑なものとなるはずである。これについても今後調べたい。

参 考 文 献

[1] 佐々木建昭 他、岩波講座応用数学「計算代数と計算幾何」、岩波書店 (東京)、1993。

[2] 伊理正夫、理工系基礎の数学12「数値計算」、朝倉書店 (東京)、1981。

[Kal85] E. Kaltofen. Polynomial-time reductions from multivariate to bi- and univariate integral polynomial factorization. *SIAM J. Comput.*, **14** (1985), No.2 469-489.

[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.

[WT79] P. S. Wang and B. M. Trager. New algorithms for polynomial square-free decomposition over the integers. *SIAM J. Comput.*, **8** (1979), 300-305.

[WR75] P. S. Wang and L. P. Rothschild. Factoring multivariate polynomials over the integers. *Math. Comp.*, **29** (1975), 935-950.

[Yun76] D. Y. Y. Yun. On squarefree decomposition algorithms, in R. Jenks, ed. *Proc. ACM Symposium on Symbolic and Algebraic Computations 1976 ACM.* 26-35.