

# 多変数多項式の近似因数分解算法の解析

佐々木建昭 (Tateaki SASAKI, 理研)

斎藤友克 (Tomokatsu SAITO, 上智大理工)

平野照比古 (Teruhiko HIRANO, 神奈川工大)

## 1. はじめに

最近, 佐々木らは因数分解の概念を近似因数分解に拡張し, 多変数多項式の近似因数分解算法も与えた〔1〕. この算法は従来とは異なる算法で, 単に近似因数分解にとどまらず, 整数上の因数分解, 代数拡大体上の因数分解, 代数的閉体上の因数分解へと拡張されていくものと期待される. しかしながら, 〔1〕では組合せ検査に基づく初等的算法と, 有望な組合せも線形演算で決める改良算法が提案されたものの, その改良算法が完全であるとの証明は与えられていない. 本稿では改良算法の完全性を証明するが, より詳しくは準備中の論文に記述するので, それを参照されたい〔2〕.

## 2. 近似因数分解, 前稿の復習

本稿では, 単純の  $k$  の多項式はすべて  $C(x, y)$  の要素とし,  $x$  を主変数,  $y$  を従変数とみなす (従変数の個数が 2 以上の場合への一般化は容易である).  $y$  のべき級数環  $E \subset C\{y\}$  と

表わす。多項式  $F$  の絶対値最大の係数の絶対値を  $\text{mmc}(F)$  と表わす。与多項式  $F$  が

$$F = GH + \Delta F, \quad \text{mmc}(\Delta F) / \text{mmc}(F) = O(\varepsilon), \quad (1)$$

ただし  $\varepsilon$  は微小正数，と表わせるとき，この分解を精度  $\varepsilon$  の近似因数分解と呼ぶ。近似因数分解は一意的でない。

以下では，一般性を失うことなく， $l_c(F) = 1$  ( $l_c$  は主係数を表わす)， $F(x, y)$  は無平方で  $F(x, 0)$  も無平方（無平方とは重複因子をもたぬこと）と仮定する。さらに，

$$F(x, y) = x^n + f_{n-1}(y)x^{n-1} + \dots + f_0(y), \quad (2)$$

とし， $\deg_y(F) = e$  とする。

近似因数分解の初等的算法は以下のものである。

入力：多変数多項式  $F(x, y)$  と精度上限  $\varepsilon$ ， $0 < \varepsilon \ll 1$ ；

出力：  $F = G_1 \cdots G_r + \Delta F$  なる，精度  $\varepsilon$  で既約な因子  $G_1, \dots, G_r$ ；

I：  $F(x, 0)$  の根  $u_1, \dots, u_n$  を数値算法で近似的に計算する；

II：  $F_i^{(0)} = x - u_i$ ， $i = 1, \dots, n$ ，を出発値とし，Hensel構成で

$$F(x, y) \equiv F_1^{(e+2)}(x, y) \cdots F_n^{(e+2)}(x, y) \pmod{y^{e+3}}$$

を満たす  $F_i^{(e+2)}$ ， $i = 1, \dots, n$ ，を計算する。

III：  $\{F_1^{(e+2)}, \dots, F_n^{(e+2)}\}$  の要素の積で， $x$  の次数が  $n/2$

以下のものを次数の低い順に作り， $F$  を割った余り  $R$

が  $\text{mmc}(R)/\text{mmc}(F) \leq \varepsilon$  とするものを探す。見つければそれが求める近似因子であり、それに含まれる要素は以後の計算では除外する。//

この算法は簡単明解であるが、ステップⅢで最悪の場合 ( $F$  が既約な場合)、 $2^{n-1}$  通りもの組合せを調べる必要があり、効率が悪く。

これに対し、(1) はさらに、因子  $F_1^{(et_2)}, \dots, F_n^{(et_2)}$  の望ましい組合せを線形演算で見出す算法も与えている。その要点は以下の通りである。

$$F = F_1 \cdots F_n, \quad F_i(x, y) = x - \varphi_i(y), \quad i = 1, \dots, n, \quad (3)$$

とおくと、 $\varphi_i$  は  $F$  の根である。今、 $G = F_1 \cdots F_m$  が  $F$  の多項式因子ならば、対称式の理論および根と係数の関係より

$$\varphi_1^l + \cdots + \varphi_m^l = (\varphi \text{ の多項式}), \quad l = 1, 2, \dots, L, \quad (4)$$

となり、しかも右辺の多項式の次数の上限  $B$  は容易に定まる。そこで、 $F_1, \dots, F_n$  の Hensel 構成を  $y^E$  項、ただし  $E$  は  $B$  より十分大きい、まで計算し、これから  $\varphi_1^l, \dots, \varphi_n^l$ ,  $l = 1, 2, \dots, L$ , を  $y^E$  項まで計算して、

$$\left\{ \begin{array}{l} \varphi_{i_1}^l + \cdots + \varphi_{i_m}^l \\ \text{E次以下} \\ \text{B+1次以上} \end{array} \right\} = 0 \quad (5)$$

となる組合せ  $(F_{i1}, \dots, F_{im})$  を探すのである。これは、 $y_i^e$ ,  $i=1, \dots, n$ , の項  $y^{B+1}, \dots, y^E$  の数係数  $E$  行列の第  $i$  行として表現し、行ベクトルの間に成立する線形関係式を求める問題である。以下、(5) なる関係式を和零関係式と呼ぶ。

### 3. 改良算法の十分性の証明

前記の近似算法では、多くの場合、 $y_1, \dots, y_n$  に対する和零関係式  $E$  を調べるだけで  $F$  の多項式因子が求まる。それで求まらない場合、 $y_1^2, \dots, y_n^2$  に対する和零関係式を調べれば、実際上はほとんどの場合に  $F$  の多項式因子が求まる。しかしながら、これらの条件は必要条件であり、十分条件ではない。理論的には、1)  $l$  の大きな値まで調べれば和零関係式は十分条件となるか？ 2) 与えられた  $l$  の値に対し、和零関係式が十分条件となるのはどのような場合か？、 $l=2$  の問題が生じる。我々は既に 1) の問題を解決し、2) の問題はごく簡単な場合のみを解決した。以下では 1) の解を与える。

これまで  $F$  の根  $y_1, \dots, y_n$  を無限級数に展開する立場で論じてきたが、本章では  $y_1, \dots, y_n$  は  $y$  の代数関数であるとみなす。無平方の仮定より  $y_i \neq y_j$  ( $i \neq j$ )。また、 $F$  の 1 次因子は容易に求まるので、それらは除外し、以下では  $y_i$ ,  $i=1, \dots, n$ , は多項式ではないと仮定する。対称式の理論より

$$y_1^l + \cdots + y_n^l = g_l(y), \quad l=1, \dots, n, \quad (6)$$

と作る  $y$  の多項式  $g_l$  が計算できる ( $g_1 = -f_{n-1}$ ,  $g_2 = f_{n-1}^2 - 2f_{n-2}$ , etc.).

このとき,  $z_1, \dots, z_n \in \mathbb{C}$  未知数とする以下の代数方程式系を  
考える:

$$\left. \begin{aligned} z_1 + \cdots + z_n &= g_1(y), \\ \vdots \\ z_1^n + \cdots + z_n^n &= g_n(y), \end{aligned} \right\} (E) \quad (7)$$

$$\left. \begin{aligned} \lambda_1 z_1 + \cdots + \lambda_n z_n &= h_1(y), \\ \vdots \\ \lambda_1 z_1^L + \cdots + \lambda_n z_n^L &= h_L(y). \end{aligned} \right\} (E')$$

ただし,  $\lambda_1, \dots, \lambda_n \in \mathbb{C}$  (複素数体),  $h_1, \dots, h_L$  は  $y$  の適  
当な多項式である。まず, これらの方程式系の意味を述べる。

(E) は  $z_1, \dots, z_n$  に関する基本対称式

$$z_1 + \cdots + z_n, \quad z_1 z_2 + \cdots + z_{n-1} z_n, \quad \dots, \quad z_1 z_2 \cdots z_n$$

に関する方程式系に書き直すことができる。このことから,

$z_1, \dots, z_n$  は

$$F(x, y) = x^n + f_{n-1}(y)x^{n-1} + \cdots + f_0(y) \quad (8)$$

の異なる  $n$  個の根に対応することになる。すなわち, (E) は

$$\left\{ (z_1 = y_{i_1}, \dots, z_n = y_{i_n}) \mid \{i_1, \dots, i_n\} = \{1, \dots, n\} \right\} \quad (9)$$

なる， $n!$ 個の異なる解をもつことが分る。次に $(E')$ について。前章に述べた改良算法は，根の $l$ 乗， $y_1^l, \dots, y_n^l$ ，が満たす線形関係式の中で， $l=1, 2, \dots, L$ に対して成立するものを求める。すなわち， $(E')$ の方程式系は改良算法によつて決められる関係式を表わしている。

$(E)$ と $(E')$ の両方を満足する解としては， $F$ の多項式因子に対応するものがある。たとえば， $G = F_1 \cdots F_m$ が $F$ の多項式因子ならば，

$$\left. \begin{aligned} z_1 + \cdots + z_m + 0 \cdot z_{m+1} + \cdots + 0 \cdot z_n &= h_1 \\ \dots \\ z_1^L + \cdots + z_m^L + 0 \cdot z_{m+1}^L + \cdots + 0 \cdot z_n^L &= h_L \end{aligned} \right\} \quad (10)$$

なる関係式が存在する。問題はこれ以外の関係式が存在するか否かである。

**〔定理〕**  $L = n$ ならば， $(E)$ と $(E')$ を満くす $(\lambda_1, \dots, \lambda_n)$ と $(h_1, \dots, h_n)$ は $F$ の多項式因子に対応する関係式のみである。

**証明**  $(E)$ において， $z_n, z_{n-1}, \dots, z_2$ を順に消去すると

$$G_n(z_1, \dots, z_n) = 0, G_{n-1}(z_1, \dots, z_{n-1}) = 0, \dots, G_1(z_1) = 0$$

が得られる。ここで， $G_n = z_1 + \cdots + z_n - g_n$ ， $G_1(z_1) = F(z_1, y)$ である（これらの以外の $G_i$ の表式については〔2〕を参照）。

さて、 $(E)$  の解のなす代数多様体  $V$ ,  $(E)+(E')$  の解のなす代数多様体  $V_L$  とすれば、以下が成立する：

$$V \supseteq V_1 \supseteq \cdots \supseteq V_L.$$

{3} によれば、 $V$  の  $V_L$  への分割は、イデアル  $I = (G_1, G_2, \dots, G_n)$  の準素分解に対応する。まず、 $G_1(z_1) = F(z_1, y)$  であるから、 $G_1$  は以下のように分解できる：

$$G_1(z_1) = \hat{F}_1(z_1, y) \cdots \hat{F}_r(z_1, y). \quad (11)$$

ここで、 $\hat{F}_i$  は  $F$  の  $\mathbb{C}$  上での既約多項式因子である。イデアルの準素分解の理論〔4, 5〕によると、準素分解により  $I$  は

$$(\hat{F}_1(z_1, y), z_2 - \hat{G}_2(z_1), \dots, z_n - \hat{G}_n(z_1, \dots, z_{n-1})) \quad (12)$$

なる形の素イデアルの共通集合に分解できる。この素イデアルの零点のなす代数多様体は既約で、それ以上に分解はできない。

一般性を失うことなく、(12) の  $\hat{F}_i$  としては  $\hat{F}_1$  を考え、

$$\hat{F}_1(x, y) = \{x - \varphi_1(y)\} \cdots \{x - \varphi_m(y)\} \quad (13)$$

とする。  $F$  の根はすべて多項式でないと仮定したから、 $m \geq 2$  である。しかるに、(12) の零点として少なくとも

$$(z_1 = y_{i_1}, \dots, z_n = y_{i_n}), \quad i_1 = 1, \dots, m, \quad (14)$$

の  $m$  個が存在する。仮定し、 $\{i_1, \dots, i_n\} = \{1, \dots, n\}$  であるところ、 $L = n$  のとき、 $(E')$  は以下と表わせる：

$$\begin{pmatrix} z_1 & \cdots & z_n \\ \vdots & & \vdots \\ z_1^n & \cdots & z_n^n \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = \begin{pmatrix} h_1 \\ \vdots \\ h_n \end{pmatrix}. \quad (15)$$

この式は  $(\lambda_1, \dots, \lambda_n)$  に対する線形関係式とみなせる。この式に (14) の解を代入し  $k$  とし、 $y_i \neq y_j$  ( $i \neq j$ ) の仮定より、行列部分は正則となる。また、(14) の異なる解を代入することは、 $(\lambda_1, \dots, \lambda_n)$  を適当に入れかえることに相当する。したがって、正則な線形方程式の解は一意的であることから、(14) の異なる解を代入し  $k$  とし、(15) は不変でなければならず、 $(\lambda_1, \dots, \lambda_n)$  の中で入れかえられるものは値が同じでなければならぬ。即ち、 $L = n$  に対して  $(E) + (E')$  を満足する解は、(10) のように、 $F$  の多項式因子に対応する解のみである。\*)

(証明終)

(系) 前章に述べた改良算法は、根の  $n$  乗和まで和零関係式を調べるとき、因数分解の十分な算法となる。



証明. 根  $y_1, \dots, y_n$  は,  $y_i(0) = u_i$ ,  $i=1, \dots, n$ , であるから,  
 $y$  の無限べき級数に展開できる。したがって, 上記定理  
 は  $z_1, \dots, z_n \in \mathbb{C}\{y\}$  の要素とみなしても成立し,  $y$  の次  
 数が  $B$  より十分大きい打ち切りべき級数環の要素として  
 も成立する。<sup>\*\*\*)</sup> 打ち切りべき級数の次数上限  $E$  としては,  
 $(y^{B+1}, y^{B+2}, \dots, y^E)$  の数係数から成る行列から  $n$  個の非零  
 列をもちょうに選んでおけば十分である。(証明終)

#### 4. あとがき

前章の証明では, 数係数は正確なものとして, 正確な因数  
 分解の場合のみを論じた。実際上の計算では, 数係数は特殊  
 な場合を除いて浮動小数として扱わざるを得ず, 誤差解析が  
 必要である。また, 近似因数分解の場合は, 係数行列におけ  
 る近似的な和零関係式と近似因数分解の精度との関係も解析  
 する必要があるが, 本稿ではそこまでは至らなかった。今後,  
 おいおい解析を進めていきたい。

#### 参考文献

- {1} T. Sasaki, M. Suzuki, M. Kolar and M. Sasaki,  
 "Approximate Factorization of Multivariate Polynomials  
 and Absolute Irreducibility Testing".

RIKEN preprint, Aug. 1990 (submitted);

数理解講究録 (「数値解析と科学計算 (1990年11月)」報告集).

[2] T. Sasaki, T. Saito and T. Hirano, preprint in preparation.

[3] B. L. van der Waerden (銀林浩訳), 現代代数学3, 第12-13章,  
東京図書, 1975 (第16刷).

[4] P. Gianni, B. Trager and G. Zacharias,

"Gröbner Bases and Primary Decomposition of Polynomial Ideals", J. Symb. Comp. 6, pp. 149-167 (1988)

[5] H. Kobayashi, S. Moritsugu and R. Hogan,

"On Radical Zero-Dimensional Ideals", J. Symb. Comp. 8,  
pp. 545-552 (1989).

\*)  $\hat{F}_1$  が既約であることから,  $\lambda_1 \neq 0$  となる (15) の解は,  
少なくとも  $\hat{F}_1$  の 1 次因子すべての入れかえに関して対称  
となる。すなわち,  $\lambda_1 = \lambda_2 = \dots = \lambda_m$  となる。

\*\*\*)  $u_i \neq u_j$  ( $i \neq j$ ) であるから, 各項  $y_i$  をべき級数で展開  
し, 任意の次数で打ち切り,  $k$  とき, 根は全て異なる。し  
たが, て, (14) の行列にここの打ち切りべき級数根を  
代入し  $k$  とき, 行列は正則となる。