数理解析研究所講究録
第753巻 1991年 1-10

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を与えた〔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，有望な組合せを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，簡単のため多項式はすべて$C[x,y]$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のべき級数環を$C\{y\}$と

表わす。多項式Fの絶対値最大の数係数の絶対値を $mmc(F)$ と表わす。与多項式Fが

$$F = GH + \Delta F,\ mmc(\Delta F)/mmc(F) = O(\varepsilon), \qquad (1)$$

ただしεは微小正数，と表わせるとき，この分解を精度ε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，$lc(F)=1$（lc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，

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

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ε，$0<\varepsilon\ll 1$；

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

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

Ⅱ：$F_i^{(0)} = x - u_i$，$i=1,\cdots,n$，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$F_i^{(e+2)}$，$i=1,\cdots,n$，を計算する。

Ⅲ：$\{F_1^{(e+2)},\cdots,F_n^{(e+2)}\}$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 $mmc(R)/mmc(F) \fallingdotseq \varepsilon$ となるものを探す。見つか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，効率が悪い。

これに対し，〔1〕はさらに，因子 $F_1^{(et+2)}, \cdots, F_n^{(et+2)}$ の望ましい組合せを線形演算で見い出す算法も与えている。その要点は以下の通りである。

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

とおくと，φ_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

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

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，$F_1, \cdots, F_n$ 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 $\varphi_1^l, \cdots, \varphi_n^l$, $l = 1, 2, \cdots, L$, を y^E 項まで計算して，

$$\left\{ \varphi_{i1}^l + \cdots + \varphi_{im}^l \right\}_{\substack{E\text{次以下} \\ B+1\text{次以上}}} = 0 \tag{5}$$

となる組合せ $(F_{i1}, \cdots, F_{im})$ を捜すのである。これは，y_i^l, $i=1, \cdots, n$, の項 $y^{B+1}, \cdots, y^E$ の数係数を行列の第 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，$y_1, \cdots, y_n$ に対する和零関係式を調べるだけで F の多項式因子が求まる。それで求まらない場合，$y_1^2, \cdots, y_n^2$ 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，十分な条件ではない。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？，の二つの問題が生じる。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。

これまでは F の根 $y_1, \cdots, y_n$ を無限級数に展開する立場で論じてきたが，本章では $y_1, \cdots, y_n$ 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, $i=1, \cdots, n$, は多項式ではないと仮定する。対称式の理論より

$$\varphi_1^l + \cdots + \varphi_n^l = g_l(y), \quad l = 1, \cdots, n, \tag{6}$$

となる y の多項式 g_l が計算できる（$g_1 = -f_{n-1}$, $g_2 = f_{n-1}^2 - 2f_{n-2}^2$, etc.）. このとき、$z_1, \cdots, z_n$ を未知数とする以下の代数方程式系を考える：

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

$$\left.\begin{aligned} &\lambda_1 z_1 + \cdots + \lambda_n z_n = h_1(y), \\ &\quad\vdots \\ &\lambda_1 z_1^L + \cdots + \lambda_n z_n^L = h_L(y). \end{aligned}\right\} (E') \tag{7}$$

ただし、$\lambda_1, \cdots, \lambda_n \in \mathbb{C}$（複素数体）, $h_1, \cdots, h_L$ 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 $z_1, \cdots, z_n$ に関する基本対称式

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

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、$z_1, \cdots, z_n$ は

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

の異なる n 個の根に対応することが分る。すなわち、（E）は

$$\{ (z_1 = y_{i1}, \cdots, z_n = y_{in}) \mid \{i1, \cdots, in\} = \{1, \cdots, n\} \} \tag{9}$$

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，$y_1^l, \cdots, y_n^l$，が満たす線形関係式の中で，$l=1,2,\cdots,L$ 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っ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，

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

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') を満たす $(\lambda_1,\cdots,\lambda_n)$ と $(h_1,\cdots,h_n)$ は F の多項式因子に対応する関係式のみである。

<u>証明</u> (E) において，$z_n, z_{n-1}, \cdots, z_2$ を順に消去すると

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

が得られる。ここで，$G_n=z_1+\cdots+z_n-g_1$，$G_1(z_1)=F(z_1,y)$ である（これら以外の 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をV, (E)+(E')の解のなす代数多様体を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$I=(G_1, G_2, \cdots, G_n)$の準素分解に対応する。まず、$G_1(x_1)=F(x_1, y)$であるから、$G_1$は以下のように分解できる：

$$G_1(x_1) = \hat{F}_1(x_1, y) \cdots \hat{F}_r(x_1, y). \qquad (11)$$

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

$$(\hat{F}_i(x_1, y),\ x_2 - \hat{G}_2(x_1),\ \cdots,\ x_n - \hat{G}_n(x_1, \cdots, x_{n-1})) \qquad (12)$$

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、

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

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。したがって、(12)の零点として少なくとも

$$(z_1 = \zeta_{i1}, \cdots, z_n = \zeta_{in}), \quad i1 = 1, \cdots, m, \qquad (14)$$

のm個が存在する。ただし、$\{i1, \cdots, in\} = \{1, \cdots, n\}$ である。

ところで、$L = n$ のとき、(E')は以下と表わせる:

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

この式は $(\lambda_1, \cdots, \lambda_n)$ に対する線形関係式とみなせる。この式に(14)の解を代入したとき、$\zeta_i \neq \zeta_j$ ($i \neq j$) 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、$(\lambda_1, \cdots, \lambda_n)$ 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たとき、(15)は不変でなければならず、$(\lambda_1, \cdots, \lambda_n)$ の中で入れかえられるものは値が同じでなければならない。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 $y_1, \cdots, y_n$ は，$y_i(0) = u_i$，$i = 1, \cdots, n$，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 $z_1, \cdots, z_n$ を $\mathbb{C}\{y\}$ 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。**) 打ち切りべき級数の次数上限 E としては，$(y^{B+1}, y^{B+2}, \cdots, y^E)$ の数係数から成る行列が n 個の非零列をもつよ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);
数理研講究録(「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, 少くともも $\hat{F}_1$ 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, $\lambda_1 = \lambda_2 = \cdots = \lambda_m$ 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ったとき, 根は全て異なる。したがって, (14)の行列にこれらの打ち切りべき級数根を代入したとき, 行列は正則となる。