Advances in Applied Mathematics 应用数学进展, 2020, 9(8), 1230-1238
Published Online August 2020 in Hans. http://www.hanspub.org/journal/aam
https://doi.org/10.12677/aam.2020.98144

Hans汉斯

The Verification of Approximate Polynomial Factorization

Jieyu Yan, Zhe Li*

School of Science, Changchun University of Science and Technology, Changchun Jilin
Email: jieyuyan0708@163.com, *zheli200809@163.com

Received: Jul. 26th, 2020; accepted: Aug. 13th, 2020; published: Aug. 20th, 2020

Abstract

It is well-known for a polynomial with perturbed coefficients, its factorization is discontinuous. Therefore, the traditional polynomial factorization is an ill-posed problem for numerical computation. This paper is to study the trusted computing of polynomial approximate factorization on the basis of interval algorithm. Given a polynomial of real coefficients, this paper uses the existing algorithm to compute the structure of factorization manifold, and provides a verification algorithm to compute a factorization with interval coefficients in the computed factorization manifold structure. The algorithm is guaranteed that there exists a real factorization within this interval factorization such that the corresponding polynomial of the real factorization is the polynomial with the minimum residual in the computed decomposition manifold structure.

Keywords

Multivariate Polynomial, Approximate Factorization, Verification

多项式近似因式分解的可信验证

严杰煜，李　喆*

长春理工大学理学院，吉林　长春
Email: jieyuyan0708@163.com, *zheli200809@163.com

收稿日期：2020年7月26日；录用日期：2020年8月13日；发布日期：2020年8月20日

摘　要

众所周知，系数有扰动多项式的因式分解是不连续的。因此，传统的多项式因式分解对于数值计算来说是一个不适定问题。本文利用区间算法，研究多项式近似因式分解的可信计算。给定一个实多项式，本

*通讯作者。

文章引用: 严杰煜, 李喆. 多项式近似因式分解的可信验证[J]. 应用数学进展, 2020, 9(8): 1230-1238.
DOI: 10.12677/aam.2020.98144

文利用已有算法计算给定多项式其因式分解流形结构，设计算法输出在该因式分解流形结构中一系数为区间的因式分解。算法保证，在该区间因式分解中存在一系数为实数的因式分解，其所对应的多项式为在确定的因式分解流形结构中与给定多项式残差最小的多项式。

关键词

多元多项式，近似因式分解，可信验证

1. 引言

多项式因式分解是多项式基本运算的主要研究问题之一，也是 Maple，Mathematica 等计算机代数系统的主要功能之一。国内外很多学者对多项式因式分解问题进行了大量的研究。Lenstra 和 Lovasz [1]首先提出了关于一元多项式因式分解的时间算法。该算法使用 Berlekamp 算法并结合 Hensel 引理对有限域上的多项式进行因式分解。Kaltofen 和 Von zur Gathen [2] [3]给出了多元多项式因式分解的时间算法，并对该算法的时间复杂性进行了严格的证明。目前，精确的二元多项式因式分解时间复杂性最低的算法是由 Lecerf [4]提出的。Gao [5]在 Ruppert [6]针对多项式微分形式相关结论的启发下，提出了一种新的因式分解算法。该算法首先利用 Hilbert 不可约定理，将多项式由多元降为二元，并提出了二元多项式任意域上的因式分解方法。

众所周知，多项式其系数微小的摄动都有可能改变其因式分解的结构。因此，对于系数有扰动的多项式，其因式分解计算是不连续的。于是当一个多项式系数的精确度有限时，其因式分解计算就显得十分困难。随着对多项式因式分解研究的逐步深入，学者们将研究工作从符号计算扩展到数值计算。Sasaki [7]通过矩阵运算尽可能多的得到零和关系，提出了一种有效算法改进了多项式的近似因式分解算法。Gao、Kaltofen、May、Yang 和 Zhi [8] [9]基于 Ruppert 和 Gao 针对多元多项式微分形式的研究成果，利用奇异值分解，结构总体最小二乘以及高斯－牛顿算法来计算多元多项式近似因式分解。Corless、Galligo 和 Giesbrecht 等人[10] [11] [12]从几何角度研究了多项式因式分解问题。他们基于参数空间中的投影和随机环上的延拓法，从一个具有扰动的多项式中重建一个近似多项式及其不可约因子，通过建立因式分解的分层复解析流形及其管状邻域，设计了多项式因式分解的数值算法。Kahan [13]发现了对于不适定代数问题不连续解的流形上隐藏的连续性，解决了对数据微小变化敏感的多项式因式分解的计算问题。Wu 和 Zeng [14]提出了基于多项式空间几何和因式分解流形分层的数值分解概念，证明了多项式数值因式分解的存在性、唯一性、李普希茨连续性和收敛性，并提出了多项式数值因式分解算法。该算法消除了传统因式分解的病态性，将数值计算中的不适定因式分解问题完全正则化。

本文利用区间算法，在文献[14]工作的基础上设计了在确定因式分解流形结构下，与给定多项式残差向量 2-范数最小的多项式的可信计算方法。

2. 预备部分

本文分别用 $\mathbb{N}$、$\mathbb{R}$ 和 $\mathbb{R}^+$ 表示非负整数集合、实数集合和正实数集合。用 $\le$ 来表示 $\mathbb{N}^n$ 上的乘积顺序，对于 $\boldsymbol{\alpha}=(\alpha_1,\alpha_2,\cdots,\alpha_n)^{\mathrm{T}}$，$\boldsymbol{\beta}=(\beta_1,\beta_2,\cdots,\beta_n)^{\mathrm{T}}\in\mathbb{N}^n$，$\boldsymbol{\alpha}\le\boldsymbol{\beta}$ 当且仅当 $\alpha_i\le\beta_i$，$i=1,2,\cdots,n$。用 $\prec_{lex}$ 表示 $\mathbb{N}^n$

上的字典序，若向量 $\boldsymbol{\beta}-\boldsymbol{\alpha}$ 的最左边的非零项是正的，记为 $\boldsymbol{\alpha}\prec_{lex}\boldsymbol{x}^{\boldsymbol{\beta}}$。假设向量 $\boldsymbol{x}=\left(x_1,x_2,\cdots,x_r\right)^{\mathrm{T}}$ 的分量为变量，$M\left(\boldsymbol{x}\right)$ 是一个 $m\times n$ 维矩阵，该矩阵的每一个分量都是关于变量 $x_1,x_2,\cdots,x_r$ 的函数，$\dfrac{\partial M\left(\boldsymbol{x}\right)}{\partial x_k}$ 表示分量为 $\dfrac{\partial M_{i,j}\left(\boldsymbol{x}\right)}{\partial x_k}$ 的矩阵，其中 $1\le i\le n$，$1\le j\le m$，$1\le k\le r$。I_n 表示 $n\times n$ 维单位矩阵，$O_{m,n}$ 表示 $m\times n$ 维零矩阵。

令 $\mathbb{R}\left[\boldsymbol{x}\right]\coloneqq\mathbb{R}\left[x_1,x_2,\cdots,x_r\right]$ 是关于变量 $x_1,x_2,\cdots,x_r$ 的 r 元多项式环。令 $\boldsymbol{x}^{\boldsymbol{\alpha}}\coloneqq x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_r^{\alpha_r}$ 为 $\mathbb{R}\left[\boldsymbol{x}\right]$ 中的单项，其中 $\boldsymbol{\alpha}=\left(\alpha_1,\alpha_2,\cdots,\alpha_r\right)\in\mathbb{N}^n$。多项式 $f\in\mathbb{R}\left[\boldsymbol{x}\right]$ 是单项式的有限线性组合，即 f 可以写成以下形式

$$f=\sum_{\boldsymbol{\beta}=\left(\beta_1,\beta_2,\cdots,\beta_n\right)^{\mathrm{T}}\in\mathbb{N}^n}c_{\boldsymbol{\beta}}\boldsymbol{x}^{\boldsymbol{\beta}},\ c_{\boldsymbol{\beta}}\in\mathbb{R}$$

令 $\deg_{x_i}\left(f\right)$ 表示多项式 f 关于变量 x_i 的次数，则多项式 f 的次数定义为 $\deg\left(f\right)=\left(\deg_{x_1}\left(f\right),\deg_{x_2}\left(f\right),\cdots,\deg_{x_n}\left(f\right)\right)^{\mathrm{T}}$。令 $\left[f\right]$ 表示 $\prod_{i=1}^{n}\left(\deg_{x_i}\left(f\right)+1\right)$ 维向量，其分量是由多项式 f 的系数按字典序降序排列而成的向量。文献[8] [9] [15]引入了多项式 w 关于次数 $\boldsymbol{l}=\left(l_1,l_2,\cdots,l_n\right)^{\mathrm{T}}$ 的卷积矩阵 $C_{\boldsymbol{l}}\left(w\right)$，对于一个 $\deg\left(w\right)=\boldsymbol{l}$ 的多项式 w，矩阵 $C_{\boldsymbol{l}}\left(w\right)$ 乘以 $\left[f\right]$ 得到的向量为多项式 w 乘以多项式 f 所得的多项式其系数按照字典序排列而成的向量。

令 $\mathbb{IR}$ 表示所有区间 $\left\{\left[\underline{x},\overline{x}\right]:\underline{x},\overline{x}\in\mathbb{R},\underline{x}\le\overline{x}\right\}$ 构成的集合。区间向量 $\boldsymbol{X}=\left(\boldsymbol{X}_1,\boldsymbol{X}_2,\cdots,\boldsymbol{X}_n\right)^{\mathrm{T}}$ 是一个分量为区间的 n 维向量组，且满足条件

$$\boldsymbol{X}=\left\{\left(x_1,x_2,\cdots,x_n\right)\in\mathbb{R}^n:x_i\in\boldsymbol{X}_i,1\le i\le n\right\}.$$

区间矩阵 $A\in\mathbb{IR}^{m\times n}$ 是具有区间项的矩阵，如果区间矩阵 A 中的任意实矩阵是满秩的，则称区间矩阵 A 满秩。如果属于区间矩阵 $M\in\mathbb{IR}^{m\times n}$ 的任意实矩阵 M，对所有的 $1\le i\le n$，$1\le j\le n$ 满足条件 $M_{i,j}=M_{j,i}$，则称区间矩阵 M 是区间对称矩阵。如果区间对称矩阵 M 中的每一个对称矩阵都为正定矩阵，则称区间对称矩阵 M 为区间对称正定矩阵。对于一个区间对称矩阵 M，INTLAB 工具箱[16]中的 isspd 函数可以验证 M 的正定性，即命令 isspd (M)返回值为 1，说明区间对称矩阵 M 为对称正定矩阵。

定理 1 (见[17])：设 $\boldsymbol{f}:\mathbb{R}^n\to\mathbb{R}^n$，$\boldsymbol{f}=\left(f_1,\cdots,f_n\right)^{\mathrm{T}}$，$f_1,\cdots,f_n$ 是连续可微函数。对于 $\tilde{\boldsymbol{x}}\in\mathbb{R}^n$ 和区间向量 $\boldsymbol{X}\in\mathbb{IR}^n$，其中 $\boldsymbol{0}\in\boldsymbol{X}$，令 $\boldsymbol{f}'\left(\tilde{\boldsymbol{x}}+\boldsymbol{X}\right)$ 表示 $\boldsymbol{f}$ 在区间 $\tilde{\boldsymbol{x}}+\boldsymbol{X}$ 处的区间雅可比矩阵。给定 $R\in\mathbb{R}^{n\times n}$ 和满足条件 $\boldsymbol{f}'\left(\tilde{\boldsymbol{x}}+\boldsymbol{X}\right)\subseteq M$ 的区间矩阵 $M\in\mathbb{IR}^{m\times n}$，若

$$-Rf\left(\tilde{\boldsymbol{x}}\right)+\left(I_n-RM\right)\boldsymbol{X}\subseteq\mathrm{int}\left(\boldsymbol{X}\right),$$

则存在唯一的 $\hat{\boldsymbol{x}}\in\tilde{\boldsymbol{x}}+\boldsymbol{X}$，使得 $\boldsymbol{f}\left(\hat{\boldsymbol{x}}\right)=\boldsymbol{0}$，其中 $\mathrm{int}\left(\boldsymbol{X}\right)$ 表示 $\boldsymbol{X}$ 的内部。

3. 多项式近似因式分解

假设 $\gamma p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$ 是多项式 $f\in\mathbb{R}\left[\boldsymbol{x}\right]$ 的近似因式分解，其中 $\gamma\in\mathbb{R}$，$k_1\le k_2\le\cdots\le k_r$，$k_i\in\mathbb{N}$，$p_1,p_2,\cdots,p_r$ 是成对互质的无平方多项式，且对于任意的 $1\le i\le r$，$\deg\left(p_i\right)=\boldsymbol{m}_i=\left(m_{i,1},m_{i,2},\cdots,m_{i,n}\right)^{\mathrm{T}}$。Wu 和 Zeng 在文献[14]中提出了基于多项式空间几何和分解流形分层的数值多项式分解的概念，并且定义多项式全体近似因式分解的子集

$$F_{\boldsymbol{m}_1^{k_1}\boldsymbol{m}_2^{k_2}\cdots\boldsymbol{m}_r^{k_r}}=\left\{\gamma p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}:\gamma\in\mathbb{R},\deg p_i\le\boldsymbol{m}_i,i=1,\cdots,r;p_1,p_2,\cdots,p_r\text{是成对互质的无平方多项式的}\right\}.\quad(1)$$

Wu 和 Zeng 称子集 $F_{\boldsymbol{m}_1^{k_1}\boldsymbol{m}_2^{k_2}\cdots\boldsymbol{m}_r^{k_r}}$ 中任意一个多项式的因式分解流形结构为 $\boldsymbol{m}_1^{k_1}\boldsymbol{m}_2^{k_2}\cdots\boldsymbol{m}_r^{k_r}$，并引入了以下向量

$$\boldsymbol{b}_i=\left(b_{i,\boldsymbol{\beta}}\middle|\boldsymbol{\beta}\in\mathbb{N}^n,\boldsymbol{\beta}\le\boldsymbol{m}_i\right)^{\mathrm{T}},\ 1\le i\le r, \tag{2}$$

其中向量 $\boldsymbol{b}_i$ 的分量是按照关于 $\boldsymbol{\beta}$ 的字典序降序排列。然后，Wu 和 Zeng 将求解因式分解流形结构 $\boldsymbol{m}_1^{k_1}\boldsymbol{m}_2^{k_2}\cdots\boldsymbol{m}_r^{k_r}$ 上的近似因式分解问题转换成计算下述超定方程组的最小二乘解

$$\phi\left(\gamma,[p_1],\cdots,[p_r]\right)=\begin{pmatrix}\left[\gamma p_1^{k_1}\cdots p_r^{k_r}-f\right]\\ \boldsymbol{b}_1^{\mathrm{T}}[p_1]-1\\ \vdots\\ \boldsymbol{b}_r^{\mathrm{T}}[p_r]-1\end{pmatrix}=0. \tag{3}$$

4. 主要结果

4.1. 数值部分

数值部分利用文献[8]中的数值多项式因式分解算法来计算因式分解流形结构 $\boldsymbol{m}_1^{k_1}\boldsymbol{m}_2^{k_2}\cdots\boldsymbol{m}_r^{k_r}$。然后，求超定方程组(3)的最小二乘解，得到该因式分解流形结构上高精度的近似解，记作

$$f\approx\overline{\gamma}\,\overline{p}_1^{k_1}\,\overline{p}_2^{k_2}\cdots\overline{p}_r^{k_r}.$$

我们引入扰动向量

$$\boldsymbol{e}_i=\left(e_{i,\boldsymbol{\beta}}\middle|\boldsymbol{\beta}\in\mathbb{N}^n,\boldsymbol{\beta}\le\boldsymbol{m}_i\right)^{\mathrm{T}},\ 1\le i\le r, \tag{4}$$

其中向量 $\boldsymbol{e}_i$ 的分量关于 $\boldsymbol{\beta}$ 的字典序降序排列。定义扰动多项式 $\overline{p}_i\left(\boldsymbol{e}_i\right)$ 为

$$\overline{p}_i\left(\boldsymbol{e}_i\right)=\overline{p}_i+\sum_{\boldsymbol{\beta}\in\mathbb{N}^n,\boldsymbol{\beta}\le m_i}e_{i,\boldsymbol{\beta}}\boldsymbol{x}^{\boldsymbol{\beta}},\ 1\le i\le r.$$

为了简化表达式，令 $\boldsymbol{e}=\left(\boldsymbol{e}_1,\boldsymbol{e}_2,\cdots,\boldsymbol{e}_r\right)^{\mathrm{T}}$，定义非线性函数

$$F\left(\boldsymbol{e}\right)=\left\|\left[\gamma\overline{p}_1\left(\boldsymbol{e}_1\right)^{k_1}\overline{p}_2\left(\boldsymbol{e}_2\right)^{k_2}\cdots\overline{p}_r\left(\boldsymbol{e}_r\right)^{k_r}-f\right]\right\|_2^2, \tag{5}$$

定义

$$\overline{q}_i\left(\boldsymbol{e}\right)=\left(\frac{k_i}{\overline{p}_i\left(\boldsymbol{e}_i\right)}\right)\gamma\overline{p}_1\left(\boldsymbol{e}_1\right)^{k_1}\overline{p}_2\left(\boldsymbol{e}_2\right)^{k_2}\cdots\overline{p}_r\left(\boldsymbol{e}_r\right)^{k_r},\ 1\le i\le r.$$

非线性函数 $F\left(\boldsymbol{e}\right)$ 的梯度为

$$F'\left(\boldsymbol{e}\right)=\begin{cases}C_{m_1}^{\mathrm{T}}\left(\overline{q}_1\left(\boldsymbol{e}\right)\right)\left[\gamma\overline{p}_1\left(\boldsymbol{e}_1\right)^{k_1}\overline{p}_2\left(\boldsymbol{e}_2\right)^{k_2}\cdots\overline{p}_r\left(\boldsymbol{e}_r\right)^{k_r}-f\right]\\ C_{m_2}^{\mathrm{T}}\left(\overline{q}_2\left(\boldsymbol{e}\right)\right)\left[\gamma\overline{p}_1\left(\boldsymbol{e}_1\right)^{k_1}\overline{p}_2\left(\boldsymbol{e}_2\right)^{k_2}\cdots\overline{p}_r\left(\boldsymbol{e}_r\right)^{k_r}-f\right]\\ \vdots\\ C_{m_r}^{\mathrm{T}}\left(\overline{q}_r\left(\boldsymbol{e}\right)\right)\left[\gamma\overline{p}_1\left(\boldsymbol{e}_1\right)^{k_1}\overline{p}_2\left(\boldsymbol{e}_2\right)^{k_2}\cdots\overline{p}_r\left(\boldsymbol{e}_r\right)^{k_r}-f\right]\end{cases}, \tag{6}$$

其中 $C_{\boldsymbol{m}_i}\left(\overline{q}_i\left(\boldsymbol{e}\right)\right)$ 是多项式 $\overline{q}_i\left(\boldsymbol{e}\right)$ 关于次数 $\boldsymbol{m}_i=\left(m_{i,1},m_{i,2},\cdots,m_{i,n}\right)^{\mathrm{T}}$ 的卷积矩阵。关于变量 $e_{i,\boldsymbol{\beta}}$，有 $F'\left(\boldsymbol{e}\right)$ 对 $e_{i,\boldsymbol{\beta}}$ 的偏导数如下

$$\frac{\partial F'(\boldsymbol{e})}{\partial e_{i,\boldsymbol{\beta}}}=\begin{pmatrix}\dfrac{\partial C_{\boldsymbol{m}_1}^{\mathrm{T}}\left(\overline{q}_1(\boldsymbol{e})\right)}{\partial e_{i,\boldsymbol{\beta}}}\left[\gamma\overline{p}_1(\boldsymbol{e}_1)^{k_1}\,\overline{p}_2(\boldsymbol{e}_2)^{k_2}\cdots\overline{p}_r(\boldsymbol{e}_r)^{k_r}-f\right]\\ \dfrac{\partial C_{\boldsymbol{m}_2}^{\mathrm{T}}\left(\overline{q}_2(\boldsymbol{e})\right)}{\partial e_{i,\boldsymbol{\beta}}}\left[\gamma\overline{p}_1(\boldsymbol{e}_1)^{k_1}\,\overline{p}_2(\boldsymbol{e}_2)^{k_2}\cdots\overline{p}_r(\boldsymbol{e}_r)^{k_r}-f\right]\\ \vdots\\ \dfrac{\partial C_{\boldsymbol{m}_r}^{\mathrm{T}}\left(\overline{q}_r(\boldsymbol{e})\right)}{\partial e_{i,\boldsymbol{\beta}}}\left[\gamma\overline{p}_1(\boldsymbol{e}_1)^{k_1}\,\overline{p}_2(\boldsymbol{e}_2)^{k_2}\cdots\overline{p}_r(\boldsymbol{e}_r)^{k_r}-f\right]\end{pmatrix}+\begin{pmatrix}C_{\boldsymbol{m}_1}^{\mathrm{T}}\left(q_1(\boldsymbol{e})\right)\\ C_{\boldsymbol{m}_2}^{\mathrm{T}}\left(q_2(\boldsymbol{e})\right)\\ \vdots\\ C_{\boldsymbol{m}_r}^{\mathrm{T}}\left(q_r(\boldsymbol{e})\right)\end{pmatrix}\frac{\partial\left[\gamma\overline{p}_1(\boldsymbol{e}_1)^{k_1}\,\overline{p}_2(\boldsymbol{e}_2)^{k_2}\cdots\overline{p}_r(\boldsymbol{e}_r)^{k_r}-f\right]}{\partial e_{i,\boldsymbol{\beta}}}. \tag{7}$$

注 1：数值部分的主要工作是计算下列优化问题的稳定点

$$\min F(\boldsymbol{e})\quad \text{s.t.}\quad\begin{cases}\boldsymbol{b}_1^{\mathrm{T}}\left[\overline{p}_1(\boldsymbol{e}_1)\right]-1=0\\ \boldsymbol{b}_2^{\mathrm{T}}\left[\overline{p}_2(\boldsymbol{e}_2)\right]-1=0\\ \vdots\\ \boldsymbol{b}_r^{\mathrm{T}}\left[\overline{p}_r(\boldsymbol{e}_r)\right]-1=0\end{cases}. \tag{8}$$

□

通过引入拉格朗日算子 $\boldsymbol{\lambda}=(\lambda_1,\lambda_2,\cdots,\lambda_r)^{\mathrm{T}}$，定义拉格朗日函数

$$G(\boldsymbol{e},\boldsymbol{\lambda})=F(\boldsymbol{e})+\sum_{i=1}^{r}\lambda_i\left(\boldsymbol{b}_i^{\mathrm{T}}\left[\overline{p}_i(\boldsymbol{e}_i)\right]-1\right), \tag{9}$$

则有

$$G'(\boldsymbol{e},\boldsymbol{\lambda})=\begin{bmatrix}F'(\boldsymbol{e})\\ \boldsymbol{b}_1^{\mathrm{T}}\left[\overline{p}_1(\boldsymbol{e}_1)\right]-1\\ \boldsymbol{b}_2^{\mathrm{T}}\left[\overline{p}_2(\boldsymbol{e}_2)\right]-1\\ \vdots\\ \boldsymbol{b}_r^{\mathrm{T}}\left[\overline{p}_r(\boldsymbol{e}_r)\right]-1\end{bmatrix}+\begin{bmatrix}\lambda_1\boldsymbol{b}_1\\ \lambda_2\boldsymbol{b}_2\\ \vdots\\ \lambda_r\boldsymbol{b}_r\\ 0\\ 0\\ \vdots\\ 0\end{bmatrix}. \tag{10}$$

由于 $G(\boldsymbol{e},\boldsymbol{\lambda})$ 的 Hession 矩阵不包含变量 λ_i，$1\le i\le r$，为了方便起见将 $G''(\boldsymbol{e},\boldsymbol{\lambda})$ 写作 $G''(\boldsymbol{e})$，显然，

$$G''(\boldsymbol{e})=\begin{bmatrix}F''(\boldsymbol{e}) & \boldsymbol{b}_1 & \boldsymbol{b}_2 & \cdots & \boldsymbol{b}_r\\ \boldsymbol{b}_1^{\mathrm{T}} & & & & \\ \boldsymbol{b}_2^{\mathrm{T}} & & & & \\ \vdots & & & O_{r\times r} & \\ \boldsymbol{b}_r^{\mathrm{T}} & & & & \end{bmatrix}. \tag{11}$$

注 2：通过选择零向量作为初始值，数值部分采用数值牛顿迭代法

$$\begin{pmatrix}\overline{\boldsymbol{e}}\\ \overline{\boldsymbol{\lambda}}\end{pmatrix}\leftarrow\begin{pmatrix}\overline{\boldsymbol{e}}\\ \overline{\boldsymbol{\lambda}}\end{pmatrix}-G''\left(\overline{\boldsymbol{e}}\right)^{-1}G'\left(\overline{\boldsymbol{e}},\overline{\boldsymbol{\lambda}}\right)\tag{12}$$

计算非线性系统 $G'\left(\boldsymbol{e},\boldsymbol{\lambda}\right)=0$ 的近似解 $\left(\overline{\boldsymbol{e}},\overline{\boldsymbol{\lambda}}\right)$。 □

4.2. 验证部分

验证部分分为两个阶段，第一阶段验证非线性系统 $G'\left(\boldsymbol{e},\boldsymbol{\lambda}\right)=0$ 近似解的可信误差界，第二阶段验证优化问题(8)的稳定点是否为其局部最优解。

注 3：对于满足 $\overline{\boldsymbol{e}}\in\tilde{\boldsymbol{E}}$ 的区间向量 $\tilde{\boldsymbol{E}}$，使用区间运算和式(6) (7) (11)计算区间雅克比矩阵 $G''\left(\tilde{\boldsymbol{E}}\right)$。利用定理 1 和 verifynlss 函数计算区间向量 $\hat{\boldsymbol{E}}$ 和 $\hat{\boldsymbol{\Lambda}}$，其满足条件存在实向量 $\hat{\boldsymbol{e}}\in\hat{\boldsymbol{E}}$ 和实向量 $\hat{\boldsymbol{\lambda}}\in\hat{\boldsymbol{\Lambda}}$，使得 $G'\left(\hat{\boldsymbol{e}},\hat{\boldsymbol{\lambda}}\right)=0$。 □

对每个 $1\le i\le r$，令 s_i 表示 $\boldsymbol{e}_i$ 的维数，令 $s=\sum_{i=1}^{r}s_i$。记 $\boldsymbol{E}=\left(\boldsymbol{E}_1,\boldsymbol{E}_2,\cdots,\boldsymbol{E}_r\right)^{\mathrm{T}}$，其中 $\boldsymbol{E}_i\in\mathbb{IR}^{s_t}$。向量 $\boldsymbol{E}_i$，$\boldsymbol{b}_i$ 和 $\boldsymbol{e}_i$ 的最后一项分别用 $E_{i,s}$，$b_{i,s}$ 和 $e_{i,s}$ 表示，令 $\boldsymbol{E}_{i,1:s_{i-1}}$，$\boldsymbol{b}_{i,1:s_{i-1}}$ 和 $\boldsymbol{e}_{i,1:s_{i-1}}$ 分别表示向量 $\boldsymbol{E}_i$，$\boldsymbol{b}_i$ 和 $\boldsymbol{e}_i$ 删除最后一项所得的向量。

不失一般性，我们假设

$$b_{i,s_i}=\max_{1\le j\le s_i}\left|b_{i,j}\right|.$$

对每一个 $1\le i\le r$，存在一个关于变量 $\boldsymbol{e}_{i,1:s_{i-1}}$ 的线性函数 l_i，其满足条件

$$\boldsymbol{e}_{i,s_i}=l_i\left(\boldsymbol{e}_{i,1:s_{i-1}}\right).$$

显然，

$$l_i\left(\boldsymbol{e}_{i,1:s_{i-1}}\right)=-\frac{1}{b_{i,s_i}}\boldsymbol{b}_{i,1:s_{i-1}}.$$

定义非线性函数

$$W\left(\boldsymbol{e}_{1,1:s_{1-1}},\boldsymbol{e}_{2,1:s_{2-1}},\cdots,\boldsymbol{e}_{r,1:s_{r-1}}\right)=F\left(\boldsymbol{e}_{1,1:s_{1-1}},l_1\left(\boldsymbol{e}_{1,1:s_{1-1}}\right),\boldsymbol{e}_{2,1:s_{2-1}},l_2\left(\boldsymbol{e}_{2,1:s_{2-1}}\right),\cdots,\boldsymbol{e}_{r,1:s_{r-1}}l_r\left(\boldsymbol{e}_{r,1:s_{r-1}}\right)\right),$$

则有约束优化问题(8)可以转化为下面无约束优化问题

$$\min W\left(\boldsymbol{e}_{1,1:s_{1-1}},\boldsymbol{e}_{2,1:s_{2-1}},\cdots,\boldsymbol{e}_{r,1:s_{r-1}}\right).\tag{13}$$

验证部分第二阶段使用 isspd 函数验证区间 Hession 矩阵 $W''\left(\hat{\boldsymbol{E}}_{1,1:s_{1-1}},\hat{\boldsymbol{E}}_{2,1:s_{2-1}},\cdots,\hat{\boldsymbol{E}}_{r,1:s_{r-1}}\right)$ 的正定性。当 isspd 函数返回值为 1 时，满足条件 $G'\left(\hat{\boldsymbol{e}},\hat{\boldsymbol{\lambda}}\right)=0$ 的实向量 $\hat{\boldsymbol{e}}$ 为问题(8)的局部最优解。

5. 主要算法

算法 1

输入 $f\in\mathbb{R}\left[\boldsymbol{x}\right]$

输出 $\boldsymbol{m}_1^{k_1}\boldsymbol{m}_2^{k_2}\cdots\boldsymbol{m}_r^{k_r}$，$\left(\gamma,\left[\overline{p}_1\right],\left[\overline{p}_2\right],\cdots,\left[\overline{p}_r\right]\right)^{\mathrm{T}}\in\mathbb{R}^{s+1}$，$\hat{\boldsymbol{E}}\in\mathbb{IR}^{s}$，或“Failure”。

步骤 1 数值部分

步骤 1.1 计算多项式 f 的因式分解流形结构 $\boldsymbol{m}_1^{k_1}\boldsymbol{m}_2^{k_2}\cdots\boldsymbol{m}_r^{k_r}$；

步骤 1.2 计算系统(3)的近似解 $\left(\gamma,\left[\overline{p}_1\right],\left[\overline{p}_2\right],\cdots,\left[\overline{p}_r\right]\right)^{\mathrm{T}}$；

步骤 1.3 计算系统 $G'\left(\overline{\boldsymbol{e}},\overline{\boldsymbol{\lambda}}\right)=0$ 的近似解 $\left(\overline{\boldsymbol{e}},\overline{\boldsymbol{\lambda}}\right)^{\mathrm{T}}$。

步骤 2 验证部分

步骤 2.1 初始化 $R=G''\left(\overline{\boldsymbol{e}},\overline{\boldsymbol{\lambda}}\right)^{-1}$，$\boldsymbol{Z}=\mathrm{intval}\left(G''\left(\overline{\boldsymbol{e}},\overline{\boldsymbol{\lambda}}\right)^{-1}G'\left(\overline{\boldsymbol{e}},\overline{\boldsymbol{\lambda}}\right)\right)$，$\boldsymbol{X}=\boldsymbol{Z}$ 和 $\mathrm{iter}=0$；

步骤 2.2 当 $\mathrm{iter}\le 10$ 进行以下操作：

令 $\mathrm{iter}\leftarrow\mathrm{iter}+1$；

$$\boldsymbol{Y}=\mathrm{hull}\left(\boldsymbol{X}\,\mathrm{inf\,sup}\left(0.9,1.1\right)+10^{-20}\,\mathrm{inf\,sup}\left(-1,1\right),0\right);$$

计算 $G''\left(\overline{\boldsymbol{e}}+\boldsymbol{Y}_{1:s},\overline{\boldsymbol{\lambda}}+\boldsymbol{Y}_{s+1:\mathrm{end}}\right)$；

令 $\boldsymbol{X}=\boldsymbol{Z}+\left(I_{s+1}-RM\right)\boldsymbol{Y}$；

若 $\boldsymbol{X}\subseteq\mathrm{int}\left(\boldsymbol{Y}\right)$，则令

$$\begin{pmatrix}\hat{\boldsymbol{E}}\\ \hat{\boldsymbol{\Lambda}}\end{pmatrix}=\begin{pmatrix}\tilde{\boldsymbol{e}}\\ \tilde{\boldsymbol{\lambda}}\end{pmatrix}+\boldsymbol{X};$$

如果 $\mathrm{iter}=10$，则返回“Failure”并停止。

步骤 2.3 计算区间 Hession 阵 $W''\left(\hat{\boldsymbol{E}}_{1,1:s_{1-1}},\hat{\boldsymbol{E}}_{2,1:s_{2-1}},\cdots,\hat{\boldsymbol{E}}_{r,1:s_{r-1}}\right)$，若 $\mathrm{isspd}\,W''\left(\hat{\boldsymbol{E}}_{1,1:s_{1-1}},\hat{\boldsymbol{E}}_{2,1:s_{2-1}},\cdots,\hat{\boldsymbol{E}}_{r,1:s_{r-1}}\right)$ 返回值为 1，则输出 $\boldsymbol{m}_1^{k_1}\boldsymbol{m}_2^{k_2}\cdots\boldsymbol{m}_r^{k_r}$，$\left(\gamma,\left[\overline{p}_1\right],\left[\overline{p}_2\right],\cdots,\left[\overline{p}_r\right]\right)^{\mathrm{T}}$ 和 $\hat{\boldsymbol{E}}$，否则，返回“Failure”。 □

注 4：在算法 1 中，给定实数 x，则 intval(x)输出区间 $\left[x,x\right]$。给定实数 a，b，其中 $a<b$，则 $\mathrm{inf\,sup}\left(a,b\right)$ 输出实区间 $\left[a,b\right]$。给定 $\boldsymbol{X}\in\mathbb{IR}^n$，则 $\mathrm{hull}\left(\boldsymbol{X},\boldsymbol{0}\right)$ 输出包含 $\boldsymbol{X}$ 和零向量的最小的区间向量。 □

通过以上分析可以得到下述定理。

定理 2：假设算法 1 成功输出因式分解流形结构 $\boldsymbol{m}_1^{k_1}\boldsymbol{m}_2^{k_2}\cdots\boldsymbol{m}_r^{k_r}$，系数向量 $\left(\gamma,\left[\overline{p}_1\right],\left[\overline{p}_2\right],\cdots,\left[\overline{p}_r\right]\right)^{\mathrm{T}}$ 和摄动区间向量 $\hat{\boldsymbol{E}}$，则存在一个实向量 $\hat{\boldsymbol{e}}\in\hat{\boldsymbol{E}}$，它是优化问题(8)的局部最优解。

6. 算例

例 1 考虑多项式 $f=p_1^2p_2+r\times10^{-9}$，其中多项式 $p_1=3x+2y+1$，$p_2=5x+2y+2$，$\deg\left(f\right)=\left(3,3\right)^{\mathrm{T}}$。摄动多项式 r 与 f 的次数相同且 r 的系数是[−5, 5]上随机的一个数。应用算法 1 可得

$$\boldsymbol{m}_1^{k_1}\boldsymbol{m}_2^{k_2}=\left(1,1\right)^2\left(1,1\right),$$

$$\left[\overline{p}_1\right]=\left(1.5803\times10^{-16}\quad 2.9997\quad 1.9998\quad 0.9997\right)^{\mathrm{T}},$$

$$\left[\overline{p}_2\right]=\left(-4.4813\times10^{-16}\quad 4.9999\quad 2.0001\quad 1.9997\right)^{\mathrm{T}},$$

$$\hat{\boldsymbol{E}}=10^{-15}\left(0.1580\quad 0.0268\quad 0.1625\quad 0.3219\quad -0.4481\quad -0.8401\quad 0.3918\quad -0.5525\right)^{\mathrm{T}}.$$

因此根据定理 2，存在一个实向量 $\hat{\boldsymbol{e}}\in\hat{\boldsymbol{E}}$，它是优化问题(8)的局部最优解。

例 2 [14] 考虑多项式 $f=p_1p_2+0.0000003x^3y+0.000007xy$，其中多项式 $p_1=3x^2+2xy-5$，$p_2=y^2-4x+6$，$\deg\left(f\right)=\left(3,3\right)^{\mathrm{T}}$。应用算法 1 可得

$$\boldsymbol{m}_1^{k_1}\boldsymbol{m}_2^{k_2}=\left(2,2\right)\left(2,2\right),$$

$$\left[\overline{p}_1\right]=\left(-1.2201\times10^{-9}\quad -2.5286\times10^{-7}\quad 3.000002251\quad -2.3292\times10^{-9}\quad 2.000001373\quad 1.4907\times10^{-6}\right.$$
$$\left.-2.2953\times10^{-7}\quad -8.3129\times10^{-8}\quad -5.000001716\right)^{\mathrm{T}},$$

$$[\bar{p}_2]=\left(3.7233\times10^{-8}\ \ -1.5356\times10^{-7}\ \ 2.1146\times10^{-7}\ \ 1.4866\times10^{-7}\ \ -4.8462\times10^{-7}\ \ 3.9999968\right.$$
$$\left.0.9999998\ \ -8.0742\times10^{-8}\ \ 5.999999\right)^{\mathrm{T}},$$

$$\hat{\boldsymbol{E}}=10^{-5}\left(-0.0001\ \ -0.0253\ \ 0.225\ \ -0.0233\ \ 0.1374\ \ 0.149\ \ -0.0230\ \ -0.0083\ \ -0.172\ \ 0.0037\right.$$
$$\left.-0.0154\ \ 0.0211\ \ 0.0149\ \ -0.048\ \ 0.313\ \ -0.0641\ \ -0.008\ \ -0.208\right)^{\mathrm{T}}.$$

因此根据定理 2，存在一个实向量 $\hat{\boldsymbol{e}}\in\hat{\boldsymbol{E}}$，它是优化问题(8)的局部最优解。

例 3 考虑单变量多项式 $f=p_1^{10}p_2+r\times10^{-10}$，其中多项式 $p_1=x-5$，$p_2=x-1$，$\deg(f)=11$。摄动多项式 r 与 f 的次数相同且 r 的系数是[−5, 5]上随机的一个数。应用算法 1 可得

$$\boldsymbol{m}_1^{k_1}\boldsymbol{m}_2^{k_2}=(1,1)^{10}(1,1),$$

$$[\bar{p}_1]=\left(0.9999999\ \ -5.0000001\right)^{\mathrm{T}},$$

$$[\bar{p}_2]=\left(-1.0000001\ \ -0.9999999\right)^{\mathrm{T}},$$

$$\hat{\boldsymbol{E}}=10^{-13}\left(-0.0066\ \ -0.0116\ \ 0.0605\ \ 0.1527\right)^{\mathrm{T}}.$$

因此根据定理 2，存在一个实向量 $\hat{\boldsymbol{e}}\in\hat{\boldsymbol{E}}$，它是优化问题(8)的局部最优解。

基金项目

吉林省自然科学基金(批准号：11601039)。

参考文献

[1] Lenstra, A., Lenstra, H. and Lovasz, L. (1982) Factoring Polynomials with Rational Coefficients. *Mathematische Annalen*, **261**, 515-534. https://doi.org/10.1007/BF01457454

[2] Von zur Gathen, J. and Kaltofen, E. (1985) Factoring Sparse Multivariate Polynomials. *Journal of Computer and System Sciences*, **31**, 265-287. https://doi.org/10.1016/0022-0000(85)90044-3

[3] Kaltofen, E. (1985) Polynomial-Time Reductions from Multivariate to Bi- and Univariate Integral Polynomial Factorization. *SIAM Journal on Computing*, **14**, 469-489. https://doi.org/10.1137/0214035

[4] Lecerf, G. (2010) New Recombination Algorithms for Bivariate Polynomial Factorization Based on Hensel Lifting. *Applicable Algebra in Engineering, Communication and Computing*, **21**, 151-176. https://doi.org/10.1007/s00200-010-0121-5

[5] Gao, S. (2003) Factoring Multivariate Polynomials via Partial Differential Equations. *Mathematics of Computation*, **72**, 801-822. https://doi.org/10.1090/S0025-5718-02-01428-X

[6] Ruppert, W. (1999) Reducibility of Polynomials *f*(*x*, *y*) Modulo *p*. *Journal of Number Theory*, **77**, 62-70. https://doi.org/10.1006/jnth.1999.2381

[7] Sasaki, T. (2001) Approximate Multivariate Polynomial Factorization Based on Zero-Sum Relations. In: *Proceedings of ISSAC* 2001, ACM Press, New York, 284-291. https://doi.org/10.1145/384101.384139

[8] Gao, S., Kaltofen, E., May, J., Yang, Z. and Zhi, L. (2004) Approximate Factorization of Multivariate Polynomials via Differential Equations. In: *Proc. ISSAC*'04, ACM Press, New York, 167-174. https://doi.org/10.1145/1005285.1005311

[9] Kaltofen, E., May, J., Yang, Z. and Zhi, L. (2008) Approximate Factorization of Multivariate Polynomials Using Singular Value Decomposition. *Journal of Symbolic Computation*, **43**, 359-376. https://doi.org/10.1016/j.jsc.2007.11.005

[10] Corless, R., Giesbrecht, M., Van Hoeij, M., Kotsireas, I. and Watt, S. (2001) Towards Factoring Bivariate Approximate Polynomials. In: *Proc. of ISSAC*'01, ACM Press, New York, 85-92. https://doi.org/10.1145/384101.384114

[11] Corless, R., Galligo, A., Kotsireas, I. and Watt, S. (2002) A Geometric-Numeric Algorithm for Absolute Factorization of Multivariate Polynomials. In: *Proc. of ISSAC*'02, ACM Press, New York, 37-45. https://doi.org/10.1145/780506.780512

[12] Galligo, A. and Van Hoeij, M. (2007) Approximate Bivariate Factorization, a Geometric Viewpoint. In: *Proceedings of*

SNC'07, ACM Press, New York, 1-10.

[13] Kahan, W. (1972) Conserving Confluence Curbs Ill-Condition. Technical Report, Computer Science Department, University of California, Berkeley.

[14] Wu, W.Y. and Zeng, Z.G. (2017) The Numerical Factorization of Polynomials. *Foundations of Computational Mathematics*, **17**, 259-286. https://doi.org/10.1007/s10208-015-9289-1

[15] Galligo, A. and Watt, S. (1997) A Numerical Absolute Primality Test for Bivariate Polynomials. In: *Proceedings of ISSAC*97, ACM Press, New York, 217-224. https://doi.org/10.1145/258726.258788

[16] Rump, S.M. (1999) INTLAB-Interval Laboratory. Springer Netherlands, Berlin. https://doi.org/10.1007/978-94-017-1247-7_7

[17] Rump, S.M. (1983) Solving Algebraic Problems with High Accuracy. In: Kulisch, W.L. and Miranker, W.L., Eds., *A New Approach to Scientific Computation*, Academic Press, San Diego, 51-120. https://doi.org/10.1016/B978-0-12-428660-3.50010-0