密级 _____

中国科学院大学
University of Chinese Academy of Sciences

硕士学位论文

单变元多项式近似最大公因子的次数的可信验证

作者姓名：刘 琦

指导教师：支丽红 研究员

中国科学院数学与系统科学研究院

学位类别：理学硕士

学科专业：应用数学

培养单位：中国科学院数学与系统科学研究院

2013年4月

Verification of the Degree of the Approximate GCD of Univariate Polynomials

By

Qi Liu

A Thesis Submitted to
University of Chinese Academy of Sciences
In partial fulfillment of the requirement
For the degree of
Master of Applied Mathematics

Academy of Mathematics and Systems Science
Chinese Academy of Sciences

May, 2013

摘　要

用符号与数值混合计算方法来计算多项式近似最大公因子 (GCD) 是一个基本而又困难的问题. 很多科研工作者对该问题进行了广泛的研究. 本文主要考虑单变元多项式近似最大公因子次数的可信验证问题. 该问题可以转化为多项式 Bezout 矩阵的子矩阵是秩亏为 1 的可信验证问题. 利用边界矩阵的性质, 证明矩阵是秩亏为 1 等价于证明对应的边界矩阵所定义的非线性隐函数组 $\boldsymbol{f} = \mathbf{0}$. 最终将原可信验证问题转化为非线性隐函数方程组零点的可信验证问题. 我们用隐行列式方法来计算隐函数组的 Jacobian 矩阵, 然后进行牛顿迭代. 特别地, 当多项式的个数为 2 时, Bezout 矩阵是对称矩阵且非线性隐函数组的个数为 1. 基于上述理论, 我们给出了单变元多项式 GCD 次数的可信验证算法 (VUP). 该算法用广义逆方法对扰动初值进行优化并用 INTLAB 包中的 **verifylss** 函数进行区间牛顿迭代. 与以往的多项式最大公因子的研究工作相比, 我们给出的算法是可信的.

关键词： 单变元多项式, 最大公因子, 可信验证

Abstract

It is a fundamental and difficult problem to compute approximate greatest common divisors (GCD) of polynomials using hybrid symbolic-numerical method. This problem has been intensely studied by many authors.

In this paper, we mainly discuss the verification of the degree of the approximate GCD for univariate polynomials with real coefficients: given s polynomials $g_1, \cdots, g_s$ and an integer k, we compute verified error bounds such that there exist perturbed polynomials with exact GCD of degree k. This problem can be transformed into computing verified error bounds such that there exist perturbed polynomials within computed error bounds whose Bezout submatrix has rank deficiency one. Using a bordered system, we can further reduce the problem to verify the implicit functions $\boldsymbol{f} = \mathbf{0}$. To compute verified bounds of the solution of implicit functions $\boldsymbol{f} = \mathbf{0}$, we propose to use the implicit determinant method. Especially, when $s = 2$, the Bezout matrix of two polynomials is symmetrical and the number of implicit functions is one. Finally, this paper presents an algorithm (VUP) for verifying the degree of approximate GCD of univariate polynomials. The VUP algorithm firstly optimizes the initial perturbed coefficient vector of polynomials by using generalized inverse method and then executes interval iterations using **verifylss** in INTLAB package. In comparison to other methods for computing approximate GCD, the degree of the approximate GCD is certified.

Keywords: Univariate polynomial, verification method, approximate GCD

目　　录

第一章　引言

1.1　符号说明

$\mathbb{N}$ 表示非负整数集合.

$\mathbb{N}^*$ 表示正整数集合.

$A_{i,:}$ 表示矩阵 $A \in \mathbb{R}^{m\times n}$ 的第 i 行, 定义如下:

$$A_{i,:} := (A_{i,1}, \ldots, A_{i,n}).$$

$A_{:,j}$ 表示矩阵 $A \in \mathbb{R}^{m\times n}$ 的第 j 列, 定义如下:

$$A_{:,j} := \begin{pmatrix} A_{1,j} \\ \vdots \\ A_{m,j} \end{pmatrix}.$$

$A_{i:j,:}$ 表示矩阵 $A \in \mathbb{R}^{m\times n}$ 的第 i 行到第 j 行组成的子矩阵, 其中 $i \le j$, 定义如下：

$$A_{i:j,:} := \begin{pmatrix} A_{i,1} & \ldots & A_{i,n} \\ \vdots & \vdots & \vdots \\ A_{j,1} & \ldots & A_{j,n} \end{pmatrix}.$$

$A_{:,i:j}$ 表示矩阵 $A \in \mathbb{R}^{m\times n}$ 的第 i 列到第 j 列组成的子矩阵, 其中 $i \le j$, 定义如下：

$$A_{:,i:j} := \begin{pmatrix} A_{1,i} & \ldots & A_{1,j} \\ \vdots & \vdots & \vdots \\ A_{m,i} & \ldots & A_{m,j} \end{pmatrix}.$$

$\mathbb{IR}$ 表示实区间集合, 定义如下:

$$\mathbb{IR} := \{x | x = [a, b], a \le b, a, b \in \mathbb{R}\}.$$

$\mathbb{PR}$ 表示实数集 $\mathbb{R}$ 的所有子集构成的集合, 定义如下:

$$\mathbb{PR} := \{X | X \subseteq \mathbb{R}\}.$$

hull(X) 表示所有包含集合 X 的集合的交; 对于任意的 $X \in \mathbb{PR}$, 定义如下:

$$\text{hull(X)} := \bigcap \{Z \in \mathbb{PR} | X \subseteq Z\}.$$

1.2 预备知识

1.2.1 可信验证

可信验证方法的主要目标是证明在计算出来的一个界内存在给定问题的解. 可信验证方法的一个非常简单的应用是证明一个矩阵的非奇异性.

引理 1.1. [54] *设给定矩阵 $A, R \in \mathbb{R}^{n\times n}$, I 表示 $n \times n$ 阶单位矩阵. 如果 $\|I - RA\| \leq \alpha < 1$, 那么 A 和 R 均非奇异; 并且*

$$\frac{\|R\|}{1+\alpha} \leq \|A^{-1}\| \leq \frac{\|R\|}{1-\alpha}.$$

本论文用到的范数都是谱范数.

引理 1.2. [55] *设给定矩阵 $A \in \mathbb{R}^{m\times n}$, A^+ 表示矩阵 A 的广义逆矩阵. 如果 $\|I - A^T A\| \leq \alpha < 1$, 那么 A 是满秩的; 并且*

$$\|A^+\| \leq \frac{\|A^T\|}{1-\alpha}.$$

注 1. 引理 1.2 给出了证明一个矩阵是满秩的可信验证方法. 然而, 条件 $\|I - A^T A\| \leq \alpha < 1$ 只是一个充分条件并非必要条件. 下面给出一个矩阵 A

$$A = \begin{pmatrix} 1 & 4 \\ 2 & 7 \\ 4 & 1 \end{pmatrix}$$

是列满秩的, 但是 A 和 A^T 不满足引理 1.2 的条件, 计算可得 $\|I - A^T A\| \geq 73$.

引理 1.3. *设矩阵 $A \in \mathbb{R}^{m\times n}$, $R \in \mathbb{R}^{n\times m}$, $m \geq n$. 如果 $\|I - RA\| < 1$, 那么 A 是满秩的.*

证明. 如果 A 不是满秩的, 那么一定存在一个非零向量 $\boldsymbol{x} \in \mathbb{R}^n$ 使得 $A\boldsymbol{x} = \mathbf{0}$. 于是有 $RA\boldsymbol{x} = \mathbf{0}$, 进而 1 为 $I - RA$ 的特征值, 这与 $\|I - RA\| < 1$ 矛盾. □

注 2. 引理 1.3 给了一般矩阵满秩的可信验证方法. 一般情况下, 给定的矩阵 A, 令 $R = \mathrm{inv}(A^TA)\cdot A^T$, 其中 $\mathrm{inv}(A^TA)$ 是由 A^TA 用浮点算法计算得到的近似逆; 那么引理 1.3 的条件 $\|I - RA\| < 1$ 很有可能满足. 当然, 也存在不是广义逆 A^+ 的矩阵 R 使得 $\|I - RA\| < 1$. 值得注意的是引理 1.3 并没有给出 $\|A^+\|$ 的误差界.

Rump [52] 给出了线性稠密系统的可信验证算法, 其中线性系统的矩阵可以是浮点矩阵, 也可以是区间矩阵. 实现这个算法的函数是在 INTLAB 函数包里的 **verifylss** 函数.

定理 1.4. [53] *给定区间矩阵 $A \in \mathbb{IR}^{n\times n}$ 和区间向量 $\boldsymbol{b} \in \mathbb{IR}^n$, 如果函数 **verifylss** 运行成功, 那么该函数计算得到的区间向量 $X \subset \mathbb{IR}^n$ 满足*

$$\Sigma(A, \boldsymbol{b}) := \{x \in \mathbb{R}^n | \widetilde{A}x = \widetilde{\boldsymbol{b}}, \widetilde{A} \in A, \widetilde{\boldsymbol{b}} \in \boldsymbol{b}\} \subseteq X.$$

Moore [47] 给出了非线性系统解的存在性的充分条件; 在此基础上 Krawczyk [35] 给出了证明非线性系统解存在性的牛顿方法区间版本. Rump [56] 做了进一步的研究工作, 改善上述方法使其能够更好地实际应用.

定理 1.5. [56] *设函数 $\boldsymbol{f} : \mathbb{R}^n \to \mathbb{R}^n$, 且 $\boldsymbol{f} = (f_1, \ldots, f_n) \in \mathcal{C}^1$. 给定向量 $\widetilde{\boldsymbol{x}} \in \mathbb{R}^n$, 区间向量 $X \in \mathbb{IR}^n$, $\mathbf{0} \in X$ 以及矩阵 $R \in \mathbb{R}^{n\times n}$, 且给定的区间矩阵 $M \in \mathbb{IR}^{n\times n}$ 满足条件*

$$\{\nabla f_i(\boldsymbol{\zeta}) | \boldsymbol{\zeta} \in \widetilde{\boldsymbol{x}} + X\} \subseteq M_{i,:}.$$

如果

$$-R\boldsymbol{f}(\widetilde{\boldsymbol{x}}) + (I - RM)X \subseteq int(X) \tag{1.1}$$

成立, 其中 $\mathrm{int}(X)$ 是 X 的内点; 那么存在唯一的点 $\widehat{\boldsymbol{x}} \in \widetilde{\boldsymbol{x}} + X$ 使得 $\boldsymbol{f}(\widehat{\boldsymbol{x}}) = 0$. 而且每个矩阵 $\widetilde{M} \in M$ 都是非奇异的.

1.2.2　边界矩阵

为了证明单变元多项式的 GCD 的次数是 k, 我们简要介绍一些边界矩阵的性质 [23, 25, 26, 46].

引理 1.6. 设矩阵 $A \in \mathbb{R}^{m\times n}$, 其中 $m \geq n$ 且 $\mathrm{rank}(A) = n-1$. 设矩阵 A 的零空间 $\mathrm{Nullspace}(A) = \mathrm{span}\{\boldsymbol{\alpha}\}$, 其转置的零空间 $\mathrm{Nullspace}(A^T) = \mathrm{span}\{\boldsymbol{\beta}_0, \ldots, \boldsymbol{\beta}_{m-n}\}$. 如果向量 $\boldsymbol{c} \in \mathbb{R}^n$ 以及向量 $\boldsymbol{b}_0, \ldots, \boldsymbol{b}_{m-n} \in \mathbb{R}^m$ 满足以下条件

$$\boldsymbol{c}^T\boldsymbol{\alpha} \neq 0, \tag{1.2}$$

$$\det \begin{pmatrix} \boldsymbol{\beta}_0^T\boldsymbol{b}_0 & \ldots & \boldsymbol{\beta}_0^T\boldsymbol{b}_{m-n} \\ \vdots & \vdots & \vdots \\ \boldsymbol{\beta}_{m-n}^T\boldsymbol{b}_0 & \ldots & \boldsymbol{\beta}_{m-n}^T\boldsymbol{b}_{m-n} \end{pmatrix} \neq 0; \tag{1.3}$$

那么 $(m+1)\times(m+1)$ 阶矩阵

$$G = \begin{pmatrix} A & \boldsymbol{b}_0 & \ldots & \boldsymbol{b}_{m-n} \\ \boldsymbol{c}^T & 0 & \ldots & 0 \end{pmatrix} \tag{1.4}$$

是非奇异的.

证明. (1.4) 是非奇异的等价于证明下面的线性系统只有零解.

$$\begin{pmatrix} A & \boldsymbol{b}_0 & \ldots & \boldsymbol{b}_{m-n} \\ \boldsymbol{c}^T & 0 & \ldots & 0 \end{pmatrix} \begin{pmatrix} \boldsymbol{\alpha}^* \\ f_0^* \\ \vdots \\ f_{m-n}^* \end{pmatrix} = \begin{pmatrix} \boldsymbol{0} \\ 0 \end{pmatrix} \tag{1.5}$$

将 (1.5) 展开得到

$$\begin{cases} A\boldsymbol{\alpha}^* + \sum_{i=0}^{m-n} \boldsymbol{b}_i f_i^* &= \boldsymbol{0}, \\ \boldsymbol{c}^T\boldsymbol{\alpha}^* &= 0. \end{cases} \tag{1.6}$$

在 (1.6) 第一个等式左乘行向量 $\boldsymbol{\beta}_j^T$, $0 \leq j \leq m-n$. 且由 $\boldsymbol{\beta}_j^T A = \boldsymbol{0}$ 得到如下线性方程组

$$\sum_{i=0}^{m-n} \boldsymbol{\beta}_j^T\boldsymbol{b}_i f_i^* = 0, \quad 0 \leq j \leq m-n.$$

写成矩阵形式如下,

$$\begin{pmatrix} \boldsymbol{\beta}_0^T\boldsymbol{b}_0 & \ldots & \boldsymbol{\beta}_0^T\boldsymbol{b}_{m-n} \\ \vdots & \ddots & \vdots \\ \boldsymbol{\beta}_{m-n}^T\boldsymbol{b}_0 & \ldots & \boldsymbol{\beta}_{m-n}^T\boldsymbol{b}_{m-n} \end{pmatrix} \begin{pmatrix} f_0^* \\ \vdots \\ f_{m-n}^* \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

由 (1.3) 知 $f_0^* = 0, \ldots, f_{m-n}^* = 0$. 于是 (1.6) 简化为

$$\begin{cases} A\boldsymbol{\alpha}^* &= \mathbf{0}, \\ \boldsymbol{c}^T\boldsymbol{\alpha}^* &= 0. \end{cases}$$

由 (1.2) 可知 $\boldsymbol{\alpha}^* = \mathbf{0}$.

□

引理 1.7. [26] 设矩阵 $A \in \mathbb{R}^{m\times n}$, $m \geq n$. 如果向量 $\boldsymbol{b}_0, \ldots, \boldsymbol{b}_{m-n} \in \mathbb{R}^m$, $\boldsymbol{c} \in \mathbb{R}^n$ 以及矩阵 A 构成的 $(m+1)\times(m+1)$ 阶矩阵

$$G = \begin{pmatrix} A & \boldsymbol{b}_0 & \ldots & \boldsymbol{b}_{m-n} \\ \boldsymbol{c}^T & 0 & \ldots & 0 \end{pmatrix} \tag{1.7}$$

是非奇异的, 那么 $\operatorname{rank}(A) = n-1$ 当且仅当线性系统

$$\begin{pmatrix} A & \boldsymbol{b}_0 & \ldots & \boldsymbol{b}_{m-n} \\ \boldsymbol{c}^T & 0 & \ldots & 0 \end{pmatrix} \begin{pmatrix} \boldsymbol{\alpha} \\ f_0 \\ \vdots \\ f_{m-n} \end{pmatrix} = \begin{pmatrix} \mathbf{0} \\ 1 \end{pmatrix} \tag{1.8}$$

的解满足条件 $f_0 = 0, \ldots, f_{m-n} = 0$.

证明. $\Longrightarrow$: (反正法) 假设不存在非零 $\boldsymbol{\gamma}$ 使得 $(\boldsymbol{\gamma}, 0, \ldots, 0)^T$ 是线性系统的 (1.8) 的解. 即方程组 $A\boldsymbol{\gamma} = 0$, $\boldsymbol{c}^T\boldsymbol{\gamma} = 1$ 无非零解. 由于 $\operatorname{rank}(A) = n-1$, 令 $\operatorname{NullSpace}(A) = \operatorname{span}\{\boldsymbol{\alpha}\}$ 那么 $c^T\boldsymbol{\alpha} \neq 0$, 否则与 (1.7) 非奇异性矛盾. 因此一定存在非零 $\lambda \in \mathbb{R}$ 使得 $\lambda\boldsymbol{\alpha}$ 是方程组 $A\boldsymbol{\gamma} = 0$, $\boldsymbol{c}^T\boldsymbol{\gamma} = 1$ 的解; 矛盾.

$\Longleftarrow$: 假设 $(\boldsymbol{\alpha}, 0, \ldots, 0)^T$ 是线性系统 (1.8) 的解, 那么 $A\boldsymbol{\alpha} = \mathbf{0}$ 和 $\boldsymbol{c}^T\boldsymbol{\alpha} = 1$; 因而 $\operatorname{rank}(A) \leq n-1$. 如果 $\operatorname{Nullspace}(A) = \operatorname{span}\{\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2\}$, 那么一定存在不全为零的 $\lambda_1, \lambda_2 \in \mathbb{R}$ 使得 $A(\boldsymbol{\lambda_1}\boldsymbol{\alpha}_1 + \lambda\boldsymbol{\alpha}_2) = \mathbf{0}$ 和 $\boldsymbol{c}^T(\lambda_1\boldsymbol{\alpha}_1 + \lambda_2\boldsymbol{\alpha}_2) = 0$. 这与矩阵 (1.7) 是非奇异的矛盾, 因此矩阵 A 零空间维数至多为 1. 从而 $\operatorname{rank}(A) = n-1$.

□

1.2.3　隐行列式方法

这一小节我们将介绍求解下面行列式方程的方法, 也就是我们所说的隐行列式方法.

$$\det(A(\varepsilon)) = 0 \tag{1.9}$$

这里为了说明该方法的思想, 我们假设 ε 是单变元. 隐行列式方法是构造一个方程

$$f(\varepsilon) = 0, \tag{1.10}$$

使得方程 (1.10) 与 (1.9) 有相同的根, 并且导数 $f_\varepsilon(\varepsilon)$ 容易估计, 从而可以用牛顿法进行迭代.

引理 1.8. [59] 设 $(\boldsymbol{x}^\star, \varepsilon^\star)$ 是下列方程组的根.

$$\begin{cases} A(\varepsilon)\boldsymbol{x} &= \boldsymbol{0}, \\ \boldsymbol{x}^H\boldsymbol{x} &= 1. \end{cases}$$

其中 $A(\varepsilon) \in \mathbb{C}^{n\times n}$ 是 Hermite 矩阵, 且 $\text{Nullspace}(A(\varepsilon^\star)) = \text{span}\{\boldsymbol{x}^\star\}$. 假设 $\boldsymbol{b}^H\boldsymbol{x}^\star \neq 0, \boldsymbol{b} \in \mathbb{C}^n$, 则 $(n+1)\times(n+1)$ 阶矩阵

$$M(\varepsilon) = \begin{pmatrix} A(\varepsilon) & \boldsymbol{b} \\ \boldsymbol{b}^H & 0 \end{pmatrix}$$

在点 $\varepsilon = \varepsilon^\star$ 处是非奇异的.

注 3. 引理 1.8 中要求 $A(\varepsilon)$ 是 Hermite 矩阵; 特别地, 如果 $A(\varepsilon)$ 是实对称矩阵, 且 $\boldsymbol{b}^T\boldsymbol{x}^\star \neq 0, \boldsymbol{b} \in \mathbb{R}^n$, 则结论同样成立. 众所周知两个单变元实系数多项式的 Bezout 矩阵以及它的 k 阶主子式是对称矩阵, 我们将在第 3.3 节中运用隐行列式方法计算隐函数组的 Jacobian 矩阵.

首先注意到 $M(\varepsilon^\star)$ 是非奇异的, 且 $A(\varepsilon)$ 是关于变量 ε 的光滑函数, 因此 $M(\varepsilon)$ 在变量 $\varepsilon^\star$ 的一个邻域内是非奇异的. 其次, 对于 $\varepsilon^\star$ 的一个邻域内的 ε 和满足 $\boldsymbol{b}^H\boldsymbol{x}^\star \neq 0$ 的向量 $\boldsymbol{b}$, 我们引入线性系统

$$\begin{pmatrix} A(\varepsilon) & \boldsymbol{b} \\ \boldsymbol{b}^H & 0 \end{pmatrix} \begin{pmatrix} \boldsymbol{x} \\ f \end{pmatrix} = \begin{pmatrix} \boldsymbol{0} \\ 1 \end{pmatrix}. \tag{1.11}$$

由于矩阵 $M(\varepsilon)$ 是非奇异的, 因此 $\boldsymbol{x}$ 和 f 是关于变量 ε 的光滑函数, 于是我们可以把它们写成 $\boldsymbol{x}(\varepsilon)$ 和 $f(\varepsilon)$. 由 Crammer 法则, 得到

$$f(\varepsilon) = \frac{\det(A(\varepsilon))}{\det(M(\varepsilon))}.$$

上式说明引入线性系统 (1.11) 的精妙之处. 由于 $\det(M(\varepsilon))$ 非零, 则 $f(\varepsilon) = 0$ 当且仅当 $\det(A(\varepsilon)) = 0$. 因此将求解行列式 $\det(A(\varepsilon)) = 0$ 的零点转化成求解方程 $f(\varepsilon) = 0$ 的零点.

定理 1.9. [59] 假设引理 *1.8* 的条件满足, 函数 $\boldsymbol{x}(\varepsilon)$ 和 $f(\varepsilon)$ 是由线性系统 *(1.11)* 定义, 那么

- $f(\varepsilon)=0$ 当且仅当 $\det(A(\varepsilon))=0$;
- 当 $\varepsilon=\varepsilon^{\star}$ 时, 由 *(1.11)* 计算得到的 $\boldsymbol{x}(\varepsilon^{\star})$ 是 $A(\varepsilon^{\star})$ 的零空间向量.

更精确地说, 隐行列式法就是将牛顿迭代应用到线性系统 (1.11) 定义的函数 $f(\varepsilon)$ 中. 为了进行牛顿迭代, 我们需要计算 $f_{\varepsilon}(\varepsilon)$. 对此, 我们将线性系统 (1.11) 关于变量 ε 进行微分

$$\begin{pmatrix} A(\varepsilon) & \boldsymbol{b} \\ \boldsymbol{b}^{H} & 0 \end{pmatrix} \begin{pmatrix} \boldsymbol{x}_{\varepsilon}(\varepsilon) \\ f_{\varepsilon}(\varepsilon) \end{pmatrix} = - \begin{pmatrix} A_{\varepsilon}(\varepsilon)\boldsymbol{x}(\varepsilon) \\ 0 \end{pmatrix}. \tag{1.12}$$

注意到求解 $f_{\varepsilon}(\varepsilon)$ 与 $f(\varepsilon)$ 都是用的相同的矩阵, 不同之处在于右端向量.

算法 1.1. 隐行列式算法

给定 ε^{0} 和 $\boldsymbol{b}\in\mathbb{C}$ 使得 $M(\varepsilon^{0})$ 是非奇异的.

- 令 $\varepsilon=\varepsilon^{i}$, 求解线性系统 *(1.11)* 得到 $f(\varepsilon^{i})$.
- 令 $\varepsilon=\varepsilon^{i}$, 利用上一步计算结果 $\boldsymbol{x}(\varepsilon^{i})$, 计算线性系统 *(1.12)* 的右端向量; 进而求解线性系统 *(1.12)* 得到 $f_{\varepsilon}(\varepsilon^{i})$.
- 牛顿迭代
$$\varepsilon^{i+1}=\varepsilon^{i}-\frac{f(\varepsilon^{i})}{f_{\varepsilon}(\varepsilon^{i})}.$$
- 迭代终止条件
$$\|\varepsilon^{i+1}-\varepsilon^{i}\|\leq tol.$$
其中 tol 是迭代容差.

算法 1.1 所用到的线性系统 (1.12) 是对单变元的情况, 对于多变元情况, 我们只需将线性系统 (1.11) 对每一个变量进行微分, 可以得到 $f(\boldsymbol{\varepsilon})$ 的 Jacobian 矩阵. 具体的推导过程我们将在 3.3 中详细介绍.

1.3 问题概述

用符号与数值混合计算方法来计算单变元多项式近似 GCD 问题是一个基本而又困难的问题. 很多学者对近似 GCD 问题进行了广泛的研究. 下面简要介绍多项式近似 GCD 问题的研究背景。

Collins [12]和 Brown [7]在无误差的情况下给了多项式精确 GCD 的算法. 当多项式信息不完全时, 近似多项式问题都会成为亟待解决的问题. 于是人们开始研究有理系数, 实系数, 复系数多项式在给定的误差范围内扰动多项式的 GCD 问题. 误差的出现改变了计算机代数问题的一些传统的性质. 例如, 传统的问题: 给定两个有理系数多项式, 他们是否存在非平凡 GCD ? 给定一个有理系数多项式是否含有 r 重根? 在有误差的情况可能变为: 给定的两个多项式附近是否有两个扰动多项式具有非平凡的 GCD ? 在给定有理系数多项式附近是否存在一个扰动多项式有 r 重根? 近似 GCD 的计算是一个不稳定的问题, 对一个多项式进行一个非常小的扰动可能完全改变问题的答案.

多项式近似 GCD 问题已经被很多科学工作者研究过. Schonhage [58] 假设输入可以是任意精度, 即多项式系数的精度可以根据需要而设定. Nada 和 Sasaki [43] 提出了计算给定多项式近似最大公因子的欧几里得算法. Hribernig 和 Stetter [30] 用多项式子结式链方法给出了近似 GCD 次数的下界. Corless [13] 则将奇异值分解方法应用到 f, g 的 Slyvester 矩阵, 并将该方法用于求解多项式系统近似零点. Pan [44] 提出用几何算法来寻找相邻的近似根. Zeng [69] 用求根法和最小二乘法来求解多变元多项式近似 GCD 问题.

上述算法是在不同的假设条件下给出计算多项式附近具有非平凡 GCD 的扰动多项式的方法. 但是他们都有一个共同点：没有给出确保能够计算出结果的一个容差. 即在给定多项式的容差 ε 范围内是否存在具有非平凡 GCD 的扰动多项式. 针对这个问题, Emirs [20, 21] 提出 gap theorem, 在某些特定的情形下用该理论修改 SVD (Singular Value Decomposition) 算法并成功求解 GCD. Karmarkar 和 LakshmanL [34] 给出了在给定的误差界内求解近似公因子的算法. Rupprecht [57] 考虑在给定容差 ε 下求解 GCD 的次数最高的扰动多项式问题, 并用广义 Sylvester 矩阵和 SVD 分解来求解该问题.

2006 年 Kaltofen [33] 等人考虑的问题是给定的一组互素实(复)数域上的多变元多项式, 如何计算出最小的实(复)多项式系数扰动使得扰动多项式 GCD 的次数至少是给定的整数 k. 该文章中给出了基于结构全局最小范数的算法

(STLN). 2011 年 Mourrain[11] 等人考虑两个单变元多项式 $f, g \in \mathbb{C}_d[x] \setminus \{0\}$ 在半径为 ε 的扰动圆盘内找到一个扰动使得扰动多项式有一个非平凡的精确 GCD , 作者将该问题转化为一个优化问题:

$$\begin{cases} \min & \|f-p\|^2 + \|g-q\|^2 \\ \text{s. t.} & f, g \in \mathbb{C}_d[x] \setminus \{0\}, \\ & \text{Resultant}_d(p,q) = 0. \end{cases}$$

并用 Smale's α 理论来证明在一个圆盘内单变元多项式最近 GCD 的存在性和唯一性.

我们结合近似 GCD 问题和可信验证方法, 提出如下问题。

问题 1.1.
设单变元多项式 $g_1, \ldots, g_s \in \mathbb{R}[x] \setminus \{0\}$, 其中 $\deg(g_i) = d_i$, $1 \le i \le s$. 设 $d_1 = \max(d_1, \ldots, d_s)$, $g_1, \ldots, g_s$ 的近似 GCD 的次数是 k, $g_1, \ldots, g_s$ 的系数扰动多项式定义如下:

$$g_i(\boldsymbol{\varepsilon}_i) := g_i + \sum_{j=0}^{d_i} \boldsymbol{\varepsilon}_{i,j} x^j, \quad i = 1, ..., s,$$

其中 $\boldsymbol{\varepsilon}_1, \ldots, \boldsymbol{\varepsilon}_s$ 是参变量向量. 如何给一个多项式 $g_1, \ldots, g_s$ 系数的扰动范围 $E_1, \ldots, E_s$, 使得一定存在一个扰动 $\widehat{\boldsymbol{\varepsilon}}_1 \in E_1, \ldots, \widehat{\boldsymbol{\varepsilon}}_s \in E_s$, 满足

$$\deg(\text{GCD}(g_1(\widehat{\boldsymbol{\varepsilon}}_1), \ldots, g_s(\widehat{\boldsymbol{\varepsilon}}_s))) = k.$$

我们在 3.3 展示怎样将单变元多项式近似 GCD 次数的可信验证问题转化为多项式 Bezout 矩阵的子矩阵秩亏为 1 的可信验证问题. 利用边界矩阵的性质, 证明多项式 Bezout 矩阵的子矩阵秩亏为 1 等价于求解隐函数方程组的零点. 最后利用函数包 INTLAB 里的函数计算隐函数方程组零点的可信区间.

1.4　论文的结构和主要结果

在这篇文章中, 我们简要介绍可信验证概述, 主要讨论非精确单变元多项式近似 GCD 次数的可信验证问题.

第二章主要分成两个部分: 浮点算法与区间算法, 可信验证方法. 第一部分首先介绍用浮点算法进行计算存在的问题, 其次介绍区间算法的引入. 第二部

分介绍以区间算法为基础发展起来的可信验证. 该部分首先介绍了可信验证方法处理的典型问题, 以及可信验证方法的设计原则和可解原则. 其次指出了可信计算过程中大家可能会进入的一些误区. 最后简要介绍了可信验证的发展历程.

第三章主要分成两个部分: 单变元多项式的 GCD 与 Bezout 矩阵, 单变元多项式近似 GCD 次数可信验证. 第一部分首先介绍两个单变元多项式 Bezout 矩阵的定义, 阐明两个单变元多项式 GCD 次数与其 Bezout 矩阵亏秩的关系. 其次, 介绍多个单变元多项式 Bezout 矩阵的定义, 以及多个单变元多项式 GCD 的次数与 Bezout 矩阵的子矩阵亏秩的关系. 第二部分是论文的核心内容, 详细介绍单变元多项式近似 GCD 次数可信验证问题的求解思路. 首先介绍如何将单变元多项式近似 GCD 次数可信验证问题转化为非线性隐函数方程组零点的可信验证问题. 其次分析了非线性隐函数组 $\boldsymbol{f}(\varepsilon)$ 变量个数与方程个数的大小关系. 最后, 在非线性隐函数组 $\boldsymbol{f}(\varepsilon)$ 是欠定的情况下, 用隐行列式方法计算 $\boldsymbol{f}(\varepsilon)$ 的 Jacobian 矩阵并用固定变量法将欠定系统 $\boldsymbol{f}(\varepsilon)$ 转化为正规系统 $\boldsymbol{f}(\varepsilon_{\mathcal{I}})$.

第四章包括两个部分: VUP 算法和数值试验. 根据第三章的理论, 我们给出单变元多项式近似 GCD 次数可信验证算法 (VUP). 该算法主要分三个步骤, 首先用广义逆方法对初值进行优化, 其次用固定变量法将欠定系统 $\boldsymbol{f}(\varepsilon)$ 转化为正规系统 $\boldsymbol{f}(\varepsilon_{\mathcal{I}})$, 最后进行区间牛顿迭代. 我们已经完成两个单变元多项式近似 GCD 次数的可信验证算法, 而且对所给的例子都能在合适的初值和初值区间下计算得到可信区间.

最后一章我们总结了已有的工作成果, 并讨论了以后可以继续努力的研究方向.

第二章　可信验证概述

2.1　浮点算法与区间算法

在符号和数值混合计算过程中, 算法只有在计算机上编译才能实现. 因为计算机只能存储有限位数, 大多数实数在计算机上是以不精确的浮点数来表示. 这种存储上的误差不可避免地会影响到计算结果. 计算机上的浮点算法可能造成额外的误差. 一般减少误差的想法是用更多的位数来表示一个实数. 然而下面的例子告诉我们更多的位数根本不能完全解决问题.

一个简单而极端的例子

$$\begin{aligned} x_0 &= 1; \\ x_1 &= \frac{1}{3}; \\ x_{n+1} &= \frac{13}{3}x_n - \frac{4}{3}x_{n-1}, \quad n = 1, 2, 3, \cdots . \end{aligned}$$

在计算机上用浮点算法得到计算结果显示该序列将收敛到 $-\infty$ 或者 $+\infty$ ($-\infty$ 还是 $+\infty$ 取决于计算机, 编程语言以及编译程序). 但是不管是采用单精度还是双精度来进行计算, 结果都是如此. 进行推导可以证明该序列等同于如下序列:

$$x_n = \left(\frac{1}{3}\right)^n, \quad n = 0, 1, 2, \cdots .$$

在数学意义上, 上述迭代序列应该收敛到 0.

众所周知, 函数 f 在 $x = x_0$ 处导数的定义是 $f'(x_0) = \lim\limits_{h\to 0} \dfrac{f(x_0+h) - f(x_0)}{h}$. 如果在计算机上构造一个数值序列, 当 h 趋近于 0 时, 估计 $f'(x_0)$ 的值; 那么我们可以断言所有连续函数都可导, 而且导函数几乎处处为零. 造成这种结果的原因是当 h 足够小的时候, $f(x_0+h)$ 和 $f(x_0)$ 在计算机上存储的值相同. 以上两个例子告诉我们浮点算法得到的数值解并不一定可信.

另一方面, 在符号计算问题中, 如果问题的输入包含不精确的浮点数, 那么输出结果比如公因式、因式分解或稀疏内插式等可能是平凡的. 一般浮点算法只能给出数学问题的一个近似解. 在数学的实际应用中, 为了简化进一步的推

导工作, 许多分析工作是在已有结果的基础上进行的. 浮点算法得到的近似解与精确解之间的误差将会累积到进一步的求解和分析过程中.

下面我们将给出一系列简单的例子来说明区间的出现是很自然的.

1. **物理常数或度量**

   通常我们知道的都是近似值. 例如, 重力加速度 g 的额定值为

   $$g = 9.80665\, m/s^2.$$

   事实上, g 的值取决于所在位置的高度, 其范围是 $[9.8045, 9.8082]$. 因此对 g 准确的描述是

   $$g \in [9.8045, 9.8082]\, m/s^2.$$

2. **数的表示**

   无论是笔算还是机器计算, 所有的数都只能用有限位数表示; 如

   $$\frac{1}{3} \approx 0.33333, \sqrt{2} \approx 1.4142, \pi \approx 3.1416.$$

   这就意味着有舍入误差. 如果能够用上下界来界定一个数, 那么这种表示方法将更加精确. 下面是五位有效数的表示

   $$\frac{1}{3} \in [0.33333, 0.33334], \sqrt{2} \in [1.4142, 1.4143], \pi \in [3.1415, 3.1416].$$

为了得到可信的数值解, 在二十世纪五十年代后期 R.E.Moore 在 [49] 中介绍了他的方法. 为了表示一个实数 r, 他提出用计算机中包含 r 的区间来表示, 而不是传统的截断或者舍入. 例如, 在计算机上无理数 π 可以表示为区间 $[3.141592653, 3.141592654]$. 用区间表示的数之间的运算也应该用区间来表示, 他定义区间运算如下:

定义 2.1. 区间运算

设 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 是两个实数区间, op 表示算术运算 (+, -, *, /). 那么 $\boldsymbol{x}$ op $\boldsymbol{y} = \{x \text{ op } y | \forall x \in \boldsymbol{x}, y \in \boldsymbol{y}\}$.

更多的区间算法运算和分析可以参考文献 [53]. 区间表示和区间运算的一大优点是可信. 基于区间分析的算法得到进一步的发展, 有兴趣的读者可以参考 [50] 和其他相关区间分析的文献. 在不等式, 近似值, 误差界以及有界凸集等相关实际工作中, 区间算法都是一个精美的工具. 区间算法在工业应用, 投资组合管理, 现金流风险控制以及基因搜索等方面的应用, 读者可以参看文章 [10].

2.2　可信验证

传统的数学证明是用笔和纸来完成的, 现在有很多数学问题的证明运用到计算机. 然而, 不管是用计算机来证明还是证明过程中用到计算机, 这种想法并不容易让人接受. 可信验证方法是, 对于给定的一个待证问题, 构造算法并证明用该算法计算出的区间内一定存在该问题的解. 下面是几个利用计算机来辅助证明的例子:

- 10 阶有限射影平面的非存在性证明.
- 李型单群 ($2^8 \cdot 3^7 \cdot 5^6 \cdot 7 \cdot 11 \cdot 31 \cdot 37 \cdot 67$ 阶) 的存在性.
- Thompson 单群的唯一性和 O'Nan 群的存在性.

上述例子的证明具有一个共同点: 基于整数计算, 没有误差. 下面的例子是基于浮点计算来进行证明的.

- 保积映射的普遍性证明.
- 离散动力系统中混沌的可信验证.
- 双泡猜想的证明.
- Lorenz 型方程组混沌的可信验证.
- Sturm-Liouville 问题低于本质谱的特征值存在性证明.

其他的一些例子, 读者可以参见 Frommer [22].

我们提到数学问题的整个证明过程有可能都在计算机上进行实现(需要程序员的精巧编译). 从这方面来看, 有很多的项目, 例如：证明助手如 Coq [67], 定理证明程序如 HOL [40], 定理证明和区间计算相结合 [15, 29], FMathL [41].

大量的非平凡的数学定理的证明是通过计算机来实现的, 包括大家熟知的代数基本定理, 三等分 60° 角的不可能性, 素数定理, Brouwer 不动点定理. 其他一些在计算机上实现的常规证明, 如有限项的积分. 对于由基本算术操作和基本标准函数构成的函数, Risch [51] 提出了一个算法来确定其积分存在性 (如果存在, 则最终计算出结果). 这个算法在 Maple (2009) 和 Mathematica (2009) 中实现, 可以在有限时间内计算出结果.

2.2.1 可信验证方法的原则

可信验证方法也称为自验证方法, 该方法阐明了如何将浮点算法用于严格证明. 用可信验证方法处理的典型问题包括

- 判断一个给定的矩阵的非奇异性.
- 计算函数 $f : D \subseteq \mathbb{R}^n \to \mathbb{R}$ 的最小值的误差界.
- 计算非线性系统 $f(x) = 0$ 零点的可信误差界.
- 计算常微分方程或者偏微分方程解的可信误差界.

大多数可信验证方法都依赖于一个好的近似初值. 尽管每个问题的解的性质可能不尽相同, 但他们求解过程中的有如下相同点.

可信验证方法的设计原则:
数学定理的假设条件的证明是在计算机的辅助下完成的.

可信验证方法是数学定理和实际应用相互作用的产物. 主要任务就是由定理和定理假设条件导出方法使得可信验证很可能成功. 绝大多数这样定理的条件是充分条件, 即如果条件满足, 那么断言为真; 如果不满足, 不能说明任何问题. 假设条件的可信验证是基于浮点算法的估计. 下面是哈达玛给出的一个问题的适定性定义: 如果一个问题有唯一解并且这个唯一解连续地依赖于输入数据, 那么我们称这个问题是适定的. 可信验证方法就是通过证明解的存在性和唯一性来求解问题的. 因此舍入误差的出现就意味着可信验证方法求解适定性问题.

可信验证方法的可解原则:
可信验证方法求解适定性问题.

一个典型的例子, 现在已经有很有效的可信验证方法来证明一个矩阵的非奇异性; 但是, 矩阵的奇异性的证明却超出了可信验证的范围, 因为在任何一个矩阵的开邻域内都有非奇异矩阵.

可信验证方法的目标是在考虑所有可能误差来源的情况下, 特别是舍入误差, 计算出严格的误差界使得在数学意义上是正确的. 进一步的目标是导出求解某类问题的可信验证算法, 其计算速度不低于现有的最好的数值算法的速度.

一般而言, 给定某个数值算法, 人们可能会问对于一个数值问题我们是否有必要计算可信的误差界. 我们可以引用 Willian Kahan 的话来回答“数值误差是稀少的, 稀少到并不需要总是考虑他; 但也并不是稀少到我们可以忽略他.”除此之外, 没有人会承认, 哥德巴赫猜想很可能是正确的仅仅是因为在数万亿的试验中没有找到反例.

可信验证方法与一般的增加可靠性的方法有本质的区别. 例如, Porte和 Vignes [45], Vignes [64, 65], Stewart [60] 和 Chatelin [8] 先后发展了随机方法. Demmel [16] 提出一个线性系统求解程序, 该程序用改良的迭代进行精化并在数以百万计的例子中证明了可信性; 但是他们中没有一个方法可以声称得到的结果肯定是可信的.

2.2.2　众所周知的陷阱

我们需要为严格的可信验证指定工具. 众所周知, 近似解有小的残差不足以说明精确解就在其附近. 同样地, 离散问题的解不需要在连续问题解的附近. 另外, 在不同的精度下计算出相似的近似, 这并不意味着这个近似值在精确值附近. 为了说明这个问题我们引用 Rump (1994) 构造的例子来加以说明.

$$f = 333.75b^6 + a^2(11a^2b^2 - b^6 - 121b^4 - 2) + 5.5b^8 + \frac{a}{2b}, \tag{2.1}$$

其中 $a = 77617, b = 33096$, 在 IBM 大型主机上进行计算, 分别以单精度, 双精度, 扩展精度计算得到的结果如下

$$\begin{array}{ll} \text{单精度} & f \approx 1.172603\cdots \\ \text{双精度} & f \approx 1.1726039400531\cdots \\ \text{扩展精度} & f \approx 1.172603940053178\cdots \end{array}$$

事实上, 精确解为 $f = -0.827386\cdots = \frac{a}{2b} - 2$.

(2.1) 的主要部分 (除了最后一个分式) 的和是 -2. 碰巧的是主要部分的浮点计算在所有精度下都近似于零; 因此计算结果近似于 $\frac{a}{2b}$. 进一步的分析可以参考 Cuyt, Verdonk, Becuwe 和 Kuterna [14] 以及 Loh 和 Walster [38].

2.2.3　可信验证发展历程

可信验证的发展历程可以分成三个主要阶段.

第一阶段, Young [68], Dwyer [19], Warmus [66] 等许许多多的的文章都定义了区间运算; 但是没有对端点进行恰当地舍入.

第二阶段, 主要的进步是用区间算法求解问题. Sunaga [63] 在东京大学时期的硕士论文中介绍:

- 区间格子, 从属分配定律, 微分, 梯度以及把区间看作拓扑群的观点等等,
- 用外舍入界来确定上下确界和中心半径的算法, 实区间, 复区间也包括高维情形,
- 包含属性, 包含原则以及子集的性质,
- 中心形式, 改良值域估计的细分,
- 区间牛顿算法,
- 标准函数精确估计的可信插值,
- 通过余数表示方法快速实现计算机算法,
- Simpson 法则求解定积分的包含,
- 逐步求精法解 ODE 方程.

Moore [48] 博士论文的发表, 掀起区间算法的热潮. Hansen 和 Smith [27] 提出的先决条件极大地挤压了对区间运算的过分高估的泡沫. 直到二十世纪七十年代中期, 严格地计算出 Simpson 法则的误差估计, Krawczyz [35] 中引入区间牛顿算法并计算得到可信验证区间. Alefeld 和 Herzberger [1] 中很多非平凡的数学问题得到进一步的解决.

第三阶段, Moore [47] 提出的存在性测试开启了可信验证领域的第三阶段, 使得可信验证从区间跨越到可信验证方法. 不管是有限维的 Brouwer 不动点定理还是无限维 Schauder 不动点定理均被用于证明一个问题的解在计算出的区间内. 为了构造这样的区间, Rump [52] 提出了一种迭代方法. 该方法是可信验证方法的标准方法.

第三章　单变元多项式近似 GCD 次数的可信验证

3.1　前言

用符号与数值混合计算方法来计算单变元多项式近似 GCD 的问题是一个基本而又困难的问题. 很多科研工作者对该问题进行了广泛地研究. 文献 [31] 中介绍多项式近似 GCD 的问题的各种算法. 在 [36, 42] 中, 引入平方和方法 (SOS) 来计算可信的扰动下界, 使得扰动的多项式的 GCD 次数是给定的值. 而在 [11] 中, 用 Smale's α 理论来证明在一个圆盘内单变元多项式最近 GCD 的存在性和唯一性.

本章首先介绍单变元多项式的 GCD 与 Bezout 矩阵, 阐明单变元多项式 GCD 次数与其 Bezout 矩阵的子矩阵秩亏的关系. 其次, 为了计算多项式 GCD 次数的可信验证区间, 我们将该问题转化为计算多项式 Bezout 矩阵的子矩阵秩亏为 1 的可信验证区间. 根据边界矩阵的性质, 矩阵秩亏为 1 等价于边界矩阵定义的隐函数组 $\boldsymbol{f} = 0$. 最后, 我们用隐行列式方法来计算隐函数组的 Jacobian 矩阵, 然后进行牛顿迭代. 特别地, 当单变元多项式的个数是 2 时, Bezout 矩阵是对称矩阵且非线性隐函数组 $\boldsymbol{f}$ 的个数为 1.

3.2　单变元多项式的 GCD 与 Bezout 矩阵

众所周知, Bezout 矩阵可以用来计算单变元多项式的 GCD, 读者可以参考文献 [2–6, 17, 18, 24, 28, 61, 62]. 同样两个单变元多项式, 他们的 Bezout 矩阵的维数比相应地 Slyvester 矩阵小, 而且两个单变元多项式的 Bezout 矩阵及其 k 阶主子式是对称矩阵.

设两个单变元非零多项式 $g_1, g_2 \in \mathbb{R}[x] \setminus \{0\}$, 次数分别是 $\deg(g_1) = m$ 和 $\deg(g_2) = n$, $m \geq n$; 设其表达式如下:

$$g_1 = u_m x^m + u_{m-1} x^{m-1} + \ldots + u_1 x + u_0, u_m \neq 0,$$
$$g_2 = v_n x^n + v_{n-1} x^{n-1} + \ldots + v_1 x + v_0, v_n \neq 0.$$

则他们的 Bezout 矩阵定义为 $\widehat{B}(g_1, g_2) = (\widehat{b}_{i,j})$, 其元素为

$$\widehat{b}_{i,j} = |u_0 v_{i+j-1}| + |u_1 v_{i+j-2}| + \ldots + |u_k v_{i+j-k-1}|,$$

其中 $|u_r v_s| = u_r v_s - u_s v_r$, $k = \min(i-1, j-1)$. 如果 $r > n$, 则 $v_r = 0$. 注意此处 Bezout 矩阵的定义与 Maple 中的定义不同; Maple 中定义如下:

$$B(g_1, g_2) = -J\widehat{B}(g_1, g_2)J,$$

其中 J 是反对角单位阵. Maple 中定义的 Bezout 矩阵 $B(g_1, g_2)$ 相当于将矩阵 $\widehat{B}(g_1, g_2)$ 旋转 180° 后再取负; 本质上两种定义是一样的.

定理 3.1. [61] *设 $g_1, g_2 \in \mathbb{R}[x] \setminus \{0\}$ 是两个非零单变元多项式, $\deg(g_1) = m$, $\deg(g_2) = n$ 且 $m \geq n$. 如果 $\deg(\gcd(g_1, g_2)) = k$, 那么 $\operatorname{rank}(B(g_1, g_2)) = m - k$ 且*

$$\det(B(g_1, g_2)_{1:l,1:l}) \begin{cases} \neq & 0, \quad l \leq m-k, \\ = & 0, \quad l > m-k. \end{cases}$$

两个单变元多项式的 Bezout 矩阵可以推广到多个非零单变元多项式. 设 $g_1, \ldots, g_s \in \mathbb{R}[x] \setminus \{0\}$ 其中 $\deg(g_i) = d_i$, $1 \leq i \leq s$. 假设 $d_1 = \max(d_1, \ldots, d_s)$, 那么 $B(g_1, \ldots, g_s) \in \mathbb{R}^{(s-1)d_1 \times d_1}$ 可以定义为

$$B(g_1, \ldots, g_s) = \begin{pmatrix} B(g_1, g_2) \\ B(g_1, g_3) \\ \vdots \\ B(g_1, g_s) \end{pmatrix}.$$

定理 3.2. [62] *设单变元多项式 $g_1, \ldots, g_s \in \mathbb{R}[x] \setminus \{0\}$, 其中 $\deg(g_i) = d_i$, $1 \leq i \leq s$, 设 $d_1 = \max(d_1, \ldots, d_s)$, 那么 $\deg(\mathrm{GCD}(g_1, \ldots, g_s)) = k$ 当且仅当 Bezout 矩阵的前 $d_1 - k + 1$ 列 $B(g_1, \ldots, g_s)_{:,1:d_1-k+1}$ 是秩亏为 1.*

注 4. 当 $s = 2$ 时, 定理 3.2 的结论简化为 $\deg(\mathrm{GCD}(g_1, g_2)) = k$ 当且仅当 Bezout 矩阵的前 $d_1 - k + 1$ 列 $B(g_1, g_2)_{:,1:d_1-k+1}$ 是秩亏 1 的. 一方面, 定理 3.1 告诉我们 $\deg(\mathrm{GCD}(g_1, g_2)) = k$, 则 $B(g_1, g_2)_{1:d_1-k+1,1:d_1-k+1}$ 是秩亏 1 的. 另一方面, 如果 $B(g_1, g_2)_{1:d_1-k+1,1:d_1-k+1}$ 是秩亏 1 的, 那么 $B(g_1, g_2)_{:,1:d_1-k+1}$ 一定是秩亏 1 的, 因此 $\deg(\mathrm{GCD}(g_1, g_2)) = k$.

推论 3.3. *设两个单变元非零多项式 $g_1, g_2 \in \mathbb{R}[x] \setminus \{0\}$, $d_1 = \max(d_1, d_2)$, $\deg(\mathrm{GCD}(g_1, g_2)) = k$ 当且仅当 $B(g_1, g_2)_{1:d_1-k+1,1:d_1-k+1}$ 是秩亏为 1.*

3.3　单变元多项式近似 GCD 次数的可信验证

问题 3.1.

设单变元多项式 $g_1,\ldots,g_s \in \mathbb{R}[x]\setminus\{0\}$, 其中 $\deg(g_i)=d_i$, $1\le i\le s$, 设 $d_1=\max(d_1,\ldots,d_s)$, $g_1,\ldots,g_s$ 的近似 GCD 的次数是 k, $g_1,\ldots,g_s$ 的系数扰动多项式定义如下:

$$g_i(\boldsymbol{\varepsilon}_i) := g_i + \sum_{j=0}^{d_i} \boldsymbol{\varepsilon}_{i,j} x^j, \quad i=1,...,s,$$

其中 $\boldsymbol{\varepsilon}_1,\ldots,\boldsymbol{\varepsilon}_s$ 是参变量向量. 如何给一个多项式 $g_1,\ldots,g_s$ 系数的扰动区间 $E_1,\ldots,E_s$, 使得一定存在一个扰动 $\widehat{\boldsymbol{\varepsilon}}_1\in E_1,\ldots,\widehat{\boldsymbol{\varepsilon}}_s\in E_s$, 满足

$$\deg(\mathrm{GCD}(g_1(\widehat{\boldsymbol{\varepsilon}}_1),\ldots,g_s(\widehat{\boldsymbol{\varepsilon}}_s)))=k.$$

这是一个 GCD 可信验证问题. 定理 3.2 结果表明 $\deg(\mathrm{GCD}(g_1,\ldots,g_s))=k$ 与 Bezout 矩阵的前 d_1-k+1 列 $B(g_1,\ldots,g_s)_{:,1:d_1-k+1}$ 是秩亏为 1 等价. 而引理 1.7 给出了一个矩阵是秩亏为 1 的等价条件. 以上定理和引理的结果给了我们求解问题的方法.

我们令

$$A(\boldsymbol{\varepsilon}_1,\ldots,\boldsymbol{\varepsilon}_s) := B(g_1(\boldsymbol{\varepsilon}_1),\ldots,g_s(\boldsymbol{\varepsilon}_s))_{:,1:d_1-k+1}.$$

假设 $A(\boldsymbol{\varepsilon}_1,\ldots,\boldsymbol{\varepsilon}_s)\subseteq\mathbb{R}^{m\times n}(\boldsymbol{\varepsilon}_1,\ldots,\boldsymbol{\varepsilon}_s)$. 构造矩阵 $G(\boldsymbol{\varepsilon}_1,\ldots,\boldsymbol{\varepsilon}_s)$ 如下:

$$G(\boldsymbol{\varepsilon}_1,\ldots,\boldsymbol{\varepsilon}_s) := \begin{pmatrix} A(\boldsymbol{\varepsilon}_1,\ldots,\boldsymbol{\varepsilon}_s) & \boldsymbol{b}_0 & \ldots & \boldsymbol{b}_{m-n} \\ \boldsymbol{c}^T & 0 & \ldots & 0 \end{pmatrix} \tag{3.1}$$

其中 $\boldsymbol{c}\in\mathbb{R}^n$, $\boldsymbol{b}_i\in\mathbb{R}^m, 0\le i\le m-n$. 如果对于某个扰动系数向量 $(\widetilde{\boldsymbol{\varepsilon}}_1,\ldots,\widetilde{\boldsymbol{\varepsilon}}_s)$, 矩阵 $G(\widetilde{\boldsymbol{\varepsilon}}_1,\ldots,\widetilde{\boldsymbol{\varepsilon}}_s)$ 是非奇异的, 那么一定存在向量 $(\widetilde{\boldsymbol{\varepsilon}}_1,\ldots,\widetilde{\boldsymbol{\varepsilon}}_s)$ 的某个邻域 $\boldsymbol{U}(\widetilde{\boldsymbol{\varepsilon}}_1,\ldots,\widetilde{\boldsymbol{\varepsilon}}_s)$, 矩阵 $G(\boldsymbol{\varepsilon}_1,\ldots,\boldsymbol{\varepsilon}_s)$ 是非奇异的. 进一步, 对于每一个邻域 $\boldsymbol{U}(\widetilde{\boldsymbol{\varepsilon}}_1,\ldots,\widetilde{\boldsymbol{\varepsilon}}_s)$ 内的点, 线性系统

$$\begin{pmatrix} A(\boldsymbol{\varepsilon}_1,\ldots,\boldsymbol{\varepsilon}_s) & \boldsymbol{b}_0 & \ldots & \boldsymbol{b}_{m-n} \\ \boldsymbol{c}^T & 0 & \ldots & 0 \end{pmatrix} \begin{pmatrix} \boldsymbol{\alpha} \\ f_0 \\ \vdots \\ f_{m-n} \end{pmatrix} = \begin{pmatrix} \boldsymbol{0} \\ 1 \end{pmatrix} \tag{3.2}$$

都有唯一解. 因此线性系统 (3.2) 定义了函数组

$$(\boldsymbol{\alpha}, f_0, \cdots, f_{m-n})^T : \boldsymbol{U}(\widetilde{\varepsilon}_1, \ldots, \widetilde{\varepsilon}_s) \longrightarrow \mathbb{R}^{m+1}$$

而 (3.2) 是函数组 $(\boldsymbol{\alpha}, f_0, \cdots, f_{m-n})^T$ 的隐函数方程.

由上面所述, 矩阵 $G(\varepsilon_1, \ldots, \varepsilon_s)$ 在邻域 $\boldsymbol{U}(\widetilde{\varepsilon}_1, \ldots, \widetilde{\varepsilon}_s)$ 内是非奇异的, 根据引理 1.7 可推出, $A(\varepsilon_1, \ldots, \varepsilon_s)$ 是秩亏为 1 当且仅当

$$(f_0(\varepsilon_1, \ldots, \varepsilon_s), \ldots, f_{m-n}(\varepsilon_1, \ldots, \varepsilon_s)) = \mathbf{0}.$$

至此, 我们将求解 $\deg(\mathrm{GCD}(g_1(\varepsilon_1), \ldots, g_s(\varepsilon_s))) = k$ 的点转换为求解方程组 $(f_0, \cdots, f_{m-n})^T = \mathbf{0}$ 的零点. 证明的思路如下:

$$\deg(\mathrm{GCD}(g_1(\varepsilon_1), \ldots, g_s(\varepsilon_s))) = k \tag{3.3}$$

$$\xrightarrow{\text{定理3.2}} \mathrm{corank}(A(\varepsilon_1, \ldots, \varepsilon_s)) = 1 \tag{3.4}$$

$$\xrightarrow[G\text{非奇异}]{\text{引理1.7}} (f_0, \cdots, f_{m-n})^T = \mathbf{0}. \tag{3.5}$$

下面我们将讨论非线性函数组

$$\boldsymbol{f}(\varepsilon_1, \ldots, \varepsilon_s) = (f_0(\varepsilon_1, \ldots, \varepsilon_s), \ldots, f_{m-n}(\varepsilon_1, \ldots, \varepsilon_s)) \tag{3.6}$$

零点的可信验证. 由多项式的 Bezout 矩阵定义可知矩阵 $A(\varepsilon_1, \ldots, \varepsilon_s)$ 是 $(s-1)d_1 \times (d_1 - k + 1)$ 阶矩阵. 因此 $m = (s-1)d_1, n = d_1 - k + 1$, 令 $q = m - n + 1 = (s-2)d_1 + k$. 而参变量的个数 $p = \sum_{i=1}^{s}(d_i + 1)$. 则

$$\boldsymbol{f} : \mathbb{R}^p \longrightarrow \mathbb{R}^q$$

非线性函数组 $\boldsymbol{f}$ 是超定还是欠定取决于 $d_i, i = 1, ..., s$. 我们按 s 的值简单地讨论如下:

- $s = 2$ 时, $p = d_1 + d_2 + 2, q = k$, 此时 $p > q$ 恒成立, 非线性函数组 $\boldsymbol{f}$ 是欠定的.
- $s = 3$ 时, $p = d_1 + d_2 + d_3 + 3, q = d_1 + k$, 此时 $p > q$ 恒成立, 非线性函数组 $\boldsymbol{f}$ 是欠定的.

- $s>3$ 时, $p=\sum_{i=1}^{s}(d_i+1), q=(s-2)d_1+k,$, $q<p$ 和 $q\geq p$ 都有可能. 假设 $s=4$, 令 $d_1=20,d_2=4,d_3=5,d_4=6,k=3$, 进行简单的计算可得 $p=39,q=43$; 如果令 $d_1=10,d_2=4,d_3=5,d_4=6,k=3$，显然有 $p=29,q=23$.

非线性函数组 $\boldsymbol{f}$ 是超定的情况, 还需要做进一步的研究工作, 在此暂时不予考虑. 以下我们总假设非线性函数组 $\boldsymbol{f}$ 是欠定的. 设 $(\widetilde{\boldsymbol{\varepsilon}}_1,\ldots,\widetilde{\boldsymbol{\varepsilon}}_s)$ 是非线性欠定系统 $\boldsymbol{f}=\boldsymbol{0}$ 的一个近似解, 假设 $\boldsymbol{f}$ 在 $(\widetilde{\boldsymbol{\varepsilon}}_1,\ldots,\widetilde{\boldsymbol{\varepsilon}}_s)$ 处的 Jacobian 矩阵 $J_{\boldsymbol{f}}(\widetilde{\boldsymbol{\varepsilon}}_1,\ldots,\widetilde{\boldsymbol{\varepsilon}}_s)$ 是满秩的, 那么非线性方程组 $\boldsymbol{f}=\boldsymbol{0}$ 零点的可信验证就转化为计算区间向量

$$X_i\in\mathbb{IR}^{\dim\boldsymbol{\varepsilon}_i}\quad 且\ \boldsymbol{0}\in X_i,\ \text{ for }\ 1\leq i\leq s \tag{3.7}$$

使得 $(\widetilde{\boldsymbol{\varepsilon}}_1+X_1,\ldots,\widetilde{\boldsymbol{\varepsilon}}_s+X_s)$ 包含非线性方程组 $\boldsymbol{f}=\boldsymbol{0}$ 的零点.

首先, 我们将介绍计算 $J_{\boldsymbol{f}}(\boldsymbol{\varepsilon}_1,\ldots,\boldsymbol{\varepsilon}_s)$ 的“隐行列式方法”, Spence 和 Poulton [59] 在 Griewank 和 Reddien [25, 26] 早期的工作的基础上, 第一次提出了隐行列式方法. 该方法是将牛顿法应用到隐函数. 为了得到进一步的结果, 我们将系统 (3.2) 对每一个变量 $\varepsilon_{i,j}$ 进行微分

$$\begin{cases} A\frac{\partial\boldsymbol{\alpha}}{\partial\varepsilon_{i,j}}+\frac{\partial A}{\partial\varepsilon_{i,j}}\boldsymbol{\alpha}+\sum_{i=0}^{m-n}b_i\frac{\partial f_i}{\partial\varepsilon_{i,j}} &=\boldsymbol{0},\\ c^T\frac{\partial\boldsymbol{\alpha}}{\partial\varepsilon_{i,j}} &=0. \end{cases}$$

$\Longrightarrow$

$$G(\boldsymbol{\varepsilon}_1,\ldots,\boldsymbol{\varepsilon}_s)\begin{pmatrix}\frac{\partial\boldsymbol{\alpha}(\boldsymbol{\varepsilon}_1,\ldots,\boldsymbol{\varepsilon}_s)}{\partial\varepsilon_{i,j}}\\ \frac{\partial\boldsymbol{f}(\boldsymbol{\varepsilon}_1,\ldots,\boldsymbol{\varepsilon}_s)}{\partial\varepsilon_{i,j}}\end{pmatrix}=\begin{pmatrix}-\frac{\partial A(\boldsymbol{\varepsilon}_1,\ldots,\boldsymbol{\varepsilon}_s)}{\partial\varepsilon_{i,j}}\boldsymbol{\alpha}(\boldsymbol{\varepsilon}_1,\ldots,\boldsymbol{\varepsilon}_s)\\ 0\end{pmatrix}. \tag{3.8}$$

对于给定的近似解 $(\widetilde{\boldsymbol{\varepsilon}}_1,\ldots,\widetilde{\boldsymbol{\varepsilon}}_s)$, 线性系统 (3.8) 中的矩阵 G 是一个常数矩阵, 而对不同的变量 $\varepsilon_{i,j}$ 进行微分得到的右端向量一般来说是不同的. 我们将求解的 p 个线性系统的向量组合起来便得到 $(\boldsymbol{\alpha},\boldsymbol{f})^T$ 在 $(\widetilde{\boldsymbol{\varepsilon}}_1,\ldots,\widetilde{\boldsymbol{\varepsilon}}_s)$ 处的 Jacobian 矩阵 J, 那么 $J_{\boldsymbol{f}}(\widetilde{\boldsymbol{\varepsilon}}_1,\ldots,\widetilde{\boldsymbol{\varepsilon}}_s)=J_{n+1:m+1,:}$.

其次, 我们将对欠定方程组 (3.6) 零点的可信验证转化为 $\mathbb{R}^n\longrightarrow\mathbb{R}^n$ 的正规系统零点的可信验证. 我们所用到的方法源于 Chen和 Womersley [9]. 选取变量的一个指标子集 $\mathcal{I}\subset\{(i,j)|1\leq i\leq s,0\leq j\leq d_i\}$ 使得 $J_{\boldsymbol{f}}(\widetilde{\boldsymbol{\varepsilon}}_1,\ldots,\widetilde{\boldsymbol{\varepsilon}}_s)_{\mathcal{I}}$ 是满的方阵. 其中 $J_{\boldsymbol{f}}(\widetilde{\boldsymbol{\varepsilon}}_1,\ldots,\widetilde{\boldsymbol{\varepsilon}}_s)_{\mathcal{I}}$ 表示 Jacobian 矩阵 $J_{\boldsymbol{f}}(\widetilde{\boldsymbol{\varepsilon}}_1,\ldots,\widetilde{\boldsymbol{\varepsilon}}_s)$ 选取指标集 $\mathcal{I}$ 中元素对应变量所对的列组成的子矩阵. 方便起见, 我们设 $\boldsymbol{\varepsilon}_{\mathcal{I}}=(\varepsilon_{i,j}:(i,j)\in\mathcal{I})$, 那么

$J_{\boldsymbol{f}}(\widetilde{\varepsilon}_1,\ldots,\widetilde{\varepsilon}_s)_{\mathcal{I}}$ 可以表示为 $J_{\boldsymbol{f}}(\widetilde{\varepsilon}_{\mathcal{I}})$. 进而欠定函数组 (3.6) 成功地转化为我们想要的函数组.

最后, 我们将不在指标集中的元素对应的变量固定成初值, 即 $\varepsilon_{i,j}=\widetilde{\varepsilon}_{i,j}$, $(i,j)\notin\mathcal{I}$, 此时

$$\boldsymbol{f}(\boldsymbol{\varepsilon}_{\mathcal{I}}):\mathbb{R}^{m-n+1}\longrightarrow\mathbb{R}^{m-n+1}$$

如果给定 $X_{\mathcal{I}}=(X_{i,j}:(i,j)\in\mathcal{I})\in\mathbb{IR}^{m-n+1}$ 且 $\mathbf{0}\in X_{\mathcal{I}}$, $R\in\mathbb{R}^{(m-n+1)\times(m-n+1)}$; 利用定理 1.5 的算法, 成功算得

$$S(X_{\mathcal{I}},\boldsymbol{\varepsilon}_{\mathcal{I}}):=-Rf(\widetilde{\varepsilon}_1,\ldots,\widetilde{\varepsilon}_s)+\{I-RJ_{\boldsymbol{f}}(\widetilde{\varepsilon}_{\mathcal{I}}+X_{\mathcal{I}})_{\mathcal{I}}\}X_{\mathcal{I}}\subseteq\mathrm{int}(X_{\mathcal{I}}).$$

那么, 我们可以得出结论: 在区间向量 E 中一定存在一个点 $(\widehat{\varepsilon}_1,\ldots,\widehat{\varepsilon}_s)$ 是方程组 $\boldsymbol{f}(\boldsymbol{\varepsilon})=\mathbf{0}$ 的零点; 其中

$$E_{i,j}:=\begin{cases}\widetilde{\varepsilon}_{i,j}, & (i,j)\notin\mathcal{I},\\ \widetilde{\varepsilon}_{i,j}+X_{i,j}, & (i,j)\in\mathcal{I}.\end{cases}$$

根据引理 1.7, 如果矩阵 $G(\boldsymbol{\varepsilon}_1,\ldots,\boldsymbol{\varepsilon}_s),(\boldsymbol{\varepsilon}_1,\ldots,\boldsymbol{\varepsilon}_s)\in E$ 是非奇异矩阵, 那么一定存在点 $(\widehat{\varepsilon}_1,\ldots,\widehat{\varepsilon}_s)\in E$ 使得矩阵 $A(\widehat{\varepsilon}_1,\ldots,\widehat{\varepsilon}_s)$ 是秩亏为 1; 从而 $\deg(\mathrm{GCD}(g_1(\widehat{\varepsilon}_1),\ldots,g_s(\widehat{\varepsilon}_s)))=k$.

注 5. 求解问题 3.1 的过程中, 我们用到了以下两个假设:

1. 非线性函数组 (3.6) 是欠定的;
2. 给定的非线性方程组 $\boldsymbol{f}(\boldsymbol{\varepsilon})=\mathbf{0}$ 初始近似解 $(\widetilde{\varepsilon}_1,\ldots,\widetilde{\varepsilon}_s)$ 使得 Jacobian 矩阵 $J_{\boldsymbol{f}}(\widetilde{\varepsilon}_1,\ldots,\widetilde{\varepsilon}_s)$ 是满秩的.

前面我们已经得出结论当 $s=2,3$ 时, 非线性函数组 (3.6) 是欠定的. 特别地, 当 $s=2$ 时, 由推论 3.3 知矩阵 $A(\boldsymbol{\varepsilon}_1,\ldots,\boldsymbol{\varepsilon}_2)=B(g_1,\ldots,g_2)_{1:d_1-k+1:,1:d_1-k+1}$ 是方阵, 因此非线性函数组 (3.6) 的个数为 1. 在选取指标集 I 时, 我们只需选取一个变元即可.

第四章　算法与数值试验

4.1　算法

根据上一节的理论, 我们设计算法如下:

算法 4.1. *VUP 算法*

输入:

▶ 单变元多项式 $g_1,\dots,g_s \in \mathbb{R}[x]\setminus\{0\}$, 其中 $d_i = \deg(g_i)$, $1 \le i \le s$ 且 $d_1 = \max\{d_1,\dots,d_s\}$.

▶ $(\widetilde{\varepsilon}_1,\dots,\widetilde{\varepsilon}_s)$: 多项式 $g_1,\dots,g_s$ 系数向量的扰动初值.

▶ $(\widetilde{X}_1,\dots,\widetilde{X}_s)$: 多项式 $g_1,\dots,g_s$ 系数区间向量的扰动初值.

▶ tol: 初值优化的容差.

▶ k: 待验证多项式 $g_1,\dots,g_s$ 近似 GCD 的次数.

输出:

▶ $(X_1,\dots,X_s)$, 其中 $X_i \in \mathbb{IR}^{\dim \varepsilon_i}$, $1 \le i \le s$.

▶ $Failure$: 未成功运行.

步骤:

1. 数值初值优化

   a 选择合适的向量 $\boldsymbol{b}_0,\dots,\boldsymbol{b}_{m-n} \in \mathbb{R}^m$ 和 $\boldsymbol{c} \in \mathbb{R}^n$ 使得 (3.1) 中的矩阵 $G(\widetilde{\varepsilon}_1,\dots,\widetilde{\varepsilon}_s)$ 非奇异.

   b 令 (3.2) 中参变量向量 $(\varepsilon_1,\dots,\varepsilon_s) = (\widetilde{\varepsilon}_1,\dots,\widetilde{\varepsilon}_s)$, 求解该线性系统得到近似解 $(\boldsymbol{\alpha}(\widetilde{\varepsilon}_1,\dots,\widetilde{\varepsilon}_s), \boldsymbol{f}(\widetilde{\varepsilon}_1,\dots,\widetilde{\varepsilon}_s))$.

   c 对于每一个变量 $\varepsilon_{i,j}, 1 \le i \le s, 0 \le j \le d_i$, 通过解线性系统 (3.8) 得到 $\frac{\partial \boldsymbol{f}(\widetilde{\varepsilon}_1,\dots,\widetilde{\varepsilon}_s)}{\partial \varepsilon_{i,j}}$ 的值; 从而得到 $J_{\boldsymbol{f}}(\widetilde{\varepsilon}_1,\dots,\widetilde{\varepsilon}_s)$.

   d 检验 $J_{\boldsymbol{f}}(\widetilde{\varepsilon}_1,\dots,\widetilde{\varepsilon}_s)$ 是否是满秩的. 如果 $J_{\boldsymbol{f}}$ 不是满秩的, 回到第一步, 重新选择初值. 如果 $J_{\boldsymbol{f}}$ 是满秩的, 进入下一步.

   e 用广义逆方法对初值进行优化, 直到 $|f_i(\widetilde{\varepsilon}_1,\dots,\widetilde{\varepsilon}_s)| < tol, 0 \le i \le m-n$.

2. 选取指标集 $\mathcal{I}$ 使得 $J_{\boldsymbol{f}}(\widetilde{\boldsymbol{\varepsilon}}_{\mathcal{I}})$ 是非奇异的方阵. 并计算 $J_{\boldsymbol{f}}(\widetilde{\boldsymbol{\varepsilon}}_{\mathcal{I}})$ 的近似逆 R.

3. 区间迭代.

   a 区间算法的初始化.

$$Y_{i,j} = X_{i,j} := \begin{cases} 0, & (i,j) \notin \mathcal{I}, \\ \widetilde{X}_{i,j}, & (i,j) \in \mathcal{I}. \end{cases}$$

   b 用 INTLAB 包中 **verifylss** 函数计算区间向量 Z 使得

$$\sum \left(G(\widetilde{\boldsymbol{\varepsilon}}_1 + Y_1, \ldots, \widetilde{\boldsymbol{\varepsilon}}_s + Y_s), \begin{pmatrix} \mathbf{0} \\ 1 \end{pmatrix} \right) \subseteq Z$$

   c 用 **verifylss** 函数计算区间矩阵 M 使得

$$J_{\boldsymbol{f}}(\widetilde{\boldsymbol{\varepsilon}}_1 + Y_1, \ldots, \widetilde{\boldsymbol{\varepsilon}}_s + Y_s)_{\mathcal{I}} \subseteq M \tag{4.1}$$

   d 令

$$X_{\mathcal{I}} = -R\boldsymbol{f}(\widetilde{\boldsymbol{\varepsilon}}_1, \ldots, \widetilde{\boldsymbol{\varepsilon}}_s) + (I - RM)Y_{\mathcal{I}}.$$

   如果 $X_{\mathcal{I}} \subseteq \mathrm{int}(Y_{\mathcal{I}})$, 那么跳出循环, 进入下一步; 否则, 将计算所得的 $X_{\mathcal{I}}$ 赋值为初始迭代区间, 进入区间迭代第一步.

   e 验证区间矩阵 $G(\widetilde{\boldsymbol{\varepsilon}}_1+X_1, \ldots, \widetilde{\boldsymbol{\varepsilon}}_s+X_s)$ 的奇异性. 如果 $G(\widetilde{\boldsymbol{\varepsilon}}_1+X_1, \ldots, \widetilde{\boldsymbol{\varepsilon}}_s+X_s)$ 是非奇异的, 那么返回 $(X_1, \ldots, X_s)$; 否则, 返回失败.

注 6. 以下是对该算法的几点补充说明:

- 用广义逆方法对初值扰动的优化提高了对初值的依赖性.
- 该区间算法部分是以定理 1.5 为基础. 而定理 1.5 只给了函数组 $\boldsymbol{f}$ 零点可信验证的一个充分条件, 有可能计算出的区间向量 X 是可信区间, 但是不满足定理 1.5 的条件.
- 当 $s = 2$ 时, 由于 $A(\boldsymbol{\varepsilon}_1, \ldots, \boldsymbol{\varepsilon}_2)$ 是方阵, 指标集 $\mathcal{I}$ 只有一个元素, 算法得到进一步的简化.

命题 4.1. *如果上述算法成功返回区间向量 $(X_1, \ldots, X_s)$, 那么一定存在向量 $(\widehat{\boldsymbol{\varepsilon}}_1, \ldots, \widehat{\boldsymbol{\varepsilon}}_s) \in (\widetilde{\boldsymbol{\varepsilon}}_1 + X_1, \ldots, \widetilde{\boldsymbol{\varepsilon}}_s + X_s)$ 使得 $\deg(\mathrm{GCD}(g_1(\widehat{\boldsymbol{\varepsilon}}_1), \ldots, g_s(\widehat{\boldsymbol{\varepsilon}}_s))) = k$.*

证明. VUP 算法成功返回区间向量 $(X_1,\ldots,X_s)$, 根据区间迭代的 d 和定理 1.5 可知, 一定存在向量 $(\widehat{\varepsilon}_1,\ldots,\widehat{\varepsilon}_s)\in(\widetilde{\varepsilon}_1+X_1,\ldots,\widetilde{\varepsilon}_s+X_s)$ 使得 $\boldsymbol{f}(\widehat{\varepsilon}_1,\ldots,\widehat{\varepsilon}_s)=\mathbf{0}$. 引理 1.7 和算法区间迭代的 e 可知 $\operatorname{corank}(A(\widehat{\varepsilon}_1,\ldots,\widehat{\varepsilon}_s))=1$. 由定理 3.2 可知 $\operatorname{corank}(A(\widehat{\varepsilon}_1,\ldots,\widehat{\varepsilon}_s))=1$ 与 $\deg(\mathrm{GCD}(g_1(\widehat{\varepsilon}_1),\ldots,g_s(\widehat{\varepsilon}_s)))=k$ 等价. 因此, 一定存在向量 $(\widehat{\varepsilon}_1,\ldots,\widehat{\varepsilon}_s)\in(\widetilde{\varepsilon}_1+X_1,\ldots,\widetilde{\varepsilon}_s+X_s)$ 使得 $\deg(\mathrm{GCD}(g_1(\widehat{\varepsilon}_1),\ldots,g_s(\widehat{\varepsilon}_s)))=k$. □

4.2　数值试验

例 4.1. [31] 考虑两个单变元多项式

$$\begin{aligned} f &= 1000x^{10}+x^3-1,\\ g &= x^2-0.01, \end{aligned}$$

待验证的近似 GCD 的次数是 1. 令

$$\begin{aligned} f(\varepsilon_1) &= (1000+\varepsilon_{1,11})x^{10}+\varepsilon_{1,10}x^9+\varepsilon_{1,9}x^8+\varepsilon_{1,8}x^7+\varepsilon_{1,7}x^6+\varepsilon_{1,6}x^5\\ &\quad +\varepsilon_{1,5}x^4+(1+\varepsilon_{1,4})x^3+\varepsilon_{1,3}x^2+\varepsilon_{1,2}x+\varepsilon_{1,1}-1,\\ g(\varepsilon_2) &= (1+\varepsilon_{2,3})x^2+\varepsilon_{2,2}x+(-0.01+\varepsilon_{2,1}) \end{aligned}$$

为他们的含参变量扰动多项式, 其中 $\varepsilon_1,\varepsilon_2$ 为系数扰动向量. 算法输入如下

$$\begin{aligned} \widetilde{\varepsilon}_1 &= [0.8399\cdot10^{-2},0.415059\cdot10^{-2},0.205103\cdot10^{-2},0.101\cdot10^{-2},\\ &\quad 0.500837\cdot10^{-3},0.247491\cdot10^{-3},0.122287\cdot10^{-3},0.604355\cdot10^{-4},\\ &\quad 0.297998\cdot10^{-4},0.147908\cdot10^{-4},0],\\ \widetilde{\varepsilon}_2 &= [-0.179618,-0.88759\cdot10^{-1},-0.43861\cdot10^{-1}],\\ tol &= 10^{-10}, \end{aligned}$$

$$\widetilde{X}_{i,j}:=\begin{cases} 0, & (i,j)\neq(2,1),\\ 10^{-11}*[-1,1], & (i,j)=(2,1). \end{cases}$$

利用算法计算得到如下区间向量, 根据命题 4.1, 一定存在系数扰动向量 $\widehat{\varepsilon}_1$, $\widehat{\varepsilon}_2$ 使得 $f(\widehat{\varepsilon}_1),g(\widehat{\varepsilon}_2)$ 的 GCD 的次数为 1, 其中 $\widehat{\varepsilon}_1\in E_1$, $\widehat{\varepsilon}_2\in E_2$.

$$
\begin{aligned}
E_1 =&[0.00839899639100, 0.00839899639101]\\
&[0.00415058821698, 0.00415058821701]\\
&[0.00205102911900, 0.00205102911901]\\
&[0.00100999956500, 0.00100999956501]\\
&[0.00050083678479, 0.00050083678481]\\
&[0.00024749089370, 0.00024749089371]\\
&[0.00012228694749, 0.00012228694751]\\
&[0.00006043547404, 0.00006043547405]\\
&[0.00002979978716, 0.00002979978718]\\
&[0.00001479079365, 0.00001479079367],
\end{aligned}
$$

$$
\begin{aligned}
E_2 =&[-0.00000000000314, -0.00000000000313]\\
&[-0.17961792278821, -0.17961792278820]\\
&[-0.08875896187001, -0.08875896186998]\\
&[-0.04386098116001, -0.04386098115998].
\end{aligned}
$$

该例子展示待验证近似 GCD 次数为 1 的两个多项式的结果. 下面将给出待验证近似 GCD 次数更高的一些例子.

例 4.2. 考虑多项式

$$
\begin{aligned}
f &= x^9 - x^6 + x^5 - x^4 + x - 1,\\
g &= x^6 + 4.0001x^5 - 0.9999x - 3.99969999.
\end{aligned}
$$

待验证近似 GCD 的次数为 5. 类似例 4.1 的方法, 我们令

$$
\begin{aligned}
f(\varepsilon_1) &= (1+\varepsilon_{1,10})x^9 + \varepsilon_{1,9}x^8 + \varepsilon_{1,8}x^7 + (-1+\varepsilon_{1,7})x^6 + \varepsilon_{1,6}x^5 + (-1+\varepsilon_{1,5})x^4\\
&\quad +\varepsilon_{1,4}x^3 + \varepsilon_{1,3}x^2 + \varepsilon_{1,2}x + (-1+\varepsilon_{1,1}),\\
g(\varepsilon_2) &= (1+\varepsilon_{2,7})x^6 + (4.0001+\varepsilon_{2,6})x^5 + \varepsilon_{2,5}x^4 + \varepsilon_{2,4}x^3 + \varepsilon_{2,3}x^2\\
&\quad +(-0.9999+\varepsilon_{2,2})x + (-3.99969999+\varepsilon_{2,1}),
\end{aligned}
$$

为他们的含参变量扰动多项式, 其中 $\varepsilon_1, \varepsilon_2$ 为系数扰动向量. 算法输入如下

$$\begin{aligned}
\widetilde{\varepsilon}_1 &= [0.2\cdot 10^{-4}, -0.2\cdot 10^{-4}, 0.23249\cdot 10^{-5}, 0.1901\cdot 10^{-5},\\
&\quad 0.3\cdot 10^{-4}, 0, 0, 0.2675\cdot 10^{-5}, 0.16753\cdot 10^{-5}, 0],\\
\widetilde{\varepsilon}_2 &= [-0.10001\cdot 10^{-3}, -0.2\cdot 10^{-4}, 0.17999\cdot 10^{-4},\\
&\quad 0.2129\cdot 10^{-4}, 0.16014\cdot 10^{-4}, -0.1\cdot 10^{-3}, -0.2\cdot 10^{-4}],\\
tol &= 10^{-10}.
\end{aligned}$$

$$\widetilde{X}_{i,j} := \begin{cases} 0, & (i,j) \neq (1,10),\\ 10^{-10} * [-1,1], & (i,j) = (1,10). \end{cases}$$

利用算法计算得到如下区间向量, 则一定存在系数扰动向量 $\widehat{\varepsilon}_1$, $\widehat{\varepsilon}_2$ 使得 $f(\widehat{\varepsilon}_1), g(\widehat{\varepsilon}_2)$ 的 GCD 的次数为 5, 其中 $\widehat{\varepsilon}_1 \in E_1$, $\widehat{\varepsilon}_2 \in E_2$.

$$\begin{aligned}
E_1 =& 10^{-3} * [0.02000000000000, 0.02000000000001]\\
& 10^{-3} * [-0.02000000000001, -0.02000000000000]\\
& 10^{-3} * [0.00232489999999, 0.00232490000001]\\
& 10^{-3} * [0.00377335052599, 0.00377335052601]\\
& 10^{-3} * [0.03748960039999, 0.03748960040001]\\
& 10^{-3} * [-0.00000002998423, -0.00000002998422]\\
& 10^{-3} * [-0.00000003986506, -0.00000003986505]\\
& 10^{-3} * [0.00267496629699, 0.00267496629700]\\
& 10^{-3} * [0.00354753818199, 0.00354753818201]\\
& 10^{-3} * [0.00748922591531, 0.00748922591532],
\end{aligned}$$

$$
\begin{aligned}
E_2 =& 10^{-3} * [-0.10188238800001, -0.10188238800000] \\
& 10^{-3} * [-0.02000005165001, -0.02000005164999] \\
& 10^{-3} * [0.01799898254999, 0.01799898255001] \\
& 10^{-3} * [0.02316240421999, 0.02316240422001] \\
& 10^{-3} * [0.01414157635999, 0.01414157636001] \\
& 10^{-3} * [-0.10187233180001, -0.10187233179999] \\
& 10^{-3} * [-0.02000004495001, -0.02000004494999].
\end{aligned}
$$

例 4.2 是文献 [62] 中例子修改而来,下面将给出次数更高一些的多项式的例子.

例 4.3. 考虑多项式

$$
\begin{aligned}
f &= 48.0001 - 135.9999x + 172.0001x^2 - 97.9999x^3 + 42.0001x^4 - 46.9999x^5 \\
&\quad +118.0001x^6 - 139.9999x^7 + 65.0001x^8 + 68.0001x^9 - 16.9999x^{10} \\
&\quad +33.0001x^{11} - 5.9999x^{12} - 13.9999x^{13} + 1.0001x^{14} + 1.0001x^{15} \\
g &= -47.9999 - 79.9999x - 75.9999x^2 + 132.0001x^3 + 46.0001x^4 - 7.9999x^5 \\
&\quad +30.0001x^6 - 32.9999x^7 - 4.9999x^8 + 7.00001x^9 - 0.99998x^{10},
\end{aligned}
$$

他们待验证的近似 GCD 的次数为 5. 令

$$
\begin{aligned}
f(\varepsilon_1) &= (48.0001 + \varepsilon_{1,1}) + (-135.9999 + \varepsilon_{1,2})x + (172.0001 + \varepsilon_{1,3})x^2 \\
&\quad +(-97.9999 + \varepsilon_{1,4})x^3 + (42.0001 + \varepsilon_{1,5})x^4 + (-46.9999 + \varepsilon_{1,6})x^5 \\
&\quad +(118.0001 + \varepsilon_{1,7})x^6 + (-139.9999 + \varepsilon_{1,8})x^7 + (65.0001 + \varepsilon_{1,9})x^8 \\
&\quad +(68.0001 + \varepsilon_{1,10})x^9 + (-16.9999\varepsilon_{1,11})x^{10} + (33.0001\varepsilon_{1,12})x^{11} \\
&\quad +(-5.9999 + \varepsilon_{1,13})x^{12} + (-13.9999 + \varepsilon_{1,14})x^{13} + (1.0001 + \varepsilon_{1,15})x^{14} \\
&\quad +(1.0001 + \varepsilon_{1,16})x^{15}, \\
g(\varepsilon_2) &= (-47.9999 + \varepsilon_{2,1}) + (-79.9999 + \varepsilon_{2,2})x + (-75.9999 + \varepsilon_{2,3})x^2 \\
&\quad +(132.0001 + \varepsilon_{2,4})x^3 + (46.0001 + \varepsilon_{2,5})x^4 + (-7.9999 + \varepsilon_{2,6})x^5 \\
&\quad +(30.0001 + \varepsilon_{2,7})x^6 + (-32.9999 + \varepsilon_{2,8})x^7 + (-4.9999 + \varepsilon_{2,9})x^8 \\
&\quad +(7.00001 + \varepsilon_{2,10})x^9 + (-0.99998 + \varepsilon_{2,11})x^{10}
\end{aligned}
$$

为他们的含参变量扰动多项式, 其中 $\varepsilon_1, \varepsilon_2$ 为系数扰动向量. 算法输入如下

$$\begin{aligned}\widetilde{\varepsilon_1} &= [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],\\ \widetilde{\varepsilon_2} &= [0,0,0,0,0,0,0,0,0,0,0],\\ tol &= 10^{-15},\end{aligned}$$

$$\widetilde{X}_{i,j} := \begin{cases} 0, & (i,j) \neq (2,11),\\ 10^{-13} * [-1,1], & (i,j) = (2,11).\end{cases}$$

利用算法计算得到如下区间向量, 则一定存在系数扰动向量 $\widehat{\varepsilon}_1$, $\widehat{\varepsilon}_2$ 使得 $f(\widehat{\varepsilon}_1), g(\widehat{\varepsilon}_2)$ 的 GCD 的次数为 5, 其中 $\widehat{\varepsilon}_1 \in E_1$, $\widehat{\varepsilon}_2 \in E_2$.

$$\begin{aligned}E_1 =& 10^{-5} * [-0.00000000276405, -0.00000000276404]\\ & 10^{-5} * [-0.00000001959114, -0.00000001959113]\\ & 10^{-5} * [-0.00000007276789, -0.00000007276788]\\ & 10^{-5} * [-0.00000019967659, -0.00000019967658]\\ & 10^{-5} * [-0.00000071602336, -0.00000071602335]\\ & 10^{-5} * [-0.00000220094790, -0.00000220094789]\\ & 10^{-5} * [-0.00000694844899, -0.00000694844898]\\ & 10^{-5} * [-0.00002080087782, -0.00002080087780]\\ & 10^{-5} * [-0.00006402605894, -0.00006402605892]\\ & 10^{-5} * [-0.00019240096661, -0.00019240096659]\\ & 10^{-5} * [-0.00058318053461, -0.00058318053459]\\ & 10^{-5} * [-0.00174972873301, -0.00174972873299]\\ & 10^{-5} * [-0.00527382035501, -0.00527382035499]\\ & 10^{-5} * [-0.01582349019001, -0.01582349018999]\\ & 10^{-5} * [-0.04756477612001, -0.04756477611999]\\ & 10^{-5} * [-0.14269152520000, -0.14269152519999],\end{aligned}$$

$$
\begin{aligned}
E_2 =& 10^{-5} * [0.00000755465420, 0.00000755465421] \\
& 10^{-5} * [0.00002301448476, 0.00002301448478] \\
& 10^{-5} * [0.00006983210637, 0.00006983210640] \\
& 10^{-5} * [0.00021118148178, 0.00021118148181] \\
& 10^{-5} * [0.00063645284219, 0.00063645284220] \\
& 10^{-5} * [0.00191540469500, 0.00191540469501] \\
& 10^{-5} * [0.00575795436799, 0.00575795436801] \\
& 10^{-5} * [0.01729827836999, 0.01729827837001] \\
& 10^{-5} * [0.05193810309999, 0.05193810310001] \\
& 10^{-5} * [0.15590106569999, 0.15590106570001] \\
& 10^{-5} * [0.46785230908456, 0.46785230908457].
\end{aligned}
$$

例 4.4. 考虑多项式

$$
\begin{aligned}
f &= x^{101} + x^{100} - x - 1 \\
g &= x^{101} - x^{100} - x + 1,
\end{aligned}
$$

其待验证近似 GCD 为 100. 令

$$
\begin{aligned}
f(\varepsilon_1) &= (-1 + \varepsilon_{1,1}) + (-1 + \varepsilon_{1,2}) + \varepsilon_{1,3}x^2 + \varepsilon_{1,4}x^3 + \varepsilon_{1,5}x^4 + \varepsilon_{1,6}x^5 + \cdots, \\
g(\varepsilon_2) &= (1 + \varepsilon_{2,1}) + (-1 + \varepsilon_{2,2}) + \varepsilon_{2,3}x^2 + \varepsilon_{2,4}x^3 + \varepsilon_{2,5}x^4 + \varepsilon_{2,6}x^5 + \cdots.
\end{aligned}
$$

为他们的含参变量扰动多项式, 其中 $\varepsilon_1, \varepsilon_2$ 为系数扰动向量. 算法输入如下:

$$
\begin{aligned}
\widetilde{\varepsilon_1} = \; & 10^{-4}[1,1,1,1,-1,1,1,1,1,-1,1,1,1,1,-1,1,1,1,1,-1,1,1,1,1, \\
& -1,1,1,1,1,-1,1,1,1,1,-1,1,1,1,1,-1,1,1,1,1,-1,1,1,1,1,-1, \\
& 1,1,1,1,-1,1,1,1,1,-1,1,1,1,1,-1,1,1,1,1,-1,1,1,1,1,-1,1, \\
& 1,1,1,-1,1,1,1,1,-1,1,1,1,1,-1,1,1,1,1,-1,1,1,1,1,-1,1,1]
\end{aligned}
$$

$$
\begin{aligned}
\widetilde{\varepsilon_2} &= 10^{-4}[1,1,-1,1,1,1,1,-1,1,1,1,1,-1,1,1,1,1,-1,1,1,1,1,-1,1,\\
&\quad 1,1,1,-1,1,1,1,1,-1,1,1,1,1,-1,1,1,1,1,-1,1,1,1,1,-1,1,1,\\
&\quad 1,1,-1,1,1,1,1,1,-1,1,1,1,1,-1,1,1,1,1,-1,1,1,1,1,-1,1,1,\\
&\quad 1,-1,1,1,1,1,-1,1,1,1,1,-1,1,1,1,1,-1,1,1,1,1,-1,1,1,1,-1],\\
tol &= 10^{-2},
\end{aligned}
$$

$$
\widetilde{X}_{i,j} := \begin{cases} 0, & (i,j) \neq (2,100), \\ 10^{-4} * [-1,1], & (i,j) = (2,100). \end{cases}
$$

利用算法计算得到一个 204 维的区间向量, 根据命题 4.1,则一定存在系数扰动向量 $\widehat{\varepsilon}_1, \widehat{\varepsilon}_2$ 使得 $f(\widehat{\varepsilon}_1), g(\widehat{\varepsilon}_2)$ 的 GCD 的次数为 100, 其中 $\widehat{\varepsilon}_1 \in E_1$, $\widehat{\varepsilon}_2 \in E_2$.

$$
\begin{aligned}
E_1 = & 10^{-3} * [0.10000000000000, 0.10000000000001] \\
& 10^{-3} * [0.10000000000000, 0.10000000000001] \\
& 10^{-3} * [0.10000000000000, 0.10000000000001] \\
& 10^{-3} * [0.10000000000000, 0.10000000000001] \\
& 10^{-3} * [-0.10000000000001, -0.10000000000000] \\
& \vdots
\end{aligned}
$$

$$
\begin{aligned}
E_2 = & 10^{-3} * [0.10000000000000, 0.10000000000001] \\
& 10^{-3} * [0.10000000000000, 0.10000000000001] \\
& 10^{-3} * [-0.10000000000001, -0.10000000000000] \\
& 10^{-3} * [0.10000000000000, 0.10000000000001] \\
& 10^{-3} * [0.10000000000000, 0.10000000000001] \\
& \vdots
\end{aligned}
$$

第五章　结论与展望

前面我们主要讨论了单变元多项式近似 GCD 次数的可信验证问题.

首先定理 3.2 结果表明 $\deg(\mathrm{GCD}(g_1,\ldots,g_s))=k$ 与 Bezout 矩阵的前 d_1-k+1 列 $B(g_1,\ldots,g_s)_{:,1:d_1-k+1}$ 是秩亏为 1 等价. 因此我们将单变元多项式近似 GCD 次数的可信验证问题转化为: 寻找多项式系数的一个扰动, 使得扰动多项式 Bezout 矩阵的前 d_1-k+1 列是秩亏为 1. 其次, 从引理 1.7 知, 如果边界矩阵 (1.7) 是非奇异的, 则 $\mathrm{rank}(A)=n-1$ 与线性系统 (1.8) 的解满足条件 $f_0=0,\ldots,f_{m-n}=0$. 因此将寻找多项式系数的一个扰动使得扰动多项式 Bezout 矩阵的前 d_1-k+1 列是秩亏 1 转化为: 求解隐函数方程组 $f_0(\boldsymbol{\varepsilon})=0,\ldots,f_{m-n}(\boldsymbol{\varepsilon})=0$ 的零点. 最后, 对于由系统 (3.2) 定义的隐函数组 $(f_0,\ldots,f_{m-n})$ 零点的可信验证问题, 我们提出用隐行列式方法求解.

可信验证方法的核心定理 1.5 的条件是 $\boldsymbol{f}:\mathbb{R}^n\to\mathbb{R}^n$, 而由系统 (3.2) 定义的隐函数组是 $\boldsymbol{f}:\mathbb{R}^p\longrightarrow\mathbb{R}^q$, 其中 p 和 q 由多项式的个数和次数决定. 分析可知隐函数组 $\boldsymbol{f}$ 可能是欠定, 超定或者正规. 在第三章中我们分析了当 $s=2,3$ 时, 隐函数组 $\boldsymbol{f}$ 是欠定的. 为此我们先考虑隐函数组 $\boldsymbol{f}$ 是欠定的情况. 此时我们固定某些变量使得 $\boldsymbol{f}:\mathbb{R}^n\to\mathbb{R}^n$; 再利用定理 1.5, 如果计算出来的区间满足条件 (1.1) 并且 (3.1) 式在计算出来的区间内是非奇异的, 那么所得区间是单变元多项式近似 GCD 次数的可信区间.

当 $s=2$ 时, 由推理 3.3 知矩阵 $A(\boldsymbol{\varepsilon}_1,\ldots,\boldsymbol{\varepsilon}_2)=B(g_1,\ldots,g_2)_{1:d_1-k+1:,1:d_1-k+1}$ 是方阵, 因此非线性方程组 (3.6) 的个数是 1, 在选取指标集 I 时, 我们只需选取一个变元即可. 我们已经完成计算两个单变元多项式近似 GCD 次数的可信验证算法, 而且对所给的例子都能在合适的初值和初值区间下得到可信区间.

多项式近似 GCD 次数的可信验证问题, 我们解决了两个单变元多项式的情况. 今后的工作可以从以下几个方面研究:

1. 我们对于隐函数组 $\boldsymbol{f}$ 是欠定的情况进行了深入研究. 但是当 $p-q>1$ 时, 在固定变量的选取方法上还有待提高. 经过多次数值试验, 我们的算法可以计算出某些例子的可信区间, 而有些例子并没有成功. 总之, 算法优化方面可以做进一步的研究.

2. 我们可以考虑隐函数组 $\boldsymbol{f}$ 是超定的情况, 此时 $p < q$, 如何引入变量将隐函数组转化为正规函数组 $\boldsymbol{f}: \mathbb{R}^n \longrightarrow \mathbb{R}^n$, 并设计算法计算可信区间.

3. 我们还可以做多变元多项式近似 GCD 次数的可信验证问题. 众所周知, 多变元多项式的 Slyvester 矩阵的亏秩与 GCD 的全次数有关. 由于多变元多项式变元较多, 研究工作将更具挑战性.

文章 [31, 33, 37] 用 Slyvester 矩阵计算多变元多项式的近似 GCD. 为了方便计算两个多变元多项式乘积多项式的系数, [32, 39] 引入扰动矩阵 $C^{[m]}(g)$. 对于给定的多变元多项式 g, 对任意全次数为 m 的多项式 u, 多项式 $u \cdot g$ 的系数向量可以用扰动矩阵 $C^{[m]}(g)$ 与多项式 u 的系数向量的乘积表示. 例如

$$\begin{aligned}\overrightarrow{(a_2x + a_1y + a_0) \cdot (b_2x + b_1y + b_0)} = & \quad C^{[1]}(a_2x + a_1y + a_0) \cdot \begin{pmatrix} b_2 \\ b_1 \\ b_0 \end{pmatrix} \\ = & \quad \begin{pmatrix} a_2 & 0 & 0 \\ a_1 & a_2 & 0 \\ 0 & a_1 & 0 \\ a_0 & 0 & a_2 \\ 0 & a_0 & a_1 \\ 0 & 0 & a_0 \end{pmatrix} \cdot \begin{pmatrix} b_2 \\ b_1 \\ b_0 \end{pmatrix}.\end{aligned}$$

定理 5.1. [31] *设 $g_1, \ldots, g_s \in \mathbb{R}[x_1, \ldots, x_r] \setminus \{0\}$, 并且 $d_i = \mathrm{tdeg}(f_i)$, 对所有的 $1 \le i \le s$ 都有 $k \le d_i$, 那么 $\mathrm{tdeg}(\mathrm{GCD}(g_1, \ldots, g_s)) \ge k$ 当且仅当 Sylvester 矩阵*

$$S_k(g_1, \ldots, g_s) = \begin{pmatrix} C^{[d_2-k]}(g_1) & 0 & \ldots & 0 & C^{[d_1-k]}(g_2) \\ 0 & C^{[d_3-k]}(g_1) & & 0 & C^{[d_1-k]}(g_3) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & C^{[d_s-k]}(g_1) & C^{[d_1-k]}(g_s) \end{pmatrix}$$

至少是秩亏 1 的.

根据上述定理的结论, 多变元多项式近似 GCD 的次数的可信验证问题可以转化为 Sylvester 矩阵的亏秩的可信验证问题. 我们只需证明下面两个方面

$$\begin{aligned} S_k\text{至少亏 } 1 &\Longrightarrow \mathrm{tdeg}(\mathrm{GCD}(g_1, \ldots, g_s)) \ge k \\ S_{k+1}\text{满秩} &\Longrightarrow \mathrm{tdeg}(\mathrm{GCD}(g_1, \ldots, g_s)) < k + 1. \end{aligned}$$

就可以证明多变元多项式 GCD 的次数为 k.

参考文献

[1] G. Alefeld and J. Herzberger. Einfuhrung in die intervallrechnung, 1974.

[2] S. Barnett. Greatest common divisor of two polynomials. *Linear Algebra and its Applications*, 3(1):7 – 9, 1970.

[3] S. Barnett. Greatest common divisor of several polynomials. 70:263–268, 1971.

[4] S. Barnett. A note on the bezoutian matrix. *SIAM Journal on Applied Mathematics*, 22(1):84–86, 1972.

[5] D. Bini and L. Gemignani. Fast parallel computation of the polynomial remainder sequence via bézout and hankel matrices. *SIAM Journal on Computing*, 24(1):63–77, 1995.

[6] Dario Bini and Victor Y. Pan. *Polynomial and matrix computations (vol. 1): fundamental algorithms*. Birkhauser Verlag, Basel, Switzerland, Switzerland, 1994.

[7] William S. Brown and J. F. Traub. On Euclid's Algorithm and the Theory of Subresultants. *Journal of The ACM*, 18:505–514, 1971.

[8] F. Chatelin. Analyse statistique de la qualite numericque et arithmetique de la resolution approchee dequations par calcul sur ordinateur. Technical Report 133, Centre Scientifique IBM-France, 1988.

[9] Xiaojun Chen and Robert S. Womersley. Existence of solutions to systems of underdetermined equations and spherical designs. *SIAM J. Numerical Analysis*, 44(6):2326–2341, 2006.

[10] Xiaoguang Yang Chenyi Hu, Shanying xu. A review on interval computation Software and Applications, url = http://europepmc.org/abstract/CIT/478160,.

[11] Guillaume Chèze, André Galligo, Bernard Mourrain, and Jean-Claude Yakoubsohn. A subdivision method for computing nearest gcd with certification. *Theor. Comput. Sci.*, 412(35):4493–4503, August 2011.

[12] George E. Collins. Subresultants and Reduced Polynomial Remainder Sequences. *Journal of The ACM*, 14:128–142, 1967.

[13] Robert M. Corless, Patrizia M. Gianni, Barry M. Trager, and Stephen M. Watt. The singular value decomposition for polynomial systems. In *International Symposium on Symbolic and Algebraic Computation*, pages 195–207, 1995.

[14] Annie A. M. Cuyt, Brigitte Verdonk, Stefan Becuwe, and Peter Kuterna. A Remarkable Example of Catastrophic Cancellation Unraveled. *Computing*, 66:309–320, 2001.

[15] Marc Daumas, Guillaume Melquiond, and César Mu?oz. Guaranteed proofs using interval arithmetic. In *Proceedings of the 17th Symposium on Computer Arithmetic, Cape Cod*, 2005.

[16] James W. Demmel, Yozo Hida, William Kahan, Xiaoye S. Li, Soni Mukherjee, and E. Jason Riedy. Error bounds from extra precise iterative refinement. Technical Report UCB/CSD-04-1344, EECS Department, University of California, Berkeley, Mar 2005.

[17] Gema M. Diaz-Toca and Laureano Gonzalez-Vega. Barnett's theorems about the greatest common divisor of several univariate polynomials through bezout-like matrices. *J. Symb. Comput.*, 34(1):59–81, July 2002.

[18] Gema M. Diaz-Toca and Laureano Gonzalez-Vega. Computing greatest common divisors and squarefree decompositions through matrix methods: The parametric and approximate cases. *Linear Algebra and its Applications*, 412:222 – 246, 2006.

[19] Paul S. Dwyer. Linear Computations. *American Journal of Physics*, 20, 1952.

[20] Ioannis Z. Emiris, AndréGalligo, and Henri Lombardi. Certified approximate univariate GCDs. *Journal of Pure and Applied Algebra*, 117:229–251, 1997.

[21] Ioannis Z. Emiris, Andre Galligo, and Henri Lombardi. Numerical Univariate Polynomial GCD. 1996.

[22] Andreas Frommer. Proving Conjectures by Use of Interval Arithmetic. 2001.

[23] Shuhong Gao, Erich Kaltofen, John May, Zhengfeng Yang, and Lihong Zhi. Approximate factorization of multivariate polynomials via differential equations. In *Proceedings of the 2004 international symposium on Symbolic and algebraic computation*, ISSAC '04, pages 167–174, New York, NY, USA, 2004. ACM.

[24] Luca Gemignani. Gcd of polynomials and bezout matrices. In *Proceedings of the 1997 international symposium on Symbolic and algebraic computation*, ISSAC '97, pages 271–277, New York, NY, USA, 1997. ACM.

[25] A. Griewank and G. Reddien. The approximate solution of defining equations for generalized turning points. *SIAM Journal on Numerical Analysis*, 33(5):1912–1920, 1996.

[26] A. Griewank and G.W. Reddien. The approximation of generalized turning points by projection methods with superconvergence to the critical parameter. *Numerische Mathematik*, 48:591–606, 1986.

[27] Eldon Hansen and Roberta Smith. Interval Arithmetic in Matrix Computations, Part II. *Siam Journal on Numerical Analysis*, 4:1–9, 1967.

[28] U. Helmke and PA Fuhrmann. Bezoutians. *Linear Algebra and its Applications*, 122:1039–1097, 1989.

[29] Johannes Holzl. Proving real-valued inequalities by computation in isabelle/hol.

[30] V. Hribernig and H. J. Stetter. Detection and validation of clusters of polynomial zeros. *Journal of Symbolic Computation*, 1995.

[31] Erich Kaltofen. Approximate greatest common divisors of several polynomials with linearly constrained coefficients and singular polynomials. *Manuscript*, 2006.

[32] Erich Kaltofen, John P. May, Zhengfeng Yang, and Lihong Zhi. Approximate factorization of multivariate polynomials using singular value decomposition. *Journal of Symbolic Computation*, 43(5):359 – 376, 2008.

[33] Erich Kaltofen, Zhengfeng Yang, and Lihong Zhi. Structured low rank approximation of a sylvester matrix. In Dongming Wang and Lihong Zhi, editors, *Symbolic-Numeric Computation*, Trends in Mathematics, pages 69–83. Birkhauser Basel, 2007.

[34] N.K. Karmarkar and Y.N. Lakshman. On approximate gcds of univariate polynomials. *Journal of Symbolic Computation*, 26(6):653 – 666, 1998.

[35] R. Krawczyk. Newton-algorithmen zur bestimmung von nullstellen mit fehlerschranken. *Computing*, 4:187–201, 1969. 10.1007/BF02234767.

[36] Bin Li, Jiawang Nie, and Lihong Zhi. Approximate gcds of polynomials and sparse sos relaxations. *Theor. Comput. Sci.*, 409(2):200–210, December 2008.

[37] Yang-Z. Li, B. and L. Zhi. Fast low rank approximation of a sylvester matrix by structured total least norm. *J. JSSAC(Japan Society for Symbolic and Algebraic Computation)*, pages 165–174, 2005.

[38] Eugene Loh and G.William Walster. Rump's example revisited. *Reliable Computing*, 8:245–248, 2002.

[39] J. P. May. *Approximate factorization of polynomials in many variables and other problems in approximate algebra via singular value decomposition methods*. North Carolina State Univ., Raleigh, North Carolina, Aug.2005.

[40] M.J.C.Gordon. *From LCF to HOL: A short history. in proof, Language, and Interaction: Essays in Honor of Robin Milner*. MIT Press, 2000.

[41] Neumaier. Formal mathematical language.

[42] Jiawang Nie, James Demmel, and Ming Gu. Global minimization of rational functions and the nearest gcds. *J. of Global Optimization*, 40(4):697–718, April 2008.

[43] M T Noda and T. Sasaki. Approximate gcd and its application to ill-conditioned algebraic equations. 1991.

[44] Victor Y. Pan. Numerical Computation Of A Polynomial GCD And Extensions. *Informs Journal on Computing*, 1996.

[45] M. Porte and J. Vignes. Etude statistique des erreurs dans l'arithmetique des ordinateurs; application au controle des resultats d'algorithmes numeriques. *Numerische Mathematik*, 23:63–72, 1974.

[46] P. Rabier and G. Reddien. Characterization and computation of singular points with maximum rank deficiency. *SIAM Journal on Numerical Analysis*, 23(5):1040–1051, 1986.

[47] R.E.Moore. a test for existence of solutions for non-linear systems. *SIAM J.Numer.Anal*, 4:611–615, 1962.

[48] R.E.Moore. *Interval arithmetic and automatic error analysis in digital computing*. Dissertation, Stanford University, 1962.

[49] R.E.Moore and C.Yang. Interval analysis i. Lockheed Missiles and Space Division, 1959.

[50] Ramon E. R.E.Moore and Fritz Bierbaum. *Methods and Applications of Interval Analysis (SIAM Studies in Applied and Numerical Mathematics) (Siam Studies in Applied Mathematics, 2.)*. Soc for Industrial & Applied Math, 1979.

[51] Robert H. Risch. The problem of integration in finite terms. *Transactions of the American Mathematical Society*, 139:pp. 167–189, 1969.

[52] S. M. Rump. *Kleine Fehlerschranken Bei Matrixproblem*. Phd thesis, Universitat Karlsruhe, 1980.

[53] Siegfried M. Rump. Verification methods: rigorous results using floating-point arithmetic. In *Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation*, ISSAC '10, pages 3–4, New York, NY, USA, 2010. ACM.

[54] Siegfried M. Rump. Verified bounds for singular values, in particular for the spectral norm of a matrix and its inverse. 51:367–384, 2011.

[55] Siegfried M. Rump. Verified bounds for least squares problems and underdetermined linear systems. *SIAM J. Matrix Analysis Applications*, pages 130–148, 2012.

[56] S.M. Rump. *Solving algebraic problems with high accuracy*. 1983.

[57] David Rupprecht. An algorithm for computing certified approximate GCD of n univariate polynomials. *Journal of Pure and Applied Algebra*, 139:255–284, 1999.

[58] Arnold Sch?nhage. Quasi-GCD computations. *Journal of Complexity*, 1:118–137, 1985.

[59] A Spence and C Poulton. Photonic band structure calculations using nonlinear eigenvalue techniques. *Journal of Computational Physics*, 204(1):65–81, March 2005. The original publication is available at www.sciencedirect.com.

[60] G. W. Stewart. Stochastic perturbation theory. *SIAM Review*, 32(4):pp. 579–610, 1990.

[61] Dongxia Sun and Lihong Zhi. Structured low rank approximation of a bezout matrix. *MM Research Preprints 25 (December 2006)*, pages 207–218, 2006.

[62] Dongxia Sun and Lihong Zhi. Structured low rank approximation of a bezout matrix. *Mathematics in Computer Science*, pages 427–437, 2007.

[63] Sunaga. Geometry of numerals. Master's thesis, University of Tokyo, 1956.

[64] J. Vignes. New methods for evaluating the validity of the results of mathematical computaions. pages 227–249, 1978.

[65] J. Vignes. Algorithmes numeriques: Analyse el mise en oeuvre 2: Equations et systemes non lineaires. In *Collection Langages el Algorithmes del'Informatique*. Editions Technip, 1980.

[66] M. Warmus. Calculus of approximations. In *Bulletin de l'Academie Polonaise des Sciences*, volume 4, pages 253–259. 1956.

[67] P.Casteran Y.Bertot. *interactive theorem proving and program development.* Texts in Theoretical Computer Scinece. Springer, 2004.

[68] RosalindCecily Young. The algebra of many-valued quantities. *Mathematische Annalen*, 104:260–290, 1931.

[69] Zhonggang Zeng and Barry H. Dayton. The approximate gcd of inexact polynomials. In *Proceedings of the 2004 international symposium on Symbolic and algebraic computation*, ISSAC '04, pages 320–327, New York, NY, USA, 2004. ACM.

发表文章目录

[1] Zhe Li and Qi Liu. The verification of the degree of approximate GCD of two univariate polynomials. Submitted

简　　历

刘琦, 女, 四川省, 1986 年出生.　E-mail: sara1008@sina.com

教育状况

2010.09–2013.07　中国科学院数学与系统科学研究院, 应用数学, 理学硕士
方向：符号与数值混合计算, 导师：支丽红研究员.

2006.09–2010.07　吉林大学, 数学学院, 数学与应用数学, 理学学士.

会议活动

2012.04 可信计算研讨会, 北京.

2012.10 第十届亚洲计算机数学会议, 北京.

2012.07 基于符号与数值混合的可信计算研讨会, 北京.

获奖经历

2012.04　　中国科学院“三好学生”

2009.12　　吉林大学二等奖学金

2009.12　　吉林大学院优秀学生

2008.12　　吉林大学国家励志奖学金

2007.12　　吉林大学一等奖学金

2007.12　　吉林大学优秀学生

致　　谢

三年的硕士生生活一晃而过, 回首这三年的岁月, 收获良多. 论文即将完成之际, 谨在此感谢多年来在学习和生活中给予我教导和关怀的各位老师, 在生活中给予我支持和鼓励的同学, 朋友以及家人表示诚挚的感谢!

首先感谢我的恩师支丽红研究员, 这篇论文的内容从选题到研究再到写作都是在支老师的悉心指导下完成的, 恩师对我的指导和影响之大, 无以言表. 支老师严谨地学术态度, 对科学高峰地执着追求, 以及兢兢业业地敬业精神深深地感染着我. 老师的严格要求和谆谆教诲时刻萦绕在我的耳边, 必将对我以后学习生活和工作生活影响良多. 学生不才, 未能在老师您身边多待几年, 多聆听您的教诲, 对此我深表遗憾!

特别感谢李喆博士后, 在写论文的过程中悉心帮我解答疑惑, 在我为课题焦头烂额时关心我, 安慰我. 感谢梁野师兄, 李楠师兄, 郭庆东师兄以及王础师弟, 在论文研究讨论中的贡献和帮助! 在同梁野师兄和李楠师兄讨论问题的过程中受到了很多启发, 非常感谢您们的热情帮助! 郭庆东师兄和王础师弟也给予了我很大帮助!

衷心感谢数学机械化中心的各位老师! 特别感谢吴文俊院士、高小山研究员、李子明研究员、李洪波研究员、王定康研究员、刘卓军研究员. 从他们那里我学习到了很多的知识. 同时感谢周代珍老师和丁健敏老师以及李佳老师的热心帮助.

衷心感谢现在或曾经在数学机械化中心学习的杨争峰师兄、李冰玉师姐、吴晓丽师姐、李斌师兄、梁野师兄、郭峰、马玥、李楠、李子佳、郭庆东、李喆以及实验室其他同学. 也感谢一起上讨论班的老师和同学. 通过讨论班上的讨论交流让我学习到了很多知识. 在此, 我还要感谢在我身边为我加油打气的好友们, 因为有了你们, 我的科研生活丰富了许多. 当我迷茫失落时, 你们总能用你们的正能量感染我, 用你们积极乐观的心态开导我. 我庆幸是与你们度过了人生中重要的三年岁月, 也感激有你们的陪伴!

最后, 要特别感谢数学与系统科学研究院以及中科院大学的各位老师, 你们辛勤地劳动为我们创造了良好的学习和生活环境.在此祝愿你们身体健康, 工作

顺利, 心情愉快!