

分类号 _____

密级 _____

UDC _____

编号 _____

中国科学院研究生院 硕士学位论文

近似多项式问题全局最优解的半定规划求解和平方和有理化验证

李斌

指导教师 _____ 支丽红 副研究员

中国科学院数学与系统科学研究院

申请学位级别 _____ 硕士 _____ 学科专业名称 _____ 基础数学 _____

论文提交日期 _____ 2008年5月 _____ 论文答辩日期 _____ 2008年6月 _____

培养单位 _____ 中国科学院数学与系统科学研究院

学位授予单位 _____ 中国科学院研究生院

答辩委员会主席 _____

Exact Certification of Global Optimality of
Approximate Polynomial Problems via
Semidefinite Programming and
Rationalizing Sums-Of-Squares

Bin Li

Supervisor:

Asso. Prof. Lihong Zhi

Key Laboratory of Mathematics Mechanization
Institute of Systems Science
Academy of Mathematics and Systems Science
Chinese Academy of Sciences

June, 2008

*Submitted in total fulfillment of the requirements for the degree of M.S.
in pure mathematics*

摘 要

在本文中, 我们主要讨论了怎样使用由平方和 (SOS) 松弛方法生成的半定规划 (SDP) 求得符号数值混合计算中的几个基本问题的全局最优解, 以及怎样通过有理化投影数值平方和来精确验证接近全局最小值的有理下界。

计算多个实或者复系数多项式的近似最大公因式 (GCD) 问题、近似因式分解问题以及 Siegfried Rump 的一个公开模型问题都可以表示成多项式或有理函数最优化问题。我们使用基于稠密或稀疏平方和松弛方法的半定规划求解这几个问题表示成的带或不带限制条件的多项式或有理函数最优化问题并且实现了相应的算法。

然后我们将 Peyrl 和 Parillo [SNC 2007 会议] 的有理化半正定 (PSD) 多项式数值平方和等式的方法推广到精确验证问题下界上。对于多项式近似最大公因式问题、多元多项式的不可约半径问题和 Rump 的模型问题在 $n \leq 14$ 时的情形, 我们的算法成功的验证了接近全局最小值的精确有理下界。

由目前的固定精度半定规划软件包 (如 SOSTOOLS、YALMIP、SeDuMi 等) 计算得到的最优值和数值平方和一般误差较大, 因此我们使用 Newton-Lagrange 方法对全局最优解进行精化并且在对数值平方和进行有理化投影前使用保持秩结构不变的 Newton 迭代来精化它。对于小问题我们可以不用半定规划而直接生成随机的数值平方和作为 Newton 迭代的初始值, 对于大问题应当探索问题中的稀疏结构以减小生成的半定规划和平方和的大小规模。

关键词: 最大公因式, 近似因式分解, 平方和, 半定规划, 全局最优化, 混合方法。

Abstract

In this paper, we discuss the global optimality of several well-known problems in hybrid symbolic-numeric computation via SOS (Sums Of Squares) relaxations and semidefinite programming (SDP), and exact certification of rational lower bounds near the global optima via rationalizing SOS.

The problem of computing approximate GCDs (Greatest Common Divisors) of several polynomials with real or complex coefficients, the approximate factorization problem and a model problem by Siegfried Rump can be formulated as polynomial or rational function optimization problems. We present algorithms based on full or sparse SOS relaxations for solving the involved polynomial or rational function optimization problems with or without constraints.

We generalize the technique by Peyrl and Parillo [Proc. SNC 2007] of transforming a numerical SOS representation of a positive semidefinite (PSD) polynomial into an exact rational identity to computing lower bound certificates. Our algorithms successfully certify accurate rational lower bounds near the global optima for benchmark approximate polynomial GCDs and multivariate polynomial irreducibility radii from the literature, and factor coefficient bounds in Rump's model problem (up to $n = 14$, factor degree = 13).

The numeric results and SOSes produced by the current fixed precision SDP packages (SOSTOOLS, YALMIP, SeDuMi etc.) are usually too coarse. Therefore, we can refine the results by Newton-Lagrange method, and before projection to exact SOSes via Maple's exact linear algebra we refine the SOSes by rank-preserving Newton iteration. For smaller problems the starting SOSes for Newton can be guessed without SDP ("SDP-free SOS"), but for larger inputs we additionally appeal to sparsity techniques in our SDP formulation.

Keywords: greatest common divisor, approximate factorization, sums of squares, semidefinite programming, global minimization, hybrid method.

目 录

摘要	i
Abstract	iii
目录	v
第一章 引言	1
1.1 问题和研究概述	1
1.2 使用的方法	3
1.2.1 半定规划 (Semidefinite Programming)	3
1.2.2 平方和 (Sums Of Squares) 和矩量 (Moment) 方法	4
1.2.3 Newton-Lagrange 方法	5
1.3 论文的主要内容	6
第二章 多项式近似最大公因式 (GCD) 问题	7
2.1 前言	7
2.2 最小化问题	8
2.2.1 多项式最小化问题	8
2.2.2 有理函数最小化问题	9
2.2.3 带限制条件的多项式最小化问题	14
2.3 最小化问题中的稀疏性	16
2.3.1 Newton 多面体稀疏性	16
2.3.2 稀疏情形下的全局最优解求解	18
2.3.3 关联结构稀疏性	20
2.3.4 不同稀疏策略的比较	21
2.4 具体实现和例子	22

第三章 多项式近似因式分解问题	25
3.1 前言	25
3.2 固定因式次数的近似因式分解问题	25
3.3 分解成多个因式的近似因式分解问题	27
第四章 多项式平方和 (SOS) 有理化精确验证方法	29
4.1 前言	29
4.2 平方和的产生和有理化技术	31
4.2.1 半定规划和 Newton 迭代	31
4.2.2 平方和有理化算法	33
4.3 应用和例子	35
4.3.1 多项式近似最大公因式问题	35
4.3.2 多项式近似因式分解问题	36
4.3.3 多项式精确平方和分解	38
4.4 Siegfried Rump 的模型问题的求解和下界验证	39
4.4.1 问题的数学背景	39
4.4.2 半定规划求解有理函数最优解	41
4.4.3 精确验证下界	43
第五章 结论与展望	45
参考文献	47
发表文章目录	55
个人简介	57
致谢	59

表 格

2.1	不同稀疏策略之间的对比试验结果	22
2.2	文章 [3, Chin et al., 1998] 中例子的试验结果	23
2.3	随机生成例子的试验结果	23
3.1	多项式近似因式分解问题的试验结果	26
4.1	半定规划与 Rump 的上界的对比试验结果	43
4.2	平方和有理化验证方法与 Rump 的下界的对比试验结果	44

第一章 引言

1.1 问题和研究概述

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。考虑一类符号数值混合计算问题, 就是怎样对不精确的浮点数输入做最小的扰动以得到非平凡的输出结果, 对这类问题的研究产生了很多数值最优化算法 (参见综述文章 [64])。在已有的研究中, 用基于 Newton 迭代和 Lagrange 乘数法的保持结构整体最小二乘 (Structured Total Least Squares) 算法, 可以有效的求解多项式近似最大公因式 (Greatest Common Divisor) 问题 [22, 23]、多变元多项式近似因式分解问题 [21] 以及稀疏多变元多项式和有理函数插值问题 [24]。这些已有的最优化技术方法可以快速求得问题的局部最优解 (上界)。实际上通过随机选取初始值和投射, 试验显示求得的往往也是全局最优解。

半定规划 (Semidefinite Programming) [37, 57, 62] 是线性规划 (Linear Programming) 较深远的更一般化的问题, 理论上它可以在多项式时间 (polynomial-time) 内用对偶内点等方法快速求解, 并且可以用它来产生以前难以求解的经典组合最优化问题的近似问题。一般的带限制条件的多项式或有理函数全局最小化问题可描述为

$$\left. \begin{aligned} r^* &:= \min_{\xi \in \mathbb{R}^n} \frac{f(\xi)}{g(\xi)} \\ s.t. \quad & h_1(\xi) \geq 0, \dots, h_l(\xi) \geq 0, \\ & \text{其中 } f, g, h_1, \dots, h_l \in \mathbb{R}[X_1, \dots, X_n] \end{aligned} \right\} \quad (1.1)$$

(无限制条件时省略 h_i)。在多项式最优化情形设 $g(X) = 1$; 在有理函数最优化情形可以假设 $g(X) \neq 0$ 在所有可行解上非负, 否则可以替换 $\frac{f(X)}{g(X)}$ 为 $\frac{f(X)g(X)}{g(X)^2}$ 。通过平方和 (Sums Of Squares) 和 Moment 方法 [42, 29, 44, 17, 39] 以及相应的稀疏技术 [47, 28, 43, 60, 30, 38], 此最优化问题可以转化成半定规划求解并得到全局最优解或下界。

平方和方法是首先由 Shor [54, 55] 引入到多项式的全局最优化问题求解中的一种方法, 后来它被扩展到了有限制条件情形和有理函数最优化情形。在问

题 (1.1) 的有限制条件情形, 根据 à la Putinar 的 Positivstellensatz [41], 当多项式 $h_1(X), \dots, h_l(X)$ 满足一定的条件时, 对于问题的任意下界 $r \in \mathbb{R}$ 存在多项式 $v_{i,j}(X) \in \mathbb{R}[X_1, \dots, X_n]$, $0 \leq i \leq l$, $1 \leq j \leq \nu_i$ 使得

$$f(X) - rg(X) = \sum_{j=1}^{\nu_0} v_{0,j}(X)^2 + \sum_{i=1}^l \left(h_i(X) \cdot \sum_{j=1}^{\nu_i} v_{i,j}(X)^2 \right), \quad (1.2)$$

此时 (1.1) 可以转化为一个等价的平方和规划 (SOS Programming) 并且可得到一个收敛的半定规划序列。在无限制条件的情形, 因为不是所有的半正定 (Positive Semidefinite) 多项式都可写成多项式平方和形式 (例如 Motzkin 多项式), 所以得到的平方和规划一般是松弛的, 但根据 Emil Artin 的定理可给 (1.2) 中的 $v_{i,j}(X)$ 添加一个公共的多项式分母使其恒成立 [48]。

多项式近似最大公因式、多项式近似因式分解等问题可以通过多种不同的方式转变为不带或带限制条件的多项式或有理函数最小化问题。将最小化问题写成 (1.1) 中的形式, 然后应用稠密或稀疏的平方和和 Moment 方法, 我们可以将问题转化成半定规划求解并且得到全局最优解或下界。结合局部 (上界) 算法我们同样可以验证解的全局最优性或得到全局最优解的范围。

很多实际问题中需要得到问题精确的下界, 而半定规划计算得到的数值结果存在浮点数舍入误差, 并且因为全局最优解可能是代数数 [40], 所以计算结果只是近似的满足等式 (1.2)。在 [45] 中 Peyrl 和 Parrillo 使用的数值平方和有理化投影的方法启发我们将其推广到通过有理化等式 (1.2) 来得到精确平方和分解并验证问题 (1.1) 的全局精确有理下界。

对于上述近似多项式问题和 Siegfried Rump 的模型问题 [51, 50], 我们可以有效求得它们的全局最优解并且精确验证其下界。在实际试验中固定精度半定规划软件的数值结果误差较大时, 我们可使用 Newton 迭代精化全局最优解以提高精度。我们试验得到了比 Rump 更好的下界, 并且试验显示我们的方法在多项式有理平方和分解和下界验证上比已有符号算法更快。半定规划比我们的局部 (上界) 算法要复杂得多, 仍然有很多值得进一步研究的地方。

1.2 使用的方法

1.2.1 半定规划 (Semidefinite Programming)

一般的半定规划 [37, 57, 62] 可写成

$$\left. \begin{aligned} p^* &:= \min_{x \in \mathbb{R}^m} c^T x \\ \text{s.t. } & F(x) \succeq 0, \end{aligned} \right\} \quad (1.3)$$

其中向量 $c \in \mathbb{R}^m$, 矩阵 $F(x) := F_0 + \sum_{i=1}^m x_i F_i$ 为实对称矩阵 F_0, F_1, \dots, F_m 的线性组合。限制条件 $F(x) \succeq 0$ 叫做线性矩阵不等式 (Linear Matrix Inequality), 表示矩阵 $F(x)$ 是半正定矩阵 (即 $z^T F(x) z \geq 0$ 对于任意实向量 z 成立)。半定规划的目标函数和限制条件都满足凸性质, 所以它的可行解集为凸集, 它是凸最优化问题并且可以使用对偶内点等方法快速求解。半定规划包含线性规划并且很多问题也可以转化为半定规划求解。

半定规划 (1.3) 的对偶半定规划为

$$\left. \begin{aligned} d^* &:= \max_Z -\text{Trace}(F_0 Z) \\ \text{s.t. } & \text{Trace}(F_i Z) = c_i, \quad i = 1, \dots, m, \\ & Z \succeq 0, \end{aligned} \right\} \quad (1.4)$$

其中变量 $Z = Z^T$ 为实对称矩阵, c_i 为向量 c 中的相应元素。记号 $\text{Trace}(\cdot)$ 表示矩阵的迹, 即矩阵主对角线上所有元素的和。对于任意半正定矩阵 A, B , 可以设 $B = VV^T$, 则 $\text{Trace}(AB) = \text{Trace}(V^T AV) \geq 0$, 等号成立当且仅当 $AB = 0$ 。半定规划 (1.3) 和 (1.4) 互为对偶问题, 对于它们的任意可行解 x, Z 成立

$$c^T x + \text{Trace}(F_0 Z) = \sum_{i=1}^m \text{Trace}(x_i F_i Z) + \text{Trace}(F_0 Z) = \text{Trace}(F(x) Z) \geq 0,$$

由此可知弱对偶 $p^* \geq d^*$ 成立, 并且 $p^* = d^*$ 时它们的任意最优解 x^*, Z^* 满足 $F(x^*) Z^* = 0$ 。如下强对偶定理的证明可参见 [37]。

定理 1.1. 如果以下条件之一成立, 那么 $p^* = d^*$ 。

1. 原始问题 (1.3) 存在严格可行解, 即存在 x 满足 $F(x) \succ 0$ 。
2. 对偶问题 (1.4) 存在严格可行解, 即存在 $Z = Z^T \succ 0$ 满足 $\text{Trace}(F_i Z) = c_i, i = 1, \dots, m$ 。

如果两个条件都成立, 那么两个对偶问题的最优解集都非空。

1.2.2 平方和 (Sums Of Squares) 和矩量 (Moment) 方法

数学很多领域的一个基本问题是判断函数的全局非负性, 这里考虑多项式函数 $p(X) \in \mathbb{R}[X_1, \dots, X_n]$ 。如果多项式 $p(X)$ 满足

$$p(\xi) \geq 0, \forall \xi \in \mathbb{R}^n,$$

则称其为半正定 (Positive Semidefinite) 多项式。显然 $p(X)$ 是半正定多项式的一个必要条件是它关于每个变元 X_i 的次数是偶数。一般的多项式全局正定性判定问题是 NP-hard 的。如果 $p(X)$ 存在一个多项式平方和分解

$$p(X) = \sum_j v_j(X)^2 \in \sum \mathbb{R}[X]^2,$$

那么肯定是半正定 (PSD) 多项式。不是每个半正定多项式都可以写成多项式平方和, 例如 Motzkin 多项式 $X_1^4 X_2^2 + X_1^2 X_2^4 + X_3^6 - 3X_1^2 X_2^2 X_3^2$ 。已知对于单变元多项式、二次多项式和双变元四次多项式, 半正定条件和存在多项式平方和分解是等价的。Emil Artin 证明了对于任意的半正定多项式 $p(X)$ 存在多项式 $v(X)$ 使得 $p(X)v(X)^2$ 可以写成多项式平方和, 肯定地回答了 Hilbert 的第十七问题, 后来 Bruce Reznick 证明了 $p(X)$ 为正定多项式时总可以取足够大的整数 N 使得 $v(X) = (\sum_{i=1}^n X_i^2)^N$ 满足要求。更多相关介绍可参见文章 [48]。

一般的多项式全局最优化问题属于 NP-hard 的问题。Shor [54, 55] 首先将平方和方法引入到多项式全局最优化问题求解中, 后来 Parrilo [42, 44] 和 Lasserre [29] 分别从平方和和 Moment 的角度进一步发展研究了相应的对偶半定规划, 文章 [17, 39] 中将其推广到了有理函数情形。对于一般多项式或有理函数最小化问题 (1.1) 的无限制条件情形, 等价于

$$\left. \begin{aligned} r^* &:= \max_{r \in \mathbb{R}} r \\ s.t. \quad & f(X) - rg(X) \geq 0. \end{aligned} \right\} \quad (1.5)$$

替换限制条件为平方和松弛 (SOS relaxation) 条件 $f(X) - rg(X) \in \sum \mathbb{R}[X]^2$ 得到的平方和规划 (SOS programming) 可以写成半定规划 [39]

$$\left. \begin{aligned} r_{sos}^* &:= \sup_{r \in \mathbb{R}, W} r \\ s.t. \quad & f(X) - rg(X) = m_d(X)^T W m_d(X), \\ & W \succeq 0, \end{aligned} \right\} \quad (1.6)$$

其中 $m_d(X)$ 为所有全次数小于等于 $d = \lceil \frac{\max(\text{tdeg}(f), \text{tdeg}(g))}{2} \rceil$ 的单项式组成的列向量, 实对称半正定矩阵 W 的行列数为 $\binom{n+d}{n}$ 并且半定规划展开后有 $\binom{n+2d}{n}$ 个等式限制条件。记 $f(X) = \sum_{\alpha} f_{\alpha} X^{\alpha}$, $g(X) = \sum_{\alpha} g_{\alpha} X^{\alpha}$, 那么半定规划 (1.6) 的对偶半定规划 [29, 39] 为

$$r_{mom}^* := \inf_y \left. \begin{array}{l} \sum_{\alpha} f_{\alpha} y_{\alpha} \\ s.t. \sum_{\alpha} g_{\alpha} y_{\alpha} = 1, \\ M_d(y) \succeq 0, \end{array} \right\} \quad (1.7)$$

其中实对称半正定矩阵 $M_d(y) := (y_{\alpha+\beta})_{0 \leq |\alpha|, |\beta| \leq d}$ 称为关于实向量 y 的第 d 次 Moment 矩阵。理论上 $r^* \geq r_{mom}^* \geq r_{sos}^*$, 当 (1.6) 有一个可行解时, 强对偶 $r_{mom}^* = r_{sos}^*$ 成立并且 $f(X) - r_{sos}^* g(X)$ 可以写成多项式平方和 [29, 39]。当计算出的对应于最优解的矩阵 $M_d(y^*)$ 满足某个平坦扩展条件时 $r^* = r_{mom}^*$, 并且原最优化问题的全局最优点可通过求解一个数值特征值问题得到 [13, 39]。

对于有限制条件的一般多项式或有理函数最小化问题 (1.1), 根据 à la Putinar 的 Positivstellensatz [41] (1.2) 可以类似的形成两个对偶半定规划序列, 在满足一定条件时它们的最优值都单调收敛到原问题的全局最小值 r^* [29, 39]。如果已知问题 (1.1) 在一个球 $\|X\|_2^2 \leq a^2$ 内肯定存在全局最优解, 那么即使在无限制条件情形也可以添加上这个限制条件以保证收敛性。对于等式限制条件可以看作两个相反的不等式限制条件。此外关于平方和规划中的稀疏性可参见 [47, 28, 43, 60, 30, 38]。

1.2.3 Newton-Lagrange 方法

考虑带等式限制条件的最优化问题

$$\left. \begin{array}{l} \min_{\xi \in \mathbb{R}^n} f(\xi) \\ s.t. \quad c(\xi) = 0, \end{array} \right\} \quad (1.8)$$

其中目标函数 $f(X)$ 和函数向量 $c(X)$ 中的函数都是光滑实函数。如果等式限制向量 $c(X)$ 的 Jacobi 矩阵 $A(X)$ (其中 $A_{i,j} = \partial c_i(X) / \partial X_j$) 在最优点的附近是行满秩的, 那么由 Lagrange 乘数法可知相应的最优点满足方程组

$$F(X, \lambda) = \begin{bmatrix} \nabla f(X) - A(X)^T \lambda \\ c(X) \end{bmatrix} = 0.$$

记 Lagrange 函数 $L(X, \lambda) = f(X) - \lambda^T c(X)$ 关于变量 X 的 Hessian 矩阵为 $H(X, \lambda) = (\frac{\partial^2 L(X, \lambda)}{\partial X_i \partial X_j})_{n \times n}$, 则上面方程组的 Newton 迭代为

$$\begin{bmatrix} \tilde{X} \\ \tilde{\lambda} \end{bmatrix} = \begin{bmatrix} X \\ \lambda \end{bmatrix} + \begin{bmatrix} \Delta X \\ \Delta \lambda \end{bmatrix}, \begin{bmatrix} H(X, \lambda) & -A(X)^T \\ A(X) & 0 \end{bmatrix} \begin{bmatrix} \Delta X \\ \Delta \lambda \end{bmatrix} = -F(X, \lambda).$$

如果在最优点的附近, $A(X)$ 是行满秩的并且 $d^T H(X, \lambda) d > 0$ 对于任意满足 $d \neq 0, A(X)d = 0$ 的向量 d 成立, 那么迭代是定义明确的。以上迭代方法有时被称作 Newton-Lagrange 方法, 该方法在初始点很接近最优解时是十分有效的。

1.3 论文的主要内容

在这篇文章中, 我们主要讨论了怎样使用半定规划求解近似多项式问题的全局最优解, 以及通过平方和有理化精确验证全局最优问题下界的方法。

在第二章, 我们详细讨论了多项式近似最大公因式问题的半定规划求解 (见 [31, 32])。首先, 我们研究了近似 GCD 问题转化成的最小化问题的形式 (多项式、有理函数和带等式限制条件的多项式形式), 并且应用相应的平方和松弛方法转化成半定规划求解。然后, 我们探索了这些最小化问题形式中的不同稀疏性 (Newton 多面体、关联矩阵结构), 并且给出了近似 GCD 问题的稀疏性分析和稀疏情形下的全局最优解求解方法。最后是具体实现和大量例子的试验结果。

在第三章, 我们讨论了多种不同形式的多项式近似因式分解问题的半定规划求解 (见 [18])。我们讨论了各种不同形式之间的关系并且给出了一些例子的试验结果。

在第四章, 我们研究了通过平方和有理化投影精确验证问题下界的方法 (见 [19])。首先, 我们详细介绍了我们的算法和技术, 包括怎样从半定规划和 Newton 迭代产生数值平方和以及有理化投影算法。然后, 我们在几个例子上示范了我们的方法在近似 GCD 问题、近似因式分解问题和求解多项式有理平方和分解上的应用。最后, 我们将半定规划和下界验证方法应用于 Siegfried Rump 的一个公开模型问题 [51, 50] 的求解。

在最后一章, 我们总结了已有的工作成果并讨论了以后可以继续工作努力的方向。

第二章 多项式近似最大公因式 (GCD) 问题

2.1 前言

设域 F 为实数域 \mathbb{R} 或复数域 \mathbb{C} , 对于多个多项式 $f_1, \dots, f_s \in F[z_1, \dots, z_t]$, 计算最小的扰动使得扰动多项式有一个全次数 $k \geq 1$ 的最大公因式 (Greatest Common Divisor) 的问题即

$$r^* := \min_{p, u_1, \dots, u_s} \|f_1 - p \cdot u_1\|_2^2 + \|f_2 - p \cdot u_2\|_2^2 + \dots + \|f_s - p \cdot u_s\|_2^2, \quad (2.1)$$

其中多项式 $p, u_1, \dots, u_s \in F[z_1, \dots, z_t]$ 的全次数 (total degree) 满足 $\text{tdeg}(p) = k$ 和 $\text{tdeg}(p \cdot u_i) \leq d_i = \text{tdeg}(f_i)$, $1 \leq i \leq s$ 。已有很多有效的方法可以快速得到近似 GCD 问题的局部最优解, 这里我们主要关注如何求得该问题的全局最优解和验证某局部最优解的全局最优性。近似 GCD 问题可以转化成不同形式的最优化问题并且可以应用多种数值最优化方法求解, 已有的研究可以参见文章 [3, 22] 以及其中的参考文献。文章 [23] 中指出最优化问题 (2.1) 在一定限制条件下有一个全局最优解。文章 [26, 27] 中提出了一个基于有理函数全局最优化的算法计算单变元多项式近似 GCD 问题, 该算法效率最低的部分是求解包含两个高次双变元多项式的方程组的所有实根。文章 [39] 中揭示了平方和 (SOS) [42, 44] 和 Moment 方法 [29] 可以被用来求解多项式或有理函数的全局最小化问题, 包括由近似 GCD 计算问题转化成的有理函数最小化问题。多项式或者有理函数最小化问题可以通过不同的平方和松弛 (SOS relaxation) 转化为平方和规划 (SOS programming), 平方和规划可以写成半定规划 (semidefinite programming) 形式, 而半定规划可以用对偶内点法等快速算法求解。关于半定规划的介绍参见文章 [37, 57, 62]。在接下来的章节里, 类似于 [3, 26, 27, 22, 39], 我们将近似 GCD 问题转化成不同的最优化问题, 并且应用不同的平方和方法将它们转化成半定规划, 然后用常见的半定规划软件包计算求解并同以往算法比较。我们也探索了在近似 GCD 问题的平方和规划中的各种稀疏性, 并且使用 Gauss-Newton 迭代方法来精化计算结果。

2.2 最小化问题

在这一节里，我们将探索怎样把近似 GCD 问题转化成最优化问题，并应用相应的平方和方法将它们转化成半定规划求解。关于平方和方法及其对偶问题的描述可参考文章 [42, 44, 29, 17, 39]。

2.2.1 多项式最小化问题

最小化问题 (2.1) 可以看作一个非线性最小二乘问题。文章 [3] 中的研究表明，如果给定一个较好的初始近似 GCD，那么用类似 Newton 迭代的最优化方法或 Levenberg-Marquardt 方法可以很快收敛到全局最优解。但是对于一般的初始近似 GCD，这些方法可能经过很多次迭代后只是收敛到某个局部最优解。

平方和方法是由 Shor [54, 55] 引入的一种新的不同的方法，后来 Parrilo [42, 44] 和 Lasserre [29] 进一步发展了这种方法。应用它的主要思想是将最小化问题 (2.1) 写成多项式最小化问题

$$\min_{\xi \in \mathbb{R}^n} f(\xi)$$

的形式并且通过平方和松弛 (SOS relaxation) 转化为如下半定规划

$$\left. \begin{aligned} r_{sos}^* &:= \sup_{r \in \mathbb{R}, W} r \\ s.t. \quad & f(X) - r = m_d(X)^T W m_d(X), \\ & W \succeq 0, \end{aligned} \right\} \quad (2.2)$$

其中 W 为实对称半正定矩阵， $m_d(X)$ 为所有全次数小于等于 d 的单项式组成的列向量。

使用待定系数法，可以知道这里目标多项式函数为

$$f(X) = \sum_{i=1}^s \|f_i - p \cdot u_i\|_2^2 = \sum_{i=1}^s \sum_{|\alpha| \leq d_i} |f_{i,\alpha} - \sum_{\beta+\gamma=\alpha} p_{\beta} u_{i,\gamma}|^2.$$

由此 $d = \lceil \frac{\text{tdeg}(f)}{2} \rceil = 2$ ，实对称矩阵 W 行列数为 $\binom{n+2}{2}$ 并且半定规划 (2.2) 展开后有 $\binom{n+4}{4}$ 个等式限制条件。

设待定多项式 p, u_1, \dots, u_s 的所有待定系数中待定变量的个数分别为 $n(p), n(u_1), \dots, n(u_s)$ (详细说明见注 1)，则目标函数的所有变量可表示为

$$X = \{p_1, \dots, p_{n(p)}\} \cup \left(\bigcup_{i=1}^s \{u_{i,1}, \dots, u_{i,n(u_i)}\} \right)$$

并且变量个数 $n = n(p) + \sum_{i=1}^s n(u_i)$ 。

注 1. 如果域 $F = \mathbb{R}$, 则实系数多项式 p, u_i 的每个系数可以对应一个待定变量并且 $n(p) = \binom{t+k}{t}$, $n(u_i) = \binom{t+d_i-k}{t}$ 。如果域 $F = \mathbb{C}$, 可以假设 p 的一个系数为实数而 p, u_i 的其他每个系数由实部和复部两个待定变量形成, 那么 $n(p) = 2\binom{t+k}{t} - 1$, $n(u_i) = 2\binom{t+d_i-k}{t}$ 。在单变元情形 ($t = 1$), 可以假设 p 是首一的, 那么 $n(p)$ 在实数情形是 k 并且在复数情形是 $2k$ 。

记 $f(X) = \sum_{\alpha} f_{\alpha} X^{\alpha}$, 则半定规划 (2.2) 的对偶半定规划 [29] 为

$$\left. \begin{aligned} r_{mom}^* &:= \inf_y \sum_{\alpha} f_{\alpha} y_{\alpha} \\ s.t. \quad &y_{0, \dots, 0} = 1, \\ &M_d(y) \succeq 0, \end{aligned} \right\} \quad (2.3)$$

其中实对称半正定矩阵 $M_d(y) := (y_{\alpha+\beta})_{0 \leq |\alpha|, |\beta| \leq d}$ 称为关于实向量 y 的第 d 次 Moment 矩阵。半定规划 (2.2) 有一个对应于 $r = 0$ 的可行解, 从而根据 [29] 中的结论可知强对偶 $r_{mom}^* = r_{sos}^*$ 成立并且 $f(X) - r_{sos}^*$ 可以写成多项式平方和。当计算出的对应于最优解的矩阵 $M_d(y^*)$ 满足某个平坦扩展条件时 $r^* = r_{mom}^*$, 并且原最优化问题的全局最优点可通过求解一个数值特征值问题得到 [13]。

2.2.2 有理函数最小化问题

记多项式 f_i, u_i, p 的系数向量分别为 $\mathbf{f}_i, \mathbf{u}_i, \mathbf{p}$, 多项式乘积 $p \cdot u_i$ 的系数向量可记为 $A_i \mathbf{u}_i$ ($A_i = A_i(\mathbf{p})$ 称为卷积矩阵), 那么最小化问题 (2.1) 可以直接写成如下矩阵向量表示的形式

$$\min_{\mathbf{p}, \mathbf{u}_1, \dots, \mathbf{u}_s} \|\mathbf{f}_1 - A_1 \mathbf{u}_1\|_2^2 + \dots + \|\mathbf{f}_s - A_s \mathbf{u}_s\|_2^2. \quad (2.4)$$

如果固定多项式 p 的系数, 那么矩阵 A_i 固定, 并且 p 非零时 A_i 是列满秩的。由线性最小二乘问题的结论可以知道, 问题取得最小值时成立

$$\mathbf{u}_i := (A_i^* A_i)^{-1} A_i^* \mathbf{f}_i, \quad 1 \leq i \leq s, \quad (2.5)$$

将其代入上面的问题可以得到最小化问题

$$\min_{\mathbf{p}} \sum_{i=1}^s (\mathbf{f}_i^* \mathbf{f}_i - \mathbf{f}_i^* A_i (A_i^* A_i)^{-1} A_i^* \mathbf{f}_i), \quad (2.6)$$

A_i^* 和 \mathbf{f}_i^* 分别表示矩阵 A_i 和向量 \mathbf{f}_i 的共扼转置。这个最小化问题是一个无限制条件的有理函数最小化问题，其目标函数的分母为正定多项式

$$\text{lcm}(\det(A_1^*A_1), \dots, \det(A_s^*A_s)).$$

以上问题形式为 [3, 15, 26, 27, 66, 65] 中计算单变元多项式近似 GCD 和 [16] 中计算有一个线性（或固定次数）公因式的最近双变元多项式问题的一般化推广。

将最小化问题 (2.6) 写成有理函数最小化问题

$$\min_{\xi \in \mathbb{R}^n} \frac{f(\xi)}{g(\xi)},$$

可知这里目标函数的分子和分母 $f(X), g(X) \in \mathbb{R}[X_1, \dots, X_n]$ 分别为半正定和正定多项式，所有变量 $X = \{p_1, \dots, p_{n(p)}\}$ 并且变量的个数 $n = n(p)$ ，全次数 $\text{tdeg}(f) \leq \text{tdeg}(g) \leq 2 \sum_{i=1}^s \binom{t+d_i-k}{t}$ 。同上一节的多项式最小化问题比较可知，虽然目标函数的变量个数大大减少了，但是其中多项式的次数却增加了很多。类似于 (2.2)，有理函数最小化问题可以通过平方和松弛（SOS relaxation）转化为半定规划 [39]

$$\left. \begin{aligned} r_{sos}^* &:= \sup_{r \in \mathbb{R}, W} r \\ \text{s.t. } & f(X) - rg(X) = m_d(X)^T W m_d(X), \\ & W \succeq 0, \end{aligned} \right\} \quad (2.7)$$

这里 $m_d(X)$ 为所有全次数小于等于 $d = \lceil \frac{\max(\text{tdeg}(f), \text{tdeg}(g))}{2} \rceil$ 的单项式组成的列向量，实对称半正定矩阵 W 的行列数为 $\binom{n+d}{n}$ 并且半定规划展开后有 $\binom{n+2d}{n}$ 个等式限制条件。记 $f(X) = \sum_{\alpha} f_{\alpha} X^{\alpha}, g(X) = \sum_{\alpha} g_{\alpha} X^{\alpha}$ ，则类似于 (2.3)，半定规划 (2.7) 的对偶半定规划 [39] 为

$$\left. \begin{aligned} r_{mom}^* &:= \inf_y \sum_{\alpha} f_{\alpha} y_{\alpha} \\ \text{s.t. } & \sum_{\alpha} g_{\alpha} y_{\alpha} = 1, \\ & M_d(y) \succeq 0. \end{aligned} \right\} \quad (2.8)$$

关于其中的对偶性、全局最优性和全局最优点求解类似于多项式情形 [13, 39]。

例 2.1. 给定两个多项式

$$f_1(z) = z(z+1)^2, f_2(z) = (z-1)(z+1)^2 + 1/10$$

并且 $k = 2, F = \mathbb{R}$ 。求解相应的半定规划 (2.2) 和其对偶问题, 目标多项式为 (待定多项式 p 首一)

$$\begin{aligned} f(X) = & \|f_1 - p \cdot u_1\|_2^2 + \|f_2 - p \cdot u_2\|_2^2 = p_1^2 u_{1,1}^2 + (1 - p_1 u_{1,2} - p_2 u_{1,1})^2 \\ & + (2 - p_2 u_{1,2} - u_{1,1})^2 + (1 - u_{1,2})^2 + (-9/10 - p_1 u_{2,1})^2 \\ & + (-1 - p_1 u_{2,2} - p_2 u_{2,1})^2 + (1 - u_{2,1} - p_2 u_{2,2})^2 + (1 - u_{2,2})^2, \end{aligned}$$

我们可以求得最优值 $r_{sos}^* \approx 9.3876e - 4$, 相应的半定规划 (2.2) 中半正定矩阵 W 的行列数为 28。从对偶问题的计算结果我们知道所求的值为原问题的全局最小值, 并且计算出一个全局最优点

$$X^* \approx (0.9335, 1.9778, 0.02569, 1.0013, -0.9739, 0.9975),$$

它对应于首一近似 GCD 多项式

$$p(z) \approx 0.9335 + 1.9778z + z^2$$

和余因式 $u_1(z) \approx 0.02569 + 1.0013z, u_2(z) \approx -0.9739 + 0.9975z$ 。

求解相应的半定规划 (2.7) 和其对偶问题, 其中的目标有理函数的分子和分母分别为

$$\begin{aligned} f(X) = & 12/5 p_2 p_1 + 7 p_1^4 + 281/100 p_2^4 - 281/50 p_2^2 p_1 + 11/5 p_1^2 p_2^2 \\ & - 6 p_2^3 + 9/5 p_1^3 + 981/100 p_1^2 + 581/100 p_2^2 + 281/100 \\ & - 6 p_2 p_1^2 - 9/5 p_2^3 p_1 + 9/5 p_1 - 2 p_2 - 2 p_2 p_1^3, \\ g(X) = & p_1^4 + p_1^2 p_2^2 + 2 p_1^2 + p_2^4 + p_2^2 + 1 - 2 p_2^2 p_1, \end{aligned}$$

我们可以求得最优值 $r_{sos}^* \approx 9.3876e - 4$, 相应的半定规划 (2.7) 中的半正定矩阵 W 的行列数为 6。从对偶问题的计算结果我们可以计算出一个最优点 $X^* \approx (0.9335, 1.9778)$, 计算目标有理函数在 X^* 点的值可知

$$\frac{f(X^*)}{g(X^*)} \approx 9.3876e - 4 \approx r_{sos}^*,$$

这表示 X^* 是全局最优点, 它对应于相同的首一近似 GCD 多项式 $p(z)$ 。

例 2.2. 给定两个多项式

$$f_1(z_1, z_2) = z_1^2 + 2z_1z_2 + z_2^2 - 1, \quad f_2(z_1, z_2) = z_1^2 + z_1z_2 - z_2 - 1.01$$

并且 $k = 1, F = \mathbb{R}$ 。求解相应的半定规划 (2.2) 和其对偶问题, 目标多项式为

$$\begin{aligned} f(X) = & \|f_1 - p \cdot u_1\|_2^2 + \|f_2 - p \cdot u_2\|_2^2 = (-1 - p_1u_{1,1})^2 + (-p_1u_{1,3} - p_3u_{1,1})^2 \\ & + (-p_1u_{1,2} - p_2u_{1,1})^2 + (2 - p_2u_{1,3} - p_3u_{1,2})^2 + (1 - p_3u_{1,3})^2 \\ & + (1 - p_2u_{1,2})^2 + (-1.01 - p_1u_{2,1})^2 + (-p_1u_{2,3} - p_3u_{2,1})^2 \\ & + (-1 - p_1u_{2,2} - p_2u_{2,1})^2 + (1 - p_2u_{2,3} - p_3u_{2,2})^2 + (1 - p_3u_{2,3})^2 + p_2^2u_{2,2}^2, \end{aligned}$$

我们可求得最优值 $r_{sos}^* \approx 3.89306e - 5$ 并且相应的半定规划 (2.2) 中半正定矩阵 W 的行列数为 55。

求解相应的半定规划 (2.7) 和其对偶问题, 其中的目标有理函数的分子和分母分别为

$$\begin{aligned} f(X) = & -20.02p_2p_3^3p_1^2 + 26.0804p_1^2p_3^2p_2^2 - 22.04p_3p_2p_1^4 - 22.02p_3p_2^3p_1^2 \\ & + 5.98p_1^4p_2^2 + 9p_1^4p_3^2 + 6.0001p_1^2p_2^4 + 10.0201p_1^2p_3^4 + 13.0402p_2^4p_3^2 \\ & + 14.0402p_2^2p_3^4 + 8p_1^6 + 4.0201p_2^6 + 4.0201p_3^6 - 10p_3^3p_2^3 - 6p_2p_3^5 \\ & - 4p_3p_2^5 - 6.04p_3p_1^3p_2^2 - 2p_2p_3^4p_1 - 6.02p_1p_3p_2^4 - 4.02p_1p_3^3p_2^2 \\ & - 2.02p_1^3p_3^3 - 2.02p_1p_3^5 + 2p_2p_1^5 + 2p_2^3p_1^3 + 2p_1p_2^5, \\ g(X) = & p_1^6 + 2p_1^4p_2^2 + 2p_1^4p_3^2 + 2p_1^2p_2^4 + 5p_1^2p_3^2p_2^2 + 2p_1^2p_3^4 + p_2^6 + 2p_2^4p_3^2 \\ & + 2p_2^2p_3^4 + p_3^6, \end{aligned}$$

我们可以求得最优值

$$r_{sos}^* \approx 3.89306e - 5.$$

注意这里 $f(X), g(X)$ 是关于公因式 p 的系数的齐次多项式, 相应的半定规划 (2.7) 中半正定矩阵 W 行列数为 10。类似单变元情形, 从对偶问题的计算结果我们计算出一个全局最优近似 GCD 多项式

$$p(z) \approx 1.00199 + 0.99937z_2 + z_1.$$

例 2.3. 给定两个多项式

$$f_1(z) = (z - 0.3)(z + 4.6)(z - 1.45)(z + 10),$$

$$f_2(z) = (z - 0.301)(z + 4.592)(z - 1.458)(z - 0.6)(z - 15)(z + 2)$$

并且 $k = 3, F = \mathbb{R}$ 。求解相应的半定规划 (2.2) 和其对偶问题, 我们求得最优值 $r_{sos}^* \approx 0.0156$ 和 $p(z) \approx 2.0120 - 7.6509z + 2.8526z^2 + z^3$, 相应的半定规划 (2.2) 中半正定矩阵 W 的行列数为 55。我们求解相应的半定规划 (2.7) 和其对偶问题可以得到最优值 $r_{sos}^* \approx 0.0156$, 相应的半定规划 (2.7) 中半正定矩阵 W 的行列数为 84, 比多项式形式得到的半定规划大。

例 2.4. [22] 给定两个多项式

$$f_1(z) = 1000z^{10} + z^3 - 1, f_2(z) = z^2 - \frac{1}{100}$$

并且 $k = 1, F = \mathbb{R}$ 。求解相应的半定规划 (2.7) 和其对偶问题, 我们可求得最优值 $r_{sos}^* \approx 0.042157904$ 和 $p(z) \approx z - 0.4941448$, 相应的半定规划 (2.7) 中半正定矩阵 W 的行列数为 13。文章 [22] 中表明, 对于不同的初始点, 在大约平均十步迭代后, STLN 算法可能收敛到如下的局部最优值

$$0.0421579, 0.0463113, 0.0474087, 0.0493292, \dots$$

例 2.5. [23] 给定两个多项式

$$f_1(z) = z^2 + 2z + 1, f_2(z) = z^2 - 2z + 2$$

并且 $k = 1, F = \mathbb{R}$ 。设 $p(z) = p_1 + z, u_1(z) = u_{1,1} + u_{1,2}z, u_2(z) = u_{2,1} + u_{2,2}z$, 求解相应的半定规划 (2.2) 和其对偶问题, 我们可以求得最优值 $r_{sos}^* \approx 2.000569$ 和一个近似 GCD 多项式

$$p(z) \approx z - 14686.677911.$$

求解相应的半定规划 (2.7) 和其对偶问题, 其中目标有理函数为

$$\frac{f(X)}{g(X)} = \frac{(p_1^2 - 2p_1 + 1)^2 + (p_1^2 + 2p_1 + 2)^2}{1 + p_1^2 + p_1^4} = \frac{12p_1^2 + 4p_1 + 3}{1 + p_1^2 + p_1^4} + 2,$$

我们可以求得最优值为 $r_{sos}^* \approx 2.000000$, 但是求不出最优点。实际上全局最小值 $r^* = 2$ 并且

$$f(X) - r^*g(X) = 12\left(p_1 + \frac{1}{6}\right)^2 + \frac{8}{3}$$

是平方和但是没有全局最优点, 所以 r^* 只是个下确界。

2.2.3 带限制条件的多项式最小化问题

如文章 [25, 22, 23] 中所示, 计算多个多项式的近似 GCD 问题也可以表示成如下形式

$$\left. \begin{array}{l} \min_{\Delta c} \quad \|\Delta c\|_2^2 \\ s.t. \quad S_k(c + \Delta c)x = 0, \exists x \neq 0. \end{array} \right\} \quad (2.9)$$

在这里 c 表示多项式 f_1, \dots, f_s 的系数组成的向量, Δc 表示多项式的系数扰动向量, 矩阵 $S_k(c + \Delta c)$ 为多个多项式的一般化 Sylvester 矩阵 [22]。这个最优化问题是一个带二次限制条件的二次最优化问题, 其中向量 $\Delta c, x$ 的长度分别为 $\sum_{i=1}^s \binom{t+d_i}{t}$ 和 $\sum_{i=1}^s \binom{t+d_i-k}{t}$ 。

类似于 [22, 23] 中的方法, 我们可以选取矩阵 S_k 的一列, 将其分解为矩阵 A 和向量 b 并且将问题重新表示为

$$\left. \begin{array}{l} \min_{\Delta c, x} \quad \|\Delta c\|_2^2 + \rho \|x\|_2^2 \\ s.t. \quad A(c + \Delta c)x = b(c + \Delta c). \end{array} \right\} \quad (2.10)$$

另两种不同的表示形式分别为

$$\left. \begin{array}{l} \min_{\Delta c, x} \quad \|\Delta c\|_2^2 \\ s.t. \quad S_k(c + \Delta c)x = 0, \\ \quad \quad \|x\|_2^2 = 1, \end{array} \right\} \quad (2.11)$$

与

$$\left. \begin{array}{l} \min_{\Delta c, x} \quad \|\Delta c\|_2^2 + \rho \|x\|_2^2 \\ s.t. \quad S_k(c + \Delta c)x = 0, \\ \quad \quad v^T x = 1, \end{array} \right\} \quad (2.12)$$

其中 ρ 表示一个很小的数并且 v 是一个随机向量。

下面利用 Lasserre 的 Moment 方法求解上述问题。将带限制条件的多项式最小化问题 (Polynomial Optimization Problem) 表示为

$$\left. \begin{array}{l} \min_{\xi \in \mathbb{R}^n} \quad \sum_{\alpha} f_{\alpha} \xi^{\alpha} \\ s.t. \quad h_1(\xi) \geq 0, \dots, h_l(\xi) \geq 0, \end{array} \right\} \quad (2.13)$$

然后转化为一个凸 LMI (Linear Matrix Inequality) 最优化问题 (即半定规划) 序列 [29]

$$\left. \begin{aligned} \inf_y \quad & \sum_{\alpha} f_{\alpha} y_{\alpha} \\ \text{s.t.} \quad & y_{0, \dots, 0} = 1, \\ & M_d(y) \succeq 0, \\ & M_{d-w_i}(h_i * y) \succeq 0, \quad 1 \leq i \leq l, \end{aligned} \right\} \quad (2.14)$$

其中 $w_i = \lceil \frac{\text{tdeg}(h_i)}{2} \rceil$, $1 \leq i \leq l$, 松弛阶数 $d \geq \max(\lceil \frac{\text{tdeg}(f(X))}{2} \rceil, w_1, \dots, w_l)$, 关于实向量 y 的 Moment 矩阵 $M_d(y)$ 和局部化矩阵 (localizing matrix) $M_{d-w_i}(h_i * y)$ 为实对称半正定矩阵, 定义见 [29]。

例 2.6. 给定两个多项式

$$f_1(z) = z^3 - 1, \quad f_2(z) = z^2 - 1.01$$

并且 $k = 1, F = \mathbb{R}, \rho = 10^{-6}$ 。采用最小化问题 (2.10) 的形式, 并选择 Sylvester 矩阵 S_1 的第一列作为向量 b , 其他列形成的子矩阵作为 A 。求解相应的一阶 (即 $d = 1$) 半定规划 (2.14) 可以得到最小值 $9.9673e - 6$, 相应的半定规划 (2.14) 中半正定矩阵 $M_d(y)$ 的行列数为 152。求解相应的二阶 (即 $d = 2$) 半定规划 (2.14) 可以得到最小值为 $2.0871e - 5$, 相应的半定规划 (2.14) 中半正定矩阵 $M_d(y)$ 的行列数为 6476, 此时可从计算结果中求出原问题的全局最优点, 说明得到了原问题的全局最小值。

对于最小化问题形式 (2.11), 求解相应的一阶和二阶半定规划得到的最小值分别为 0 和 $2.0852e - 5$ 。这里我们注意到, 对于齐次模型形式 (2.11) 的一阶半定规划, 一个可行解为 $y = [1, 0, \dots, 0, 1]^T$, 相应的最小值为 0。

如 Erich Kaltofen 所指出的那样, 如果想通过求解问题形式 (2.10) 来得到最小化问题 (2.9) 的解, 那么必须尝试向量 b 的所有可能的选择。这是非常浪费时间的, 因此我们建议使用问题形式 (2.12)。对于最小化问题形式 (2.12), 相应的一阶和二阶半定规划的计算结果随其中的随机向量 v 的选取而稍有些不同, 对于当前例子计算得到的最小值大约数量级分别为 10^{-6} 和 10^{-5} 。

试验显示, 通过一阶半定规划的求解, 我们可以得到和原问题全局最优解相关的一些有用信息。虽然我们可通过求解高阶的半定规划得到原问题的全局最优解, 但是相应的半正定矩阵的大小会增加很快, 计算起来更困难。

2.3 最小化问题中的稀疏性

在这一节里，我们通过探索多项式近似 GCD 计算问题转化成的最小化问题的特殊结构，研究怎样降低相应的半定规划的大小规模。从例 2.1 和例 2.2 可以看出，相应有理函数最小化问题的分子和分母一般是稠密并且无特殊结构的，因此接下来我们只探索多项式最小化问题得到的半定规划 (2.2) 中的稀疏性。问题 (2.9) 也可以应用类似的方法。

2.3.1 Newton 多面体稀疏性

在 [47, 42, 28, 60] 中研究和介绍了通过探索多项式平方和展开中的稀疏性来减少平方和规划 (SOS programming) 中多余单项式的算法，已经有的研究结果说明只有 Newton 多面体中的部分单项式是必需的，但是实际计算大问题的稀疏性十分耗时。近似 GCD 问题 (2.1) 的稀疏结构可由下面的定理和推论推导出来而并不需要复杂计算。

对于任意多项式 $p(X) = \sum_{\alpha} p_{\alpha} X^{\alpha}$ ，记 $\text{supp}(p) = \{\alpha | p_{\alpha} \neq 0\}$ 的凸包为 $C(p)$ (Newton polytope)。下面用符号 $H(\cdot)$ 表示任意次数集合的凸包。

定理 2.1. [47] 对于任意多项式 p ，成立 $C(p^2) = 2C(p)$ ；对于任意半正定 (PSD) 多项式 f 和 g ，成立 $C(f) \subseteq C(f+g)$ ；如果 $f = \sum g_j^2$ ，则 $C(g_j) \subseteq \frac{1}{2}C(f)$ 。

推论 2.2. 对于任意半正定多项式 f 和 g ，成立 $C(f+g) = H(\text{supp}(f) \cup \text{supp}(g))$ ；如果 $f = \sum g_j^2$ ，则 $C(f) = 2H(\bigcup \text{supp}(g_j))$ 。

证明. 由多项式的加法可以知道 $\text{supp}(f+g) \subseteq \text{supp}(f) \cup \text{supp}(g)$ 。 f 和 g 都是半正定多项式，根据定理 2.1 $\text{supp}(f) \cup \text{supp}(g) \subseteq C(f) \cup C(g) \subseteq C(f+g)$ 。从

$$C(f+g) = H(\text{supp}(f+g)) \subseteq H(\text{supp}(f) \cup \text{supp}(g)) \subseteq C(f+g)$$

可以看出 $C(f+g) = H(\text{supp}(f) \cup \text{supp}(g))$ 。

如果 $f = \sum g_j^2$ ，根据定理 2.1 $C(g_j^2) = 2C(g_j)$ ，加上前面证明可以得到 $C(f) = H(\bigcup \text{supp}(g_j^2)) = H(\bigcup C(g_j^2)) = 2H(\bigcup C(g_j)) = 2H(\bigcup \text{supp}(g_j))$ 。□

近似 GCD 问题的多项式形式的半定规划 (2.2) 中的平方和松弛 (SOS relaxation) 条件可以写作

$$f(X) - r = m_d(X)^T W m_d(X) = \sum_j v_j(X)^2.$$

设 X^σ 为 $v_j(X)$ 中出现的任一单项式, 则由定理 2.1 和推论 2.2 可知

$$\sigma \in \frac{1}{2}\mathbb{C}(f(X) - r) = \mathbb{H}(O \cup \left(\bigcup_{i=1, |\alpha| \leq d_i}^s \text{supp}(f_{i,\alpha} - \sum_{\beta+\gamma=\alpha} p_\beta u_{i,\gamma}) \right)),$$

其中 O 表示原点。当某个待定系数 p_β 中包含非零常数项时, 可以知道出现在 $f_{i,\alpha} - \sum_{\beta+\gamma=\alpha} p_\beta u_{i,\gamma}$, $1 \leq i \leq s$, $|\alpha| \leq d_i$ 中的所有单项式为

$$1, p_1 u_{1,1}, \dots, p_1 u_{s,n(u_s)}, \dots, p_{n(p)} u_{1,1}, \dots, p_{n(p)} u_{s,n(u_s)}, u_{1,1}, \dots, u_{s,n(u_s)}, \quad (2.15)$$

此时可以设 $p_{n(p)+1} = 1$ 以及 $n_1(p) = n(p) + 1$; 否则所有单项式为

$$1, p_1 u_{1,1}, \dots, p_1 u_{s,n(u_s)}, \dots, p_{n(p)} u_{1,1}, \dots, p_{n(p)} u_{s,n(u_s)}, \quad (2.16)$$

这时设 $n_1(p) = n(p)$ 。次数 σ 在这些单项式的次数集合形成的凸包里, 由凸包的性质可知, 存在实数 $\lambda_{j,i,k} \geq 0$, $1 \leq j \leq n_1(p)$, $1 \leq i \leq s$, $1 \leq k \leq n(u_i)$ 满足 $\sum_{j,i,k} \lambda_{j,i,k} \leq 1$ 并且

$$X^\sigma = \prod_{j,i,k} (p_j u_{i,k})^{\lambda_{j,i,k}} = \prod_j p_j^{e_j} \prod_{i,k} u_{i,k}^{e_{i,k}}.$$

因为 $e_j, e_{i,k}$ 都是非负整数并且 $\sum_j e_j = \sum_{i,k} e_{i,k} = \sum_{j,i,k} \lambda_{j,i,k} \leq 1$, 所以单项式 X^σ 或者是 1, 或者存在某个 j, i, k 使其等于 $p_j u_{i,k}$, 这说明在近似 GCD 问题的多项式形式的半定规划 (2.2) 中只需上面那些单项式。最后得到近似 GCD 问题 (2.1) 的稀疏形式的半定规划

$$\left. \begin{aligned} r_{\text{sos1}}^* &:= \sup_{r \in \mathbb{R}, W} r \\ \text{s.t. } & f(X) - r = m_{\mathcal{G}}(X)^T W m_{\mathcal{G}}(X), \\ & W \succeq 0, \end{aligned} \right\} \quad (2.17)$$

单项式向量 $m_{\mathcal{G}}(X) = (1, p_1 u_{1,1}, \dots, p_1 u_{s,n(u_s)}, \dots, p_{n_1(p)} u_{1,1}, \dots, p_{n_1(p)} u_{s,n(u_s)})^T$ 。设 $n(u) = \sum_{i=1}^s n(u_i)$, 则实对称半正定矩阵 W 的行列数为 $1 + n_1(p)n(u)$ 并且半定规划展开后有 $1 + n_1(p)n(u) + \binom{n_1(p)+1}{2} \binom{n(u)+1}{2}$ 个等式限制条件。

2.3.2 稀疏情形下的全局最优解求解

多项式稀疏形式的半定规划 (2.17) 的对偶半定规划为

$$\left. \begin{array}{l} \inf_y \quad \sum_{\alpha} f_{\alpha} y_{\alpha} \\ s.t. \quad y_{0, \dots, 0} = 1, \\ \quad \quad M_{\mathcal{G}}(y) \succeq 0, \end{array} \right\} \quad (2.18)$$

其中实对称半正定 Moment 矩阵 $M_{\mathcal{G}}(y) := (y_{\alpha+\beta})_{\alpha, \beta \in \mathcal{G}}$ 的行和列对应于单项式向量 $m_{\mathcal{G}}(X)$ (\mathcal{G} 表示其中的单项式次数集合)。

将求解上面半定规划得到的最优 Moment 矩阵写成分块矩阵

$$M_{\mathcal{G}}(y^*) = \begin{bmatrix} 1 & \gamma_1^T \\ \gamma_1 & M_1 \end{bmatrix}.$$

设 $M_1 = VV^T$ 是计算得到的一个 Cholesky 分解并且矩阵 V 有 $c = \text{rank}(M_1)$ 列。对于任意满足 $V^T \gamma = 0$ 的向量 γ , 由 $\gamma^T [-\gamma_1, I] M_{\mathcal{G}}(y^*) [-\gamma_1, I]^T \gamma = -(\gamma_1^T \gamma)^2 \geq 0$ 可知 $\gamma_1^T \gamma = 0$, 所以存在向量 γ_2 使得 $\gamma_1 = V \gamma_2$, 由此我们得到分解

$$M_{\mathcal{G}}(y^*) = \begin{bmatrix} \gamma_2^T \\ V \end{bmatrix} \begin{bmatrix} \gamma_2 & V^T \end{bmatrix} + \begin{bmatrix} 1 - \gamma_2^T \gamma_2 & 0 \\ 0 & 0 \end{bmatrix}.$$

因为 V 列满秩, 令 $\gamma = [1, -\gamma_2^T (V^T V)^{-1} V^T]^T$ 可知 $1 - \gamma_2^T \gamma_2 = \gamma^T M_{\mathcal{G}}(y^*) \gamma \geq 0$ 。如果 $\text{rank}(M_{\mathcal{G}}(y^*)) > c$, 那么 $1 - \gamma_2^T \gamma_2 > 0$, 分解后的两个矩阵分别除以各自最左上角元素正规化后也是 (2.18) 的最优 Moment 矩阵, 由此 $y = [1, 0, \dots, 0]^T$ 是一个最优解并且 $X^* = 0$ 是使其取得全局最小值的原问题的一个全局最优点; 如果 $\text{rank}(M_{\mathcal{G}}(y^*)) = c$, 那么 $\gamma_2^T \gamma_2 = 1$, 对于近似 GCD 问题 (2.1) 一般只可能为这种情形。

如果 $c = 1$, 我们可以记 $V = (v_{1,1}, \dots, v_{1,n(u)}, \dots, v_{n_1(p),1}, \dots, v_{n_1(p),n(u)})^T$ 并且将其中的元素重新组合成一个矩阵 $B = (v_{i,j})_{n_1(p) \times n(u)}$ 。根据上面稀疏 Moment 矩阵定义中的结构和 $M_1 = VV^T$ 可以知道 $v_{i_1, j_1} v_{i_2, j_2} = v_{i_1, j_2} v_{i_2, j_1}$ 对于任意 $1 \leq i_1, i_2 \leq n_1(p), 1 \leq j_1, j_2 \leq n(u)$ 成立, 也即矩阵 B 的任意 2×2 子矩阵的行列式为 0, 又因为 V 是非零向量所以 $\text{rank}(B) = 1$ 。此时我们可以知道得到了全局最小值并且通过分解 $B/\gamma_2 = (p_1, \dots, p_{n_1(p)})^T (u_{1,1}, \dots, u_{s,n(u_s)})$ 可以得到一个全局最优点。

例 2.7. 给定两个多项式

$$f_1(z) = z^3 - z, f_2(z) = 3z^2 - 1$$

并且 $k = 1, F = \mathbb{R}$ 。求解相应的半定规划 (2.17) 和其对偶问题 (2.18)，其中单项式向量

$$m_G(X) = [1, p_1 u_{1,1}, p_1 u_{1,2}, p_1 u_{1,3}, p_1 u_{2,1}, p_1 u_{2,2}, u_{1,1}, u_{1,2}, u_{1,3}, u_{2,1}, u_{2,2}]^T,$$

我们可以得到最优值 $r_{\text{sos1}}^* \approx 0.0991769059$ 以及 $\text{rank}(M_G(y^*)) = \text{rank}(M_1) = 2$ 。通过奇异值分解 (SVD) 我们可以计算得到 γ_2 和 $V = [V_1, V_2]^T$ 。因为 $\text{rank}(V_2) = 2$ ，所以我们可以将 $\tilde{V} = [V_2, V_1, \gamma_2]^T$ 列消去成 U 并求解相应的共同特征值问题得到两个解中 p_1 的值，对应的两个近似 GCD 为 $z - 0.5878795$ 和 $z + 0.5878795$ ，相应的余因式为

$$\begin{aligned} u_1 &\approx 1.0518891z^2 + 0.7066490z - 0.4344338, & u_2 &\approx 2.9913164z + 1.7437641, \\ u_1 &\approx 1.0518891z^2 - 0.7066490z - 0.4344338, & u_2 &\approx 2.9913164z - 1.7437641. \end{aligned}$$

应用 Gauss-Newton 迭代精化上面的数值结果，我们得到

$$f(X^*(1)) \approx 0.0991769059, f(X^*(2)) \approx 0.0991769059,$$

由于 $f(X^*(1)) = f(X^*(2)) \approx r_{\text{sos1}}^*$ 可知得到了全局最优解。

2.3.3 关联结构稀疏性

在近似 GCD 问题的多项式最小化形式的半定规划 (2.2) 里

$$f(X) = \sum_{i=1}^s \|f_i - p \cdot u_i\|_2^2,$$

由此我们可以定义关联变量子集

$$X_{\Delta_i} = \{p_1, \dots, p_{n(p)}\} \cup \{u_{i,1}, \dots, u_{i,n(u_i)}\}.$$

可以看出这些变量子集 $X_{\Delta_1}, \dots, X_{\Delta_s}$ 之间满足如下的运行相交性质：

对于 $k = 1, \dots, s-1$

$$X_{\Delta_{k+1}} \cap \bigcup_{j=1}^k X_{\Delta_j} \subseteq X_{\Delta_i}, \exists 1 \leq i \leq k,$$

因此我们可以应用 [60, 30, 38] 中的稀疏平方和松弛 (SOS relaxation) 的方法, 然后得到如下的关联结构稀疏形式的半定规划

$$\left. \begin{aligned} r_{sos2}^* &:= \sup_{r \in \mathbb{R}, W_1, \dots, W_s} r \\ \text{s.t. } f(X) - r &= \sum_{i=1}^s m(X_{\Delta_i})^T W_i m(X_{\Delta_i}), \\ W_i &\succeq 0, 1 \leq i \leq s, \end{aligned} \right\} \quad (2.19)$$

其中 $m(X_{\Delta_i})$ 为所有全次数小于等于 2 的单项式组成的列向量, 实对称半正定矩阵 W_i 的行列数为 $\binom{n(p)+n(u_i)+2}{2}$ 。

同时应用 Newton 多面体稀疏性和关联结构稀疏性, 我们可以得到如下的稀疏形式的半定规划

$$\left. \begin{aligned} r_{sos3}^* &:= \sup_{r \in \mathbb{R}, W_1, \dots, W_s} r \\ \text{s.t. } f(X) - r &= \sum_{i=1}^s m_{\mathcal{G}_i}(X)^T W_i m_{\mathcal{G}_i}(X), \\ W_i &\succeq 0, 1 \leq i \leq s, \end{aligned} \right\} \quad (2.20)$$

其中 $m_{\mathcal{G}_i}(X)$ 为单项式 1 和 $p_j u_{i,k}$, $1 \leq j \leq n_1(p)$, $1 \leq k \leq n(u_i)$ 组成的列向量, 实对称半正定矩阵 W_i 的行列数为 $1 + n_1(p)n(u_i)$ 。

2.3.4 不同稀疏策略的比较

下面比较原多项式最小化问题 (2.1) 和半定规划 (2.2), 以及前面三种稀疏形式的半定规划 (2.17),(2.19),(2.20)。它们的最优值之间有如下关系

$$r^* \geq r_{sos}^* = r_{sos1}^* \geq r_{sos2}^* \geq r_{sos3}^*.$$

三种稀疏形式的半定规划中所有半正定矩阵的元素个数和分别为

$$m_1 = (1 + n_1(p)n(u))^2, m_2 = \sum_{i=1}^s \binom{n(p)+n(u_i)+2}{2}^2, m_3 = \sum_{i=1}^s (1 + n_1(p)n(u_i))^2,$$

它们之间有如下关系

$$s \cdot m_2 \geq s \cdot m_3 = s \sum_{i=1}^s (1 + n_1(p)n(u_i))^2 \geq (s + n_1(p)n(u))^2 \geq m_1 \geq m_3.$$

表 2.1: 不同稀疏策略之间的对比试验结果

f_1	$z(z+1)^2$	$(z+1)^2$	$z_1^2 + 2z_1z_2 + z_2^2 - 1$
f_2	$(z-1)(z+1)^2 + 0.1$	$z^2 + 2z + 1.01$	$z_1^2 + z_1z_2 - z_2 - 1.01$
k	2	1	1
r_{sos}^*	9.3876e-4	3.3167e-5	3.8931e-5
size	785	442	3026
r_{sos1}^*	9.3876e-4	3.3167e-5	3.8931e-5
size	170	82	362
r_{sos2}^*	4.2616e-7	3.3167e-5	3.6525e-6
size	451	201	1569
r_{sos3}^*	1.2123e-10	3.3167e-5	3.6502e-6
size	99	51	201

表 2.1 中显示了对三对多项式 f_1 和 f_2 的近似 GCD 问题的四种不同稀疏策略的半定规划 (2.2),(2.17),(2.19),(2.20) 的计算结果。可以看出第一和第三种稀疏形式的半定规划的规模相对非常小, 但第三种稀疏形式的半定规划的计算结果一般只是原问题的下界。

2.4 具体实现和例子

我在 Matlab 中使用半定规划软件包 SOSTOOLS [46]、YALMIP [34] 以及 SeDuMi [56] 中的函数和算法实现了前面描述的方法, 并且在 Maple 中使用 Gauss-Newton 迭代来改进半定规划计算结果的精度。

在表 2.2 中, 我们对 [3] 中的例子应用多种不同的数值方法求解并比较它们的计算结果。其中第三到第五列分别为半定规划 (2.2),(2.7),(2.17) 的计算结果, 第六列为对半定规划的计算结果应用 Gauss-Newton 迭代精化后的结果, 最后一列为 [22] 中的 STLN 局部最优化方法的计算结果。

注 2. 在我们的试验里, Matlab 中的固定精度半定规划函数经常碰到数值问题并且计算结果的精度不高。从表中可以看出, 有时计算得到的下界 r_{sos}^* 甚至比相应的 STLN 方法得到的局部最小值还大, 因此我们需要使用 Gauss-Newton 迭代来精化得到的全局最优解。实际试验中只需要很少的迭代就可以非常快地得到精度很高的结果。

表 2.2: 文章 [3, Chin et al., 1998] 中例子的试验结果

d_i	k	polynomial	rational	poly. sparse	Newton	STLN
5,4	2	1.620473e-8	1.579375e-8	1.560388e-8	1.560294e-8	1.560294e-8
4,6	3	1.561803e-2	1.561770e-2	1.561754e-2	1.561754e-2	1.561754e-2
3,3	2	1.702596e-2	1.702596e-2	1.702596e-2	1.702596e-2	1.702596e-2
5,5	4	7.086761e-5	7.086331e-5	7.086312e-5	7.086311e-5	7.086311e-5
3,2,3	2	1.729192e-5	1.729175e-5	1.729175e-5	1.729175e-5	1.729175e-5

表 2.3: 随机生成例子的试验结果

n	d_i	k	rational or poly. sparse	Newton	STLN
1	65,65	1	7.85073312e-6	7.84895293e-6	7.84895293e-6
	20,20	1	8.77479920e-6	8.72559736e-6	8.72559736e-6
	19,19	2	6.90363904e-5	6.88055540e-5	6.88055540e-5
	15,16	3	5.40141468e-5	5.40041186e-5	5.40041186e-5
	15,15	4	2.03530157e-4	2.03408558e-4	2.03408558e-4
	14,14	5	1.61530926e-4	1.61402027e-4	1.61402027e-4
	13,14	6	3.20576318e-4	3.20568077e-4	3.20568077e-4
	13,14	7	1.01396122e-4	1.01208845e-4	1.01208845e-4
	13,13	8	2.71981668e-4	2.71825700e-4	2.71825699e-4
	10,10	5	1.08249380e-4	1.08207747e-4	1.08207747e-4
	6,4	3	1.13839852e-2	1.13839851e-2	1.13839851e-2
	3,3	2	1.32223417e-5	1.32185834e-5	1.32185834e-5
	3,2	2	5.07694667e-3	5.07694668e-3	5.07694668e-3
	2,2	1	1.04706956e-4	1.04706621e-4	1.04706621e-4
2	5,5	1	4.28360491e-4	4.28336831e-4	4.28336831e-4
	4,5	2	7.44701587e-4	7.44633647e-4	7.44633647e-4
	4,5	3	4.94579319e-6	4.94240926e-6	4.94240926e-6
	5,5	4	1.20576057e-5	1.20467080e-5	1.20467080e-5
	3,3	2	4.09496306e-6	4.09320783e-6	4.09320783e-6
	3,2	2	3.51277009e-4	3.51276829e-4	3.51276829e-4

表 2.3 是我们用和 [22] 中一样的方法生成的随机例子的试验结果, 其中第一个例子是使用半定规划 (2.7) 并且其他例子是使用半定规划 (2.17) 求解的。对于这些随机例子, 求得的 Moment 矩阵的秩都是 1 并且得到了全局最优解。

注 3. 在表 2.2 和表 2.3 中, 通过 STLN 方法 [22] 得到的计算结果近似等于求解半定规划和 Gauss-Newton 迭代的计算结果。但是正如例 2.4 中所显示的那样, 对于不同的初始值 STLN 方法可能会不收敛于全局最优解。而在这些例子中求解相应的半定规划得到的 Moment 矩阵的秩都是 1 并且保证计算结果是全局最优解。

一般求解半定规划得到的计算结果是原问题的下界。对于近似 GCD 问题以及一些其他问题, 我们在 [19] 中给出了一个通过有理化半定规划得到的数值平方和来精确验证下界的有效算法。

第三章 多项式近似因式分解问题

3.1 前言

设域 F 为实数域 \mathbb{R} 或复数域 \mathbb{C} , 对于多变元多项式 $q \in F[z_1, \dots, z_s]$, 计算最小的扰动使得扰动多项式可约的近似因式分解问题可以表示为

$$\left. \begin{aligned} r^* &:= \min_{\tilde{q}} \|q - \tilde{q}\|_2^2 \\ &s.t. \quad \tilde{q} \text{ 可约,} \end{aligned} \right\} \quad (3.1)$$

其中多项式 $\tilde{q} \in F[z_1, \dots, z_s]$ 的全次数 (total degree) 满足 $\text{tdeg}(\tilde{q}) \leq t = \text{tdeg}(q)$ 。已有的计算实或复系数多项式的最近可约多项式的有效算法可以参见 [7, 21] 和其中的参考文献。类似于第二章里的多项式近似最大公因式问题, 近似因式分解问题同样可以转化成多种不同形式的多项式或有理函数最小化问题。这里我们考虑应用平方和 (Sums Of Squares) [42, 44, 39] 和 Moment 方法 [29] 将多项式或有理函数最小化问题转化成稠密或稀疏形式的半定规划 (Semidefinite Programming) [37, 57, 62] 求解并得到全局最优解或下界 [18]。

3.2 固定因式次数的近似因式分解问题

给定整数 $1 \leq k < t$, 计算距离多项式 q 最近的有 k 次因式的多项式的近似因式分解问题可表示为

$$\min_{u_1, u_2} \|q - u_1 \cdot u_2\|_2^2 \quad (3.2)$$

其中因式 $u_1, u_2 \in F[z_1, \dots, z_s]$ 的全次数满足 $\text{tdeg}(u_1) = k, \text{tdeg}(u_2) = t - k$ 。如果要求解问题 (3.1) 并得到多项式 q 的不可约半径 $\sqrt{r^*}$ [20], 需要对所有的 $1 \leq k \leq \lfloor \frac{t}{2} \rfloor$ 求解问题 (3.2)。

问题 (3.2) 可看作多项式近似 GCD 问题 (2.1) 中只有一个多项式的情形, 使用待定系数法将其转化为多项式最小化问题 $\min_{\xi \in \mathbb{R}^n} f(\xi)$, 可知 $F = \mathbb{R}$ 时 $n = \binom{s+k}{s} + \binom{s+t-k}{s}$ 并且 $F = \mathbb{C}$ 时 $n = 2\binom{s+k}{s} + 2\binom{s+t-k}{s} - 1$ (见注 1)。同样地应用 [42, 29] 中的方法将该多项式最小化问题转化成半定规划求解, 其稀疏性和近似 GCD 问题也一样。

表 3.1: 多项式近似因式分解问题的试验结果

	s	t	$k, t - k$	rational	poly. sparse	Newton
f_1	2	2	1,1	6.84663283e-4	6.84663368e-4	6.84663291e-4
f_2	2	5	1,4	2.94779281e-1	2.94778174e-1	2.94778174e-1
			2,3		4.13702070e-4	4.13701810e-4
f_3	2	3	1,2	4.06628630e-2	4.06628630e-2	4.06628630e-2

记 $\mathbf{q}, \mathbf{u}_1, \mathbf{u}_2$ 分别为 q, u_1, u_2 的系数向量并且 $A = A(\mathbf{u}_1)$ 为相应的卷积矩阵, 同样类似于 (2.4) 将问题 (3.2) 写成矩阵向量表示的形式 $\min_{\mathbf{u}_1, \mathbf{u}_2} \|\mathbf{q} - A\mathbf{u}_2\|_2^2$ 并且类似于 (2.6) 将其转化为有理函数最小化问题

$$\min_{\mathbf{u}_1} (\mathbf{q}^* \mathbf{q} - \mathbf{q}^* A (A^* A)^{-1} A^* \mathbf{q}). \quad (3.3)$$

该有理函数形式也可以看作 [16] 中双变元情形的推广, 同样地可应用 [39] 中的平方和方法将其转化为半定规划求解。

例 3.1. 给定三个多项式

$$\begin{aligned} f_1 &= (z_1 + z_2 + 1)(z_1 - 2z_2 + 1) + 0.1z_1, \\ f_2 &= (z_1^2 + z_1z_2 + 2z_2 - 1)(z_1^3 + z_2^2z_1 - z_2 + 7) + 0.2z_1, \\ f_3 &= (z_1^2 + 3z_2^2 + 4z_1 + 1)(z_1 - 2z_2 - 1) + 0.1z_1^3 + 0.2z_2^2 + 0.3z_1z_2, \end{aligned}$$

并且 $F = \mathbb{R}$, 其中 f_2 是 [20] 中的第三个例子并且出自 [36]。表 3.1 为求解近似因式分解问题 (3.2) 转化成的有理函数形式的半定规划 (2.7) 和多项式稀疏形式的半定规划 (2.17) 的计算结果, 以及用 Gauss-Newton 迭代精化后的计算结果。同 [21] 中的 SVD+Gauss-Newton 算法相比较结果一致, 说明求得了全局最优解。对于 f_2 在 $k = 2$ 时, 问题对应的有理函数复杂的无法求得, 但使用多项式稀疏形式的半定规划 (2.17) 可以求解并且得到近似因式分解

$$\begin{aligned} u_1 &\approx -0.4995510020 + 0.9999999483z_2 + 0.01508424336z_1 - 0.001851829728z_2^2 \\ &\quad + 0.4993139380z_2z_1 + 0.4980546263z_1^2, \\ u_2 &\approx 14.01307538 - 1.975808855z_2 + 0.02696536291z_1 - 0.007358241803z_2^2 \\ &\quad - 0.01060870629z_2z_1 - 0.04118078726z_1^2 - 0.0008349554328z_2^3 \\ &\quad + 2.008251357z_2^2z_1 - 0.01747658780z_1^2z_2 + 2.022755708z_1^3. \end{aligned}$$

3.3 分解成多个因式的近似因式分解问题

在 [20, 7, 21] 中推广应用了 [52, 53, 6] 中判定多变元多项式不可约性的事实, 描述如下

定理 3.1. 非常数多变元多项式 $q \in \mathbb{C}[z_1, z_2, \dots, z_s]$ 的重次数记为 (d_1, d_2, \dots, d_s) , 即 $\deg_{z_i}(q) = d_i$. 若 $\gcd(q, \frac{\partial q}{\partial z_1}) = 1$, 则 q 在复数域 \mathbb{C} 上可约当且仅当存在不全为零的多项式 $p_1, p_2, \dots, p_s \in \mathbb{C}[z_1, z_2, \dots, z_s]$ 成立

$$\frac{\partial}{\partial z_i} \left(\frac{p_1}{q} \right) = \frac{\partial}{\partial z_1} \left(\frac{p_i}{q} \right), \quad i = 2, \dots, s,$$

其中多项式 p_1, p_2, \dots, p_s 的次数满足

$$\begin{aligned} \deg(p_1) &\leq (d_1 - 2, d_2, \dots, d_s), \\ \deg(p_i) &\leq (d_1, d_2, \dots, d_i - 1, \dots, d_s), \quad i = 2, \dots, s. \end{aligned}$$

将上面所有等式展开后得到一个关于多项式 p_1, p_2, \dots, p_s 的系数向量 \mathbf{x} 的齐次线性方程组 $R(q)\mathbf{x} = 0$, 其中矩阵 $R(q)$ 叫做 *Ruppert* 矩阵。如果 q 在复数域 \mathbb{C} 上可分解成 r 个不可约因式的乘积, 那么矩阵 $R(q)$ 的亏秩为 $r - 1$ (组合系数向量 \mathbf{x} 的空间维数)。

对于复数域 \mathbb{C} 上求解离多变元多项式 q 最近的至少可分解成 r 个因式乘积的多项式的近似因式分解问题, 我们利用以上事实可以将其表示为如下带限制条件的多项式最小化问题

$$\left. \begin{aligned} \min_{\Delta q, Q} \quad & \|\Delta q\|_2^2 \\ \text{s.t.} \quad & R(q + \Delta q)Q = 0, \\ & Q^H Q = I_{r-1}. \end{aligned} \right\} \quad (3.4)$$

类似于近似 GCD 情形 [22], 该问题的最优解不一定能够产生一个可因式分解的多项式, 因为最优解 $q + \Delta q$ 可能有更低的次数或者有一个重数大于 2 的因式。

问题 (3.4) 是一个带二次等式限制条件的二次多项式最优化问题。我们可以用基于 Lagrange 乘数法的 STLS 算法来求解, 也可以类似于多项式近似 GCD 问题, 应用文章 [29] 中的方法将其转化为半定规划(2.14) 求解。对比 SVD+Gauss-Newton 和 STLS 方法 [21], 用半定规划求得的结果被验证为问题

的下界（带一些浮点误差）。问题 (3.4) 的一阶的 Lasserre 松弛 (2.14) 的最优解总是 0，因此需要更高阶的松弛。类似于近似 GCD 问题，我们也可将近似因式分解问题 (3.1)（即 (3.4) 中 $r = 2$ 的情形）转化为如下随机问题

$$\left. \begin{array}{l} \min_{\Delta q, x} \quad \|\Delta q\|_2^2 + \rho \|x\|_2^2 \\ s.t. \quad R(q + \Delta q)x = 0, \\ \quad \quad v^T x = 1, \end{array} \right\} \quad (3.5)$$

其中 ρ 为一个很小的数并且 v 是一个随机向量。从该问题的一阶 Lasserre 松弛计算结果可以得到一些信息。类似于 [22]，我们也可以选择矩阵 R 的一列作为向量 b ，其他列作为矩阵 A ，并且将限制条件替换为 $Ax = b$ 。

第四章 多项式平方和 (SOS) 有理化精确验证方法

4.1 前言

在很多实际问题中需要得到问题精确的下界，而在一般多项式或有理函数最小化问题 (1.1) 的半定规划的求解中，因为计算的数值结果存在浮点数舍入误差并且全局最优解可能是代数数 [40]，所以计算结果只是近似的满足平方和等式 (1.2)。对于半定规划计算结果中的浮点精度问题，我们考虑引入精确的符号计算方法比如有理化方法使得等式 (1.2) 精确成立。因为全局最优解可能是代数数，所以我们将只是检验一个邻近的有理下界 $\tilde{r} \lesssim r, \tilde{r} \in \mathbb{Q}$ 。一般我们假设问题 (1.1) 中多项式的系数是精确表示的有理数或者可以转化为有理数的小数，实际上对于系数中存在有精确表示的非有理代数数的情形也是可行的（见注 5）。因为精确有理化方法对于初始输入的容错性很高，所以我们在半定规划求解中可以采取更大稀疏性和一些启发式方法而不用太关注返回的结果，甚至可以不用半定规划而直接用 Newton 迭代就能得到一个近似的数值平方和等式。同样不同于 Rump 和 Villard 的完全分析并且合法的数值方法（参见 [59] 和其中的参考文献），我们的范式允许没有严格理论保证的数值方法和低精度浮点数。

考虑一般多项式或有理函数最小化问题 (1.1) 的无限制条件情形

$$\min_{\xi \in \mathbb{R}^n} \frac{f(\xi)}{g(\xi)}, \quad (4.1)$$

通过平方和 (Sums Of Squares) 和 Moment 方法 [42, 29, 44, 17, 39] 将其转化成半定规划

$$\left. \begin{aligned} r^* &:= \sup_{r \in \mathbb{R}, W} r \\ s.t. \quad & f(X) - rg(X) = m_d(X)^T W m_d(X), \\ & W \succeq 0, \end{aligned} \right\} \quad (4.2)$$

其中 $m_d(X)$ 为所有全次数小于等于 $d = \lceil \frac{\max(\text{tdeg}(f), \text{tdeg}(g))}{2} \rceil$ 的单项式组成的列向量，实对称半正定矩阵 W 的行列数为 $\binom{n+d}{n}$ 并且半定规划展开后有 $\binom{n+2d}{n}$ 个等式限制条件。

在无限制条件情形，寻找有理平方和分解 (1.2) 的问题等价于寻找满足半定规划 (4.2) 的有理对称半正定 (PSD) 矩阵 W (见 (4.11))。受 Peyrl 和 Parillo 在 [45] 中的有理化投影方法启发，我们将求解半定规划 (4.2) 计算得到的数值矩阵 W 作为初始值，不同的是我们随后用 Newton 迭代方法来精化矩阵 W ，然后将 r^* 减小为一个有理下界 \tilde{r} ，将矩阵 W 转化为一个有理矩阵并且将其投影到如下仿射线性超平面上 (对比 (4.2) 中的限制条件)

$$\mathcal{X} = \{A \mid A^T = A, f(X) - \tilde{r}g(X) = m_d(X)^T \cdot A \cdot m_d(X)\}. \quad (4.3)$$

实际上投影等价于精确地求解一个有理最小二乘问题 (4.9)。记投影在 \mathcal{X} 上的矩阵为 \widetilde{W} ，如果 \widetilde{W} 是半正定的，那么可以得到精确的有理平方和等式并验证了下界 \tilde{r} ；如果 \widetilde{W} 不是半正定的，那么我们可以增加精度或进一步减小 \tilde{r} 并且重试。因为最优解 W 在一个邻域内保持半正定性质 [45, 命题 3.1]，所以使用足够多的位数总是可以得到一个有理半正定矩阵。通过探索半定规划 (4.2) 中的稀疏性 [47, 28, 43, 60, 30, 38, 32] 可以将其中的限制条件替换为

$$f(X) - rg(X) = m_G(X)^T W m_G(X), \quad W \succeq 0, \quad (4.4)$$

并且降低精确验证问题的大小规模 (见 2.3.1 和 4.4.2)。

我们对多项式近似最大公因式问题、多项式近似因式分解问题和 Siegfried Rump 的模型问题 [51, 50] 应用了上面的精确验证策略。我们的方法也可以用来产生多项式的精确有理平方和分解。在试验中，验证得到的下界十分接近于求得的上界。只需片刻的计算我们就验证了近似 GCD 问题 [22, 例 4.2] 的一个精确到小数点后 5 位的下界，这说明相应的病态 Sylvester 矩阵的结构是良好的。我们也只需很短的时间就验证了例子 [20, 例 3] 的不可约半径，并且求得了 [5] 中一个多项式 “Vor1” (4.13) 及它关于变量 u 的判别多项式的精确平方和分解，对这几个以前难以求解的例子甚至比已有的数值或符号算法都要好。对于 Rump 的模型问题 (4.14) 的最优值 μ_n ，我们精确验证到了 $n = 14$ 时的下界并通过半定规划和 Newton-Lagrange 迭代方法 [1] (见 1.2.3) 至少可以得到 $n = 63$ 时的上界。在 $n = 14$ 时我们计算得到 $1.62 \cdot 10^{11} < \frac{1}{\mu_{14}} < 3.12 \cdot 10^{11}$ ，同时 Mignotte 的下界 (4.16) [35] 为 $\frac{1}{\mu_n} \leq \binom{2n-2}{n-1}^2 = \binom{26}{13}^2 \approx 1.08 \cdot 10^{14}$ ，在实际计算 μ_{14} 的下界时精度受固定精度半定规划软件的限制。接下来我们将详细阐述怎样扩展 [45] 中的方法到有理平方和精确验证上，我们也探索了从一个和 W 相同秩的随机对称半正定矩阵开始的可能性。不用半定规划，我们成功地验证了 Rump 问题直到 $n = 10$ 的下界。

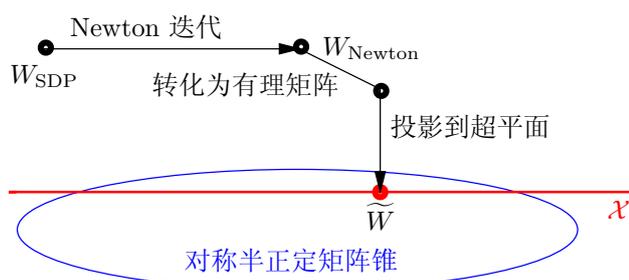


图 4.1: 平方和有理化过程

4.2 平方和的产生和有理化技术

半定规划 (4.2) 可以用软件包 SOSTOOLS [46]、YALMIP [34] 和 SeDuMi [56] 中的算法快速求解。但是因为它们都是固定精度软件 Matlab 中的软件包，所以我们只是得到了一个数值的半正定矩阵 W 和浮点数 r^* ，它们近似满足

$$f(X) - r^*g(X) \approx m_d(X)^T \cdot W \cdot m_d(X), \quad W \succeq 0, \quad (4.5)$$

这里 r^* 是 (4.1) 的近似下界。在一些实际应用比如 Rump 的模型问题 (4.14) 中，由于数值误差，计算得到的下界甚至可能比上界大（见表 4.1）。这些促使我们考虑怎样用精确线性代数工具来验证半定规划计算得到的下界。

我们说下界 \tilde{r} 被验证即存在精确半正定矩阵 \tilde{W} 满足如下条件

$$f(X) - \tilde{r}g(X) = m_d(X)^T \cdot \tilde{W} \cdot m_d(X), \quad \tilde{W} \succeq 0. \quad (4.6)$$

接下来，我们首先使用 Gauss-Newton 迭代来精化近似满足 (4.5) 的 r^* 和 W ，然后计算有理数 \tilde{r} 和满足 (4.6) 的精确有理对称半正定矩阵 \tilde{W} 。图 4.1 中显示了我们的平方和有理化方法的过程。

4.2.1 半定规划和 Newton 迭代

记 θ 为后向误差

$$\theta = \|f(X) - rg(X) - m_d(X)^T \cdot W \cdot m_d(X)\|,$$

其中浮点数 r 可以通过求解半定规划 (4.2) 或其他局部最优化方法 [8, 21] 计算得到，但为了产生一个令人满意的验证下界，从一个比较接近最优解的下界 r^* 开始很重要。

对于给定的 r^* , 近似的对称半正定矩阵 W 可以通过求解如下的半定规划得到

$$\left. \begin{array}{l} \inf_W \text{Trace}(W) \\ \text{s.t. } f(X) - r^*g(X) = m_d(X)^T W m_d(X), \\ W \succeq 0. \end{array} \right\} \quad (4.7)$$

这里我们使用矩阵 W 的迹 $\text{Trace}(W)$ 作为目标函数, 在无目标函数的问题转换成半定规划时一般使用这种技术。

我们将半正定矩阵 W 分解并且得到近似的平方和展开

$$f(X) - r^*g(X) \approx \sum_{i=1}^k \left(\sum_{\alpha} c_{i,\alpha} X^{\alpha} \right)^2 \in \mathbb{R}[X], \quad (4.8)$$

这里 k 为矩阵 W 的秩。由半定规划的对偶性和 Moment 理论可以知道矩阵 W 的亏秩一般对应于全局最优解的个数。在一些应用中, 如果已知全局最优解的个数, 那么 k 也就知道了。对于 Rump 的模型问题 (4.18), 矩阵 W 的亏秩在 n 为偶数时为 1 并且在 n 为奇数时为 2。给定一个公差, 我们可以通过对矩阵 W 的奇异值分解 (SVD) 来计算秩 k 。

我们对关于 $c_{i,\alpha}$ 的平方和形式的目标函数

$$\|f(X) - r^*g(X) - \sum_{i=1}^k \left(\sum_{\alpha} c_{i,\alpha} X^{\alpha} \right)^2\|_2^2$$

应用 Gauss-Newton 迭代计算 $\Delta c_{i,\alpha} X^{\alpha}$ 使其满足

$$f(X) - r^*g(X) = \sum_{i=1}^k \left(\sum_{\alpha} c_{i,\alpha} X^{\alpha} + \Delta c_{i,\alpha} X^{\alpha} \right)^2 + O\left(\sum_{i=1}^k \left(\sum_{\alpha} \Delta c_{i,\alpha} X^{\alpha} \right)^2 \right)$$

并将矩阵 W 更新为 $W + \Delta W$ 。当 θ 比一个给定的公差 τ 小的时候停止迭代。如果 θ 经过几步迭代后仍然比给定的公差 τ 大, 我们可以增加半定规划以及 Gauss-Newton 迭代计算中的精度或者使用更小的 r^* 并且重新尝试计算。

单项式向量 $m_d(X)$ 中单项式 X^{α} 的个数为 $\binom{n+d}{d}$ 并且相应的 Gauss-Newton 迭代的计算量非常大, 所以一般必须探索半定规划 (4.2), (4.7) 中的稀疏性并且使用 (4.4) 中的稀疏单项式向量 $m_G(X)$ 。幸运地, 对于很多由近似多项式计算产生的最优化问题, 稀疏性可以通过分析 Newton 多面体来发现 (参见 2.3.1), 在 4.4.2 我们显示了 Rump 的模型问题 (4.18) 中的稀疏性。

注 4. 通过指定一些限制条件比如秩、稀疏性, 我们可以随机地构造对称半正定矩阵 W , 但是如果相应的后向误差 θ 很大, 我们可能需要很多次的 Gauss-Newton 迭代来减少 θ 使其小于 τ .

4.2.2 平方和有理化算法

文章 [45] 中介绍了通过使用 Macaulay 2 软件包从一个有理系数非负多项式的数值平方和分解开始计算其精确的平方和分解的方法, 我们推广了其中的方法并且可以对多项式 $f(X) - \tilde{r}g(X)$ 构造一个精确多项式平方和分解, 这样就验证了 \tilde{r} 为有理函数最小化问题 (4.1) 的下界。

假设经过 Gauss-Newton 迭代精化后的矩阵 W 满足 $\|f(X) - r^*g(X) - m_d(X)^T \cdot W \cdot m_d(X)\| < \tau$ 。我们由 r^* 得到一个邻近的有理数 $\tilde{r} \lesssim r^*$, 然后将 W 转化成有理矩阵并将其正交投影到 (4.3) 中超平面 \mathcal{X} 上得到有理矩阵 \widetilde{W} 。投影等价于求解下面的最小二乘问题

$$\left. \begin{aligned} \min_{\widetilde{W}} \quad & \|W - \widetilde{W}\|_F^2 \\ \text{s.t.} \quad & f(X) - \tilde{r}g(X) = m_d(X)^T \widetilde{W} m_d(X), \end{aligned} \right\} \quad (4.9)$$

而它等价于求解一些更小的最小二乘问题

$$\left. \begin{aligned} \min_{\widetilde{W}} \quad & \sum_{\alpha} \sum_{\beta+\gamma=\alpha} (W_{\beta,\gamma} - \widetilde{W}_{\beta,\gamma})^2 \\ \text{s.t.} \quad & f_{\alpha} - \tilde{r}g_{\alpha} = \sum_{\beta+\gamma=\alpha} \widetilde{W}_{\beta,\gamma}. \end{aligned} \right\} \quad (4.10)$$

对所有 α 求解问题 (4.10) 得到有理矩阵 \widetilde{W} , 然后计算精确 L^TDL 分解 [11]

$$\left. \begin{aligned} f(X) - \tilde{r}g(X) &= m_d(X)^T \cdot \widetilde{W} \cdot m_d(X) \\ &= m_d(X)^T \cdot L^T \cdot D \cdot L \cdot m_d(X), \\ &= \sum_i D_{i,i} (L_i \cdot m_d(X))^2, \end{aligned} \right\} \quad (4.11)$$

其中 $D_{i,i}$ 为对角矩阵 D 的第 i 个对角元素并且 L_i 是 L 的第 i 行。可以看出 \widetilde{W} 的半正定性等价于 D 的所有对角元素都是非负的。如果 \widetilde{W} 不是半正定矩阵, 即矩阵 D 的一个对角元是负的, 我们可以减少 \tilde{r} 或者增加 Gauss-Newton 迭代的次数并重复前面的计算过程。在实际试验中, 我们通常选取 $\rho \in [0.1 \cdot \theta, 0.5 \cdot \theta]$ 并减少 r^* 为 $\tilde{r} = r^* - \rho$, 根据经验此时得到的矩阵 \widetilde{W} 一般是半正定矩阵。

注 5. 验证的一个关键性质是可以只用有理算术来计算矩阵 \widetilde{W} 的 L^TDL 分解。从 $f(X) - \tilde{r}g(X) = \sum_i (\sqrt{D_{i,i}} \cdot L_i \cdot m_d(X))^2$ 可以看出虽然得到的平方和分解是精确的，但其中却不一定是有理多项式。如果所有系数是有理数，那么必存在一个有理平方和 [14]，但在我们的验证中并不一定需要具体的分解。如果 f 和 g 的系数是在一个精确（不是必须完全的）实代数扩域 $K = \mathbb{Q}[\eta]/(\varphi(\eta))$ 上，其中 $\varphi(\eta) \in \mathbb{Q}[\eta]$ 并且符号 η 表示 φ 的一个指定实根，验证可通过 K 上的算术运算以同样的方式精确地检验。注意 \tilde{r} 仍然在有理数域 \mathbb{Q} 中选取。

算法：下界检验

输入：▶ $f(X_1, \dots, X_n), g(X_1, \dots, X_n) \in \mathbb{Q}[X_1, \dots, X_n]$ ：目标多变元有理函数的分子和分母。

- ▶ r^* （可选）：最小化问题的近似最小值。
- ▶ $\tau \in \mathbb{R}_{>0}$ ：给定公差。

输出：▶ \tilde{r} ：待验证下界。

1. Gauss-Newton 迭代精化

(a) 得到一个近似半正定矩阵 W 或平方和分解。

情形 1 用半定规划计算 W ：

- A. 如果给定 r^* ，用半定规划 (4.7) 计算 W 使其近似满足 (4.5)；
否则，用半定规划 (4.2) 计算 r^* 和 W 使其近似满足 (4.5)。
- B. 计算 W 的数值秩 k 并探索平方和中的稀疏结构。

情形 2 不用半定规划计算 W ：

随机构造满足秩条件和给定稀疏结构的对称半正定矩阵 W 。

(b) 应用 Gauss-Newton 迭代方法精化 (4.8) 并且计算 θ 。

(c) 如果 $\theta < \tau$ ，那么得到精化后的矩阵 W ；
否则，减小 r^* 并且回到步骤 1(a)A。

2. 计算精确平方和分解

(a) 将 r^* 减少为有理数 \tilde{r} 并且将 W 转化为有理矩阵。

(b) 通过求解 (4.9) 计算得到有理矩阵 \widetilde{W} 。

(c) 检查矩阵 \widetilde{W} 是否半正定。如果是，返回 \tilde{r} ；否则选择 $\rho \in [0.1 \cdot \theta, 0.5 \cdot \theta]$ ，
令 $\tilde{r} = r^* - \rho$ 并返回步骤 2b。

注 6. 我们的思想是, 对于尽可能接近 r^* 的有理数 \tilde{r} , 通过有理化投影方法尝试获得半正定的有理对称矩阵 \widetilde{W} 并且验证 \tilde{r} 为下界。我们在应用 Gauss-Newton 迭代精化 W 时采用 r^* (或稍小一些的值) 而在投影时使用甚至更小的 \tilde{r} , 因为在迭代精化时直接使用验证目标 \tilde{r} 容易使求得的 W 距离半正定矩阵锥的边界太近而有理化投影验证不易成功。

4.3 应用和例子

4.3.1 多项式近似最大公因式问题

多项式近似最大公因式问题 (2.1) 可以通过多种不同方式转化成多项式或有理函数最小化问题, 应用平方和方法并且探索其中的稀疏性可以将其转化成半定规划求解, 具体介绍参见第二章或者 [31, 32] 以及其中的参考文献。我们也可以从 STLN [22] 等局部算法得到近似 GCD 问题的局部最小值 r^* , 然后应用我们的精确下界验证算法。实际试验中, 我们可以有效地验证较好的下界 \tilde{r} 。

例 4.1 (例 4.2 [22]). 给定两个多项式

$$1000z^{10} + z^3 - 1, z^2 - \frac{1}{100}.$$

对于它们的近似 GCD 问题, 我们用 STLN 方法计算得到的局部最小值为

$$r^* = 0.0421579164. \quad (4.12)$$

我们用半定规划 [32] 也得到了同样的值。然后我们将 r^* 减去 4×10^{-8} 得到 $r^* = 0.0421578636$ 并且尝试验证下界。将近似 GCD 问题转化为有理函数最小化问题, 有理函数的分子和分母 $f(X), g(X) \in \mathbb{Q}[X]$ 可以从 [27, 15, 32] 中的形式得到, 参见 2.2.2。

我们通过求解半定规划 (4.2) 计算得到矩阵 W 并且其中 $\dim(m_d(X)) = 13$, 然后求得

$$\begin{aligned} \theta &= \|f(X) - r^*g(X) - m_d(X)^T \cdot W \cdot m_d(X)\| \\ &= 1.9430e-7. \end{aligned}$$

情形 1: 不使用 Gauss-Newton 迭代, 我们减少 r^* 到有理下界

$$\tilde{r}_1 = 1414583 \cdot 2^{-27} \approx 0.0421578586.$$

我们的 SDP-SOS 算法用了 0.02 秒¹ 求解 (4.9) 并且得到了有理矩阵 \widetilde{W} , 其中在 Maple 11 下精确计算求解时 Digits:=20。通过 L^TDL 分解我们发现 \widetilde{W} 是一个半正定矩阵

$$f(X) - \tilde{r}_1 g(X) = m_d(X)^T \cdot \widetilde{W} \cdot m_d(X) \geq 0,$$

因此 \tilde{r}_1 被验证为问题的下界。

情形 2: 应用 Gauss-Newton 迭代, 误差减少到

$$\begin{aligned} \theta &= \|f(X) - r^* g(X) - m_d(X)^T \cdot W \cdot m_d(X)\| \\ &= 1.8140e-13. \end{aligned}$$

我们减少 r^* 到有理下界

$$\tilde{r}_2 = 45266661 \cdot 2^{-30} \approx 0.0421578633.$$

我们的 SDP-SOS 算法用了 47.6 秒得到了有理半正定矩阵 \widetilde{W} 并且 \tilde{r}_2 也被验证为是问题的下界。

比较两种情形可知 \tilde{r}_2 比 \tilde{r}_1 更好些。因此我们将 $\tilde{r} = \tilde{r}_2$ 作为该问题的验证下界, 并且知道 STLN 方法 [22] 计算得到的局部最小值为近似全局最小值。

注意在 [22] 中我们已经通过区间算术最小化 [63] 验证了值 (4.12) 的全局最优性。最小值的验证很重要, 因为例 4.1 的 Sylvester 矩阵是非常病态的并且与奇异性的结构距离很大, 这是在我们之前已经研究了很多的一个现象 [2, 33]。

4.3.2 多项式近似因式分解问题

类似于多项式近似 GCD 问题, 近似因式分解问题 (3.2) 也可以转化成多项式或有理函数最小化问题并应用半定规划求解, 具体介绍参见第三章或者 [18] 以及其中的参考文献。在 [18] 中指出, 如果不探索半定规划 (4.2) 中的稀疏性, 甚至很难验证 [20] 中的例 3 (出自 [36, 例 1]) 的下界, 而关于稀疏性的探索可以参见 2.3 [32]。实际试验中, 我们可以有效的验证近似因式分解问题的下界 \tilde{r} , 也即不可约半径。

¹ 所有时间是在一台带 9GB 内存的 4 CPU (3GHz Xeon) MacPro 电脑和 Linux 2.6.22-14 (Ubuntu) 系统下计算得到的。

例 4.2 (例 3 [20]). 给定多项式

$$(z_1^2 + z_2 z_1 + 2z_2 - 1)(z_1^3 + z_2^2 z_1 - z_2 + 7) + \frac{1}{5} z_1,$$

我们将验证该多项式的近似因式分解问题的下界。在因式次数 $k = 1, 2$ 时, 求解稀疏形式的半定规划 (2.17) 计算得到的全局最小值 r^* 分别是 0.2947781736518 和 0.000413702070。在 [21, Table 1, Example 1] 中给出的上界是 0.00041370181014226, 它比半定规划的计算结果小。相应的目标函数 $f(X) \in \mathbb{Q}[X]$ 可以从 (3.2) (也可见 [32]) 中得到。

在 $k = 1$ 时, 我们可通过求解稀疏形式的半定规划 (2.17) 计算得到矩阵 W 并且 $\dim(m_G(X)) = 46$, 然后得到

$$\theta = \|f(X) - r^* - m_G(X)^T \cdot W \cdot m_G(X)\| = 1.06591917\text{e-}11.$$

不使用 Gauss-Newton 迭代, 我们减少 r^* 到有理数

$$\tilde{r} = 633031307 \cdot 2^{-31} \approx 0.2947781733237$$

并且在 Maple 11 中精确计算求解 (4.9) 得到有理矩阵 \widetilde{W} 。通过 L^TDL 分解我们发现 \widetilde{W} 是一个半正定矩阵

$$f(X) - \tilde{r}g(X) = m_G(X)^T \cdot \widetilde{W} \cdot m_G(X) \geq 0.$$

因此 \tilde{r} 被验证为问题的下界, 并且求解稀疏形式得半定规划 (2.17) 计算得到的局部最小值是近似全局最优解。算法验证下界用了 0.56 秒。

在 $k = 2$ 时, 我们可通过求解稀疏形式的半定规划 (2.17) 计算得到矩阵 W 并且 $\dim(m_G(X)) = 61$, 然后得到

$$\theta = \|f(X) - r^* - m_G(X)^T \cdot W \cdot m_G(X)\| = 1.04543742\text{e-}11.$$

不使用 Gauss-Newton 迭代, 我们减少 r^* 到有理数

$$\tilde{r} = 111052 \cdot 2^{-28} \approx 0.000413700938$$

并且在 Maple 11 中精确计算求解 (4.9) 得到有理矩阵 \widetilde{W} 。通过 L^TDL 分解我们发现 \widetilde{W} 是一个半正定矩阵

$$f(X) - \tilde{r}g(X) = m_G(X)^T \cdot \widetilde{W} \cdot m_G(X) \geq 0.$$

因此 \tilde{r} 被验证为问题的下界, 使用近似因式分解方法计算得到的局部最小值是近似全局最优值。算法验证下界用了 2.56 秒。就平方和分解中平方的数目来说这是我们最大的验证, 其中有理数的分子和分母最大有 1132 位。

http://www4.ncsu.edu/~kaltofen/software/certif/factor_SOS.txt.

4.3.3 多项式精确平方和分解

任意给定一个有理系数多项式, 通过对它的最小化问题应用平方和松弛方法转化成一个半定规划求解, 我们可以得到它的一个下界以及相应的数值平方和分解。应用我们的精确下界验证方法可以得到一个精确的有理平方和分解。通过探索多项式中的 Newton 多面体稀疏性 [47, 28] 可以大大减少相应的半正定矩阵的大小, 试验显示我们的方法十分有效。

例 4.3. 考虑文章 [5] 中的非负多项式 “Vor1” (也可见 Safey El Din 在 ISSAC 2008 会议中的文章)

$$\begin{aligned}
& 16a^2(\alpha^2 + 1 + \beta^2)u^4 + 16a(-\alpha\beta a^2 + ax\alpha + 2a\alpha^2 + 2a + 2a\beta^2 + ay\beta \\
& - \alpha\beta)u^3 + ((24a^2 + 4a^4)\alpha^2 + (-24\beta a^3 - 24a\beta - 8ya^3 + 24xa^2 - 8ay)\alpha \\
& + 24a^2\beta^2 + 4\beta^2 - 8\beta xa^3 + 4y^2a^2 + 24y\beta a^2 - 8ax\beta + 16a^2 + 4x^2a^2)u^2 \\
& + (-4\alpha a^3 + 4ya^2 - 4ax - 8a\alpha + 8\beta a^2 + 4\beta)(\beta - a\alpha + y - ax)u \\
& + (a^2 + 1)(\beta - a\alpha + y - ax)^2 \quad (4.13)
\end{aligned}$$

我们要验证该多项式的下界。在 Matlab 中用 YALMIP [34] 软件包来计算对应的半定规划并探索相应的 Newton 多面体稀疏性。我们可以得到 $\dim(m_G(X)) = 19$ 并且矩阵 W 的秩为 3。应用 Gauss-Newton 迭代和有理正交投影, 我们验证了 0 是下界并且该多项式可写成 3 个多项式的平方和, 即

$$\begin{aligned}
& 16(au + au^2)^2 + (ay + a\beta + 2auy + 4a\beta u - a^2x - a^2\alpha + 4a\beta u^2 - 2a^2\alpha u)^2 \\
& + (y + \beta + 2\beta u - ax - a\alpha - 2aux - 4a\alpha u - 4a\alpha u^2)^2
\end{aligned}$$

我们的算法 (YALMIP 求解数值平方和+Gauss-Newton 迭代+有理正交投影) 总共花费了不到 2 秒的时间就得到了上面的精确平方和分解形式。

多项式 “Vor1” 关于变量 u 的判别式 “Vor2” 是一个有 253 个单项式的 18

次多项式, 我们的算法用了总共不到 10 秒就得到了它的多项式平方和分解

$$\begin{aligned}
& (-a\beta^3x + 2a^4\alpha^2y^2 + 4a^4\beta^2x^2 - 2a\beta x - 4a^4 + a^6\alpha^2 + a^4y^2 + a^2x^2 - 4a^2 + 4a^5\beta x - a^5\alpha^3y \\
& + a^5\alpha^2\beta x + a^3\beta xy^2 + a^3\alpha x^2y + a\alpha\beta^2y - 2a^5\alpha y - a^3\beta x^3 - a^3\alpha y^3 + 2a^2\beta^2x^2 + 4a^2\alpha^2y^2 + \beta^2 \\
& - 6a^2\alpha\beta xy + 4a\alpha y - 6a^4\alpha\beta xy)^2 + (-a\beta^2y + 4ay + 4a^2\alpha + 4a^3y + 4a^4\alpha - a^3y^3 - a^6\alpha^3 \\
& - 6a^2\beta xy - 6a^3\alpha\beta x - 4a^4\beta xy - 4a^5\alpha\beta x + 4a^2\alpha y^2 - a^2\alpha\beta^2 - a^3x^2y + 4a^3\alpha^2y + a^4\alpha y^2 \\
& - a^4\alpha x^2 + a^5\alpha^2y)^2 + (-4a^2\beta - 4a^3x - 4a^4\beta + a^3x^3 - 4a^5x + 4a\alpha\beta y + 4a^2\alpha xy + 6a^3\alpha\beta y \\
& + 6a^4\alpha xy + \beta^3 - a\beta^2x + a^2\beta y^2 - a^2\beta x^2 + a^3xy^2 - 4a^3\beta^2x - 4a^4\beta x^2 + a^4\alpha^2\beta + a^5\alpha^2x)^2 \\
& + \frac{1}{7}(-a^2\beta^2xy + a^2\alpha\beta y^2 - a^3\beta x^2y + a^3\alpha xy^2 - a^3\alpha\beta^2x + a^3\alpha^2\beta y - a^4\alpha\beta x^2 + a^4\alpha^2xy \\
& + 14a\beta y + 14a^2xy + 14a^2\alpha\beta + 13a^3\beta y + 14a^3\alpha x + 13a^4xy + 13a^4\alpha\beta + 13a^5\alpha x)^2 \\
& + \frac{27}{7}(a^2\beta^2xy - a^2\alpha\beta y^2 + a^3\beta x^2y - a^3\alpha xy^2 + a^3\alpha\beta^2x - a^3\alpha^2\beta y + a^4\alpha\beta x^2 - a^4\alpha^2xy \\
& + a^3\beta y + a^4xy + a^4\alpha\beta + a^5\alpha x)^2.
\end{aligned}$$

4.4 Siegfried Rump 的模型问题的求解和下界验证

在这一部分, 我们使用稀疏平方和松弛方法将 Rump 提出的一个模型问题转化成半定规划求解并使用 Newton-Lagrange 方法来精化得到的全局最优解。此外我们使用前面的有理化精确验证方法验证问题的下界。

4.4.1 问题的数学背景

Rump 的模型问题 [51, 50] 为如下最小化问题

$$\begin{aligned}
\mu_n = \min\{\|PQ\|^2 \mid P, Q \in \mathbb{R}[z], \deg(P) = \deg(Q) = n - 1, \\
\|P\| = \|Q\| = 1\}. \quad (4.14)
\end{aligned}$$

对于一个非奇异线性方程组 $A\xi = b$, 我们记它的 Toeplitz 条件数为 $\kappa^{\text{Toep}}(A, \xi)$, 它刻画了 ξ 关于矩阵 A 的无限小 Toeplitz 结构扰动和向量 b 的扰动的敏感性。文章 [49] 中证明了 Toeplitz 条件数和无结构条件数的比满足

$$\frac{\kappa^{\text{Toep}}(A, \xi)}{\kappa(A, \xi)} = \alpha \frac{\|A^{-1}J\Psi_\xi\|}{\|A^{-1}\|\|\xi\|} \geq \frac{1}{\sqrt{n}} \frac{\sigma_{\min}(\Psi_\xi)}{\|\xi\|},$$

其中矩阵 Ψ_ξ 为

$$\Psi_\xi := \begin{bmatrix} \xi_1 & \cdots & \xi_n & & \\ & & \cdots & & \\ & & \xi_1 & \cdots & \xi_n \end{bmatrix} \in \mathbb{R}^{n \times (2n-1)},$$

$J \in \mathbb{R}^{n \times n}$ 是将 $(1, \dots, n)^T$ 映射到 $(n, \dots, 1)^T$ 的置换矩阵并且 $\frac{1}{\sqrt{n}} \leq \alpha \leq \sqrt{2}$ 。从文章 [51] 中可知对于任意的 n 成立

$$\sqrt{\mu_n} = \min_{\|\xi\|=1} \sigma_{\min}(\Psi_\xi) = \min_{\|\xi\|=\|\eta\|=1} \|\Psi_\xi \eta\| = \min_{\|\xi\|=\|\eta\|=1} \|\Psi_\eta \xi\|.$$

Rump 的模型问题的反问题是如下因式系数界问题 [9, 134-139 页]

$$\max \|P\|^2 \text{ such that } \|P\| = \|Q\| \text{ and } \|PQ\|^2 = 1. \quad (4.15)$$

设多项式 $F(z) = P(z)Q(z) = a(z - \alpha_1) \cdots (z - \alpha_{n-1}) \cdot b(z - \alpha_n) \cdots (z - \alpha_{2n-2})$ ，则由 $F(z)$ 的 Mahler 测度满足

$$M(F) = \prod_{i=1}^{2n-2} \max\{1, |\alpha_i|\}, \quad M(F) \leq \frac{\|F\|}{|ab|}$$

可以得到

$$\begin{aligned} \|P\|^2 \|Q\|^2 &= a^2 \sum_{i=0}^{n-1} \left| \sum_{1 \leq j_1 \leq \cdots \leq j_i \leq n-1} \alpha_{j_1} \cdots \alpha_{j_i} \right|^2 \times b^2 \sum_{k=0}^{n-1} \left| \sum_{n \leq l_1 \leq \cdots \leq l_k \leq 2n-2} \alpha_{l_1} \cdots \alpha_{l_k} \right|^2 \\ &\leq (ab)^2 \sum_{i=0}^{n-1} \sum_{k=0}^{n-1} \left(\binom{n-1}{i} \binom{n-1}{k} M(F) \right)^2 \\ &\leq \|F\|^2 \sum_{i=0}^{n-1} \sum_{k=0}^{n-1} \binom{n-1}{i}^2 \binom{n-1}{k}^2 = \binom{2n-2}{n-1}^2. \end{aligned}$$

由此得到 Mignotte 的下界 [35]

$$\frac{\|PQ\|^2}{\|P\|^2 \|Q\|^2} \geq \frac{1}{\binom{2n-2}{n-1}}. \quad (4.16)$$

μ_n 的上界可以很快的求解，目前主要的问题是计算 μ_n 的严格下界。在文章 [50] 中对于 $n \leq 8$ 的情形给出了一个下界。我们知道在 $n \leq 14$ 时 Mignotte 的下界要远远小于实际下界。接下来，我们将通过对稀疏形式的半定规划的计算结果应用有理化精确验证方法，对于 $n \leq 14$ 的情形求解更好的精确验证下界。

4.4.2 半定规划求解有理函数最优解

问题 (4.14) 等价于如下的有理函数最小化问题

$$\mu_n = \min \left\{ \frac{\|PQ\|^2}{\|P\|^2\|Q\|^2} \mid P(z) = \sum_{i=1}^n p_i z^{i-1}, Q(z) = \sum_{i=1}^n q_i z^{i-1} \in \mathbb{R}[z] \right\}. \quad (4.17)$$

可以看出目标有理函数中来自 P, Q 的待定变元个数分别为 $n(P) = n(Q) = n$ 。一般讨论的是范数 $\|\cdot\|$ 为 $\|\cdot\|_2$ 的情形, 在 [51] 中证明了当问题取得最优值时, 多项式 P, Q 的所有根都在单位圆上并且它们的系数向量一定是对称或反对称的。由此可以给上述问题加上如下三种不同的限制条件

$$\begin{aligned} p_{n+1-i} &= p_i, & q_{n+1-i} &= q_i, & 1 \leq i \leq n, \\ p_{n+1-i} &= p_i, & q_{n+1-i} &= -q_i, & 1 \leq i \leq n, \\ p_{n+1-i} &= -p_i, & q_{n+1-i} &= -q_i, & 1 \leq i \leq n, \end{aligned}$$

并且求解得到的三个最小值中最小的等于 μ_n 。以上最小化问题的目标有理函数 $f(X)/g(X)$ 的分子和分母分别为

$$f(X) = \|PQ\|^2 = \sum_{k=2}^{2n} \left(\sum_{i+j=k} p_i q_j \right)^2, \quad g(X) = \|P\|^2 \|Q\|^2 = \left(\sum_{i=1}^n p_i^2 \right) \left(\sum_{j=1}^n q_j^2 \right),$$

其中所有待定变量为

$$X = \{p_1, \dots, p_{n(P)}\} \cup \{q_1, \dots, q_{n(Q)}\}.$$

可知加上对称或反对称条件后变元的个数减少为 $n(P) = n(Q) = \lceil n/2 \rceil$ 。将问题转化为如下半定规划求解可以得到 μ_n 的一个近似值

$$\left. \begin{aligned} \mu_n^* &:= \sup_{r \in \mathbb{R}, W} r \\ \text{s.t. } & f(X) - rg(X) = m_d(X)^T \cdot W \cdot m_d(X), \\ & W \succeq 0, W^T = W, \end{aligned} \right\} \quad (4.18)$$

这里 $\deg(f) = \deg(g) = 4$ 并且 $m_d(X)$ 为所有全次数小于等于 $d = 2$ 的单项式组成的列向量, 实对称半正定矩阵 W 的行列数为 $\binom{n(P)+n(Q)+2}{2}$ 并且问题展开后有 $\binom{n(P)+n(Q)+4}{4}$ 个等式限制条件。

类似于 2.3.1 [32], 我们探索半定规划 (4.18) 中的稀疏结构。记 $C(p)$ 为多项式 $p(X) = \sum_{\alpha} p_{\alpha} X^{\alpha}$ 中所有次数 $\text{supp}(p) = \{\alpha \mid p_{\alpha} \neq 0\}$ 的凸包, 则半定规划 (4.18) 中的平方和松弛条件为

$$f(X) - rg(X) = m_d(X)^T \cdot W \cdot m_d(X) = \sum_k v_k(X)^2.$$

设 $u(X) = \sum_{i=1}^{n(P)} \sum_{j=1}^{n(Q)} p_i q_j$, X^{σ} 是 $v_k(X)$ 中的任意单项式, 则根据定理 2.1

$$\sigma \in \frac{1}{2}C(f(X) - rg(X)) \subseteq \frac{1}{2}C(u(X)^2) = C(u(X)).$$

由凸包的性质, 存在 $\lambda_{i,j} \geq 0$, $1 \leq i \leq n(P), 1 \leq j \leq n(Q)$ 满足

$$X^{\alpha} = \prod_{i,j} (p_i q_j)^{\lambda_{i,j}} = \prod_i p_i^{\sum_j \lambda_{i,j}} \prod_j q_j^{\sum_i \lambda_{i,j}}, \sum_{i,j} \lambda_{i,j} = 1.$$

因此存在某个 i, j 使得 $X^{\alpha} = p_i q_j$ 。由此得到问题 (4.17) 的稀疏形式的半定规划

$$\left. \begin{aligned} \mu_n^* &:= \sup_{r \in \mathbb{R}, W} r \\ \text{s.t. } & f(X) - rg(X) = m_G(X)^T \cdot W \cdot m_G(X), \\ & W \succeq 0, W^T = W, \end{aligned} \right\} \quad (4.19)$$

其中 $m_G(X)$ 为所有单项式 $p_i q_j$, $1 \leq i \leq n(P), 1 \leq j \leq n(Q)$ 组成的列向量, 实对称半正定矩阵 W 的行列数为 $n(P)n(Q)$ 并且问题展开后有 $\binom{n(P)+1}{2} \binom{n(Q)+1}{2}$ 个等式限制条件。对于 $n = 14$, 稀疏形式的半定规划 (4.19) 有 784 个等式限制条件并且 $\dim(W) = 49$, 而稠密形式的半定规划 (4.18) 有 3060 个等式限制条件并且 $\dim(W) = 120$ 。

对于半定规划 (4.19) 可使用半定规划软件包 SOSTOOLS [46]、YALMIP [34] 和 SeDuMi [56] 里的算法快速求解。但是从表 4.1 中可以看出, 由固定精度半定规划软件包计算得到的下界精度不够, 并且因为误差的原因甚至可能比 [50] 中给出的上界还大。我们可以使用其他方法来改善计算结果, 比如对

$$\left. \begin{aligned} \min_{P,Q} & \|PQ\|^2 \\ \text{s.t. } & \|P\|^2 = 1, \|Q\|^2 = 1 \end{aligned} \right\}$$

应用 Newton-Lagrange 方法 (见 1.2.3)。

表 4.1: 半定规划与 Rump 的上界的对比试验结果

n	μ_n^* from fixed prec. SDP	Newton-Lagrange	Rump's upper bound
3	0.111111111111111132	0.11111111111111112	0.11111111111111113
4	0.0174291733214352	0.01742917332143266	0.01742917332143269
5	0.00233959554819155	0.002339595548155594	0.002339595548155599
6	0.00028973187528375	0.0002897318752796807	0.0002897318752796843
7	0.0000341850701964797	0.00003418506980008289	0.00003418506980008323
8	0.00000390543564465773	0.000003905435649755721	0.000003905435649755845
9	4.36004072290608e-007	4.360016539181021e-007	4.360016539181362e-007
10	4.78395278113997e-008	4.783939568771179e-008	4.783939568772086e-008
11	5.18272812166654e-009	5.178749097446552e-009	5.178749097451150e-009
12	5.54188889223539e-010	5.545881831162859e-010	5.545881831173105e-010
13	4.06299438537872e-011	5.886688081195787e-011	5.886688081216679e-011
14	2.26410681869460e-010	6.202444992001861e-012	6.202444992172272e-012

从表 4.1 中我们可以看出, 用 Matlab 求解稀疏形式的半定规划 (4.19) 得到的全局最优解和在 Maple 11 中设 Digits := 16 时用 Newton-Lagrange 方法精细化后的计算结果都比 Rump 给出的上界 [50] 更小。实际上我们可以对任意给定的初始多项式 P 和 Q 应用 Newton-Lagrange 方法, 而不是必须使用求解半定规划 (4.19) 的计算结果。但是半定规划 (4.19) 的计算结果提供给我们一个初始的半正定矩阵 W , 它可以被用在接下来的精确下界验证上。

4.4.3 精确验证下界

给定一个有理下界 $r_n = \mu_n^* - \rho_n$, 其中 ρ_n 是一个很小的正数。我们将求解稀疏形式的半定规划 (4.19) 计算得到的矩阵 W 作为初始近似半正定矩阵, 并对由如下稀疏平方和分解得到的方程组应用 Gauss-Newton 迭代精化

$$f(x) - r_n g(x) = m_G(x)^T \cdot W \cdot m_G(x) = \sum_k \left(\sum_\alpha c_{k,\alpha} x^\alpha \right)^2 \in \mathbb{R}[x].$$

我们得到精化后的矩阵 W 并将其转化为有理矩阵。通过求解最小二乘问题

$$\left. \begin{array}{l} \min_{\tilde{W}} \sum_{i,j} (w_{i,j} - \tilde{w}_{i,j})^2 \\ \text{s.t. } f(x) - r_n g(x) = m_G(x)^T \tilde{W} m_G(x) \end{array} \right\} \quad (4.20)$$

第五章 结论与展望

前面我们讨论了怎样用半定规划求解多项式近似 GCD 问题和近似因式分解问题，它们都可以转化为一个关于因式多项式系数的无限制条件的四次多项式最优化问题。这是一个非凸非线性最小二乘问题，并且一般很难寻找全局最优解。我们提议用多种不同的平方和松弛方法生成的半定规划来求解这个特殊的多项式最优化问题。使用稠密的平方和松弛方法来求解全局最优解通常很好，但是对于大问题的计算是很困难的。通过探索近似 GCD 问题和近似因式分解问题得到的四次多项式的特殊稀疏结构，我们研究了在稀疏情形下的全局最优解求解方法，并且提议使用基于不同的最小化问题形式和稀疏技术的多种稀疏平方和松弛方法来求解。我们实现了算法并通过数值试验显示了这些不同松弛方法的效果。

在选择这些不同的稀疏松弛方法时各有优劣，稀疏平方和松弛 (2.17) 是整体质量最好的（它的计算结果和稠密平方和松弛相同），但是它在这些稀疏松弛中最费时。稀疏平方和松弛 (2.20) 的计算结果最差，但是它是最快的并且可以求解更大的问题。实际中为了求解更大的问题，我们建议使用平方和松弛 (2.20) 来寻找一个近似解，然后应用 STLN 等局部方法来精化结果。在 Rump 的模型问题求解上，我们同样探索了其中的特殊稀疏性。

近似 GCD 问题和近似因式分解问题也可以等价地转化为一个无限制条件有理函数最小化问题 (2.7)。这种形式在因式次数很小且变量很少时比多项式形式的半定规划 (2.2) 更快。但是当原问题很大时问题 (2.7) 很难求解。探索 (2.7) 中的特殊结构并得到更有效的方法也是一个值得感兴趣的工作。

平方和松弛方法的优点在于它们不需要一个初始解并且总是能返回一个全局最小值的下界。当在某个点计算得到了这个下界，我们立刻知道找到了全局最优解。我们前面的试验显示，这些平方和松弛方法在求解近似 GCD 问题和近似因式分解问题上效果很好，对于我们的所有例子返回的都是全局最优解。

我们提议使用基于非线性最小二乘形式 (2.1),(3.2) 的稀疏平方和松弛方法。因为近似 GCD 问题和近似因式分解问题也可以分别等价地转化为 (2.9),(3.4) 的形式，所以探索其中的特殊稀疏结构也是有可能的。一个值得感兴趣的未来工作是对 (2.10)-(2.12) 和基于它们的特殊结构得到更有效的平方和松弛。

半定规划得到的数值结果是不精确的，通过有理化数值平方和使得平方和等式精确成立，我们可以消去半定规划求得的数值结果中的不精确性，并且精确验证下界以及得到精确的平方和分解。我们验证了几个符号数值混合计算中以前不能验证的问题的下界。我们的验证方法要求输入中的有理 Moment 矩阵是半正定矩阵，这可以通过对半定规划得到的数值平方和使用保持秩结构条件的 Gauss-Newton 迭代精化来达到。我们的验证方法也要求可以得到一个精确的平方和等式表示形式，这可以通过松弛下界的投影来达到。

仍然不清楚的是，是否半定规划对于 Gauss-Newton 迭代是必须的，以及是否正交投影是保持半正定性的最好方法（见注 6）。最后要提到的是，平方和可以通过 Artin 形式的有理函数平方和形式，或者通过添加叫做“大球”限制的方法来去掉松弛性并且变成紧的（已知存在非负多项式 f ，对于任意 $\delta \geq 0$ ， $f + \delta$ 都不是平方和）。我们以后将继续探索研究这些方向，探讨怎样用符号和数值混合方法来验证全局最优解。

参考文献

- [1] David Boyd, Erich Kaltofen, and Lihong Zhi. Integer polynomials with large single factor coefficient bounds. In preparation, 2008.
- [2] Guillaume Chèze and Jean-Claude Yakoubsohn. Distance computation to the resultant variety, November 2007. Talk at the Journées 2007 da l'ANR GECKO, URL: <http://www-sop.inria.fr/galaad/conf/07gecko/Yakoubshon.J.C.pdf>.
- [3] Paulina Chin, Robert M. Corless, and George F. Corliss. Optimization strategies for the approximate GCD problem. In Gloor [10], pages 228–235.
- [4] R. M. Corless, P. M. Gianni, and B. M. Trager. The reordered Schur factorization method for zero-dimensional polynomial systems with multiple roots. In W. Küchlin, editor, *Proc. 1997 Internat. Symp. Symbolic Algebraic Comput. ISSAC'97*, pages 133–140, New York, N. Y., 1997. ACM Press.
- [5] Hazel Everett, Daniel Lazard, Sylvain Lazard, and Mohab Safey El Din. The Voronoi diagram of three lines in r^3 . In *SoCG '07: Proceedings of the 23-rd Annual Symposium on Computational Geometry*, pages 255–264. ACM, New York, USA, 2007.
- [6] Shuhong Gao. Factoring multivariate polynomials via partial differential equations, 2001. Available from <http://www.math.clemson.edu/~sgao/pub.html>. To appear in *Math. Comput.*.
- [7] Shuhong Gao, Erich Kaltofen, John P. May, Zhengfeng Yang, and Lihong Zhi. Approximate factorization of multivariate polynomials via differential equations. In Gutierrez [12], pages 167–174. ACM SIGSAM's ISSAC 2004 Distinguished Student Author Award (May and Yang).

- [8] Shuhong Gao, Erich Kaltofen, John P. May, Zhengfeng Yang, and Lihong Zhi. Approximate factorization of multivariate polynomials via differential equations. In Gutierrez [12], pages 167–174.
- [9] A. O. Gelfond. *Transcendental and algebraic numbers. Translated from the 1st Russian ed. by Leo F. Boron.* Dover, New York, 1960.
- [10] O. Gloor, editor. *ISSAC 98 Proc. 1998 Internat. Symp. Symbolic Algebraic Comput.*, New York, N. Y., 1998. ACM Press.
- [11] G. H. Golub and C. F. Van Loan. *Matrix Computations.* Johns Hopkins University Press, Baltimore, Maryland, third edition, 1996.
- [12] Jaime Gutierrez, editor. *ISSAC 2004 Proc. 2004 Internat. Symp. Symbolic Algebraic Comput.*, New York, N. Y., 2004. ACM Press.
- [13] Didier Henrion and Jean Bernard Lasserre. Detecting global optimality and extracting solutions in gloptipoly. In D. Henrion and A. Garulli, editors, *Positive Polynomials in Control*, volume 312 of *Lecture Notes in Control and Information Sciences*, pages 293–310. Springer Verlag, Berlin, 2005.
- [14] Christopher Hillar. Sums of polynomial squares over totally real fields are rational sums of squares. *Proc. American Math. Society*, 2008. To appear. URL: <http://www.math.tamu.edu/~chillar/files/totallyrealsos.pdf>.
- [15] M. A. Hitz and E. Kaltofen. Efficient algorithms for computing the nearest polynomial with constrained roots. In Gloor [10], pages 236–243.
- [16] M. A. Hitz, E. Kaltofen, and Lakshman Y. N. Efficient algorithms for computing the nearest polynomial with a real root and related problems. In S. Dooley, editor, *Proc. 1999 Internat. Symp. Symbolic Algebraic Comput. (ISSAC'99)*, pages 205–212, New York, N. Y., 1999. ACM Press.
- [17] Dorina Jibetean and Etienne de Klerk. Global optimization of rational functions: a semidefinite programming approach. *Mathematical Programming*, 106(1):93–109, 2006.

-
- [18] Erich Kaltofen, Bin Li, Kartik Sivaramakrishnan, Zhengfeng Yang, and Lihong Zhi. Lower bounds for approximate factorizations via semidefinite programming (extended abstract). In Verschelde and Watt [58], pages 203–204.
- [19] Erich Kaltofen, Bin Li, Zhengfeng Yang, and Lihong Zhi. Exact certification of global optimality of approximate factorizations via rationalizing sums-of-squares with floating point scalars. In David Jeffrey, editor, *ISSAC 2008 Proc. 2008 Internat. Symp. Symbolic Algebraic Comput.*, New York, N. Y., 2008. ACM Press.
- [20] Erich Kaltofen and John May. On approximate irreducibility of polynomials in several variables. In J. R. Sendra, editor, *ISSAC 2003 Proc. 2003 Internat. Symp. Symbolic Algebraic Comput.*, pages 161–168, New York, N. Y., 2003. ACM Press.
- [21] Erich Kaltofen, John May, Zhengfeng Yang, and Lihong Zhi. Approximate factorization of multivariate polynomials using singular value decomposition. *J. Symbolic Comput.*, 43(5):359–376, 2008.
- [22] Erich Kaltofen, Zhengfeng Yang, and Lihong Zhi. Approximate greatest common divisors of several polynomials with linearly constrained coefficients and singular polynomials. In Jean-Guillaume Dumas, editor, *ISSAC MMVI Proc. 2006 Internat. Symp. Symbolic Algebraic Comput.*, pages 169–176, New York, N. Y., 2006. ACM Press.
- [23] Erich Kaltofen, Zhengfeng Yang, and Lihong Zhi. Approximate greatest common divisors of several polynomials with linearly constrained coefficients and singular polynomials. Manuscript, 21 pages, December 2006.
- [24] Erich Kaltofen, Zhengfeng Yang, and Lihong Zhi. On probabilistic analysis of randomization in hybrid symbolic-numeric algorithms. In Verschelde and Watt [58], pages 11–17.
- [25] 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. Birkhäuser Verlag, Basel, Switzerland, 2007. Preliminary version in [61], pp. 188–201.
- [26] N. Karmarkar and Lakshman Y. N. Approximate polynomial greatest common divisors and nearest singular polynomials. In Lakshman Y. N., editor, *ISSAC 96 Proc. 1996 Internat. Symp. Symbolic Algebraic Comput.*, pages 35–42, New York, N. Y., 1996. ACM Press.
- [27] N. K. Karmarkar and Lakshman Y. N. On approximate GCDs of univariate polynomials. *J. Symbolic Comput.*, 26(6):653–666, 1998. Special issue on Symbolic Numeric Algebra for Polynomials S. M. Watt and H. J. Stetter, editors.
- [28] M. Kojima, S. Kim, and H. Waki. Sparsity in sums of squares of polynomials. *Mathematical Programming*, 103:45–62, 2005.
- [29] Jean Bernard Lasserre. Global optimization with polynomials and the problem of moments. *SIAM Journal on Optimization*, 11(3):796–817, 2001.
- [30] Jean Bernard Lasserre. Convergent SDP-relaxations in polynomial optimization with sparsity. *SIAM Journal on Optimization*, 17(3):822–843, 2006.
- [31] Bin Li, Jiawang Nie, and Lihong Zhi. Approximate GCDs of polynomials and SOS relaxation. In Verschelde and Watt [58], pages 205–206.
- [32] Bin Li, Jiawang Nie, and Lihong Zhi. Approximate GCDs of polynomials and sparse SOS relaxations. Revised version submitted to Theoretical Computer Science, 2008.
- [33] Bingyu Li, Zhuojun Liu, and Lihong Zhi. Structured condition numbers of Sylvester matrices (extended abstract), December 2007. Presented at MACIS 2007, URL: http://www-spiral.lip6.fr/MACIS2007/Papers/submission_17.pdf.

- [34] J. Löfberg. YALMIP: A toolbox for modeling and optimization in MATLAB. In *Proceedings of the CACSD Conference*, pages 284–289, Taipei, Taiwan, 2004. URL: <http://control.ee.ethz.ch/~joloef/yalmip.php>.
- [35] M. Mignotte. Some useful bounds. In B. Buchberger, G. Collins, and R. Loos, editors, *Computer Algebra*, pages 259–263. Springer Verlag, Heidelberg, Germany, 2 edition, 1982.
- [36] Kosaku Nagasaka. Towards certified irreducibility testing of bivariate approximate polynomials. In T. Mora, editor, *Proc. 2002 Internat. Symp. Symbolic Algebraic Comput. (ISSAC'02)*, pages 192–199, New York, N. Y., 2002. ACM Press.
- [37] Yurii Nesterov and Arkadii Nemirovskii. *Interior-Point polynomial algorithms in convex programming*, volume 13 of *Studies in Applied Mathematics*. SIAM, Philadelphia, PA, 1994.
- [38] Jiawang Nie and James Demmel. Sparse SOS relaxations for minimization functions that are summation of small polynomials, 2007. URL: <http://www.arxiv.org/abs/math.OC/0606476>.
- [39] Jiawang Nie, James Demmel, and Ming Gu. Global minimization of rational functions and the nearest GCDs. *Journal of Global Optimization*, 40(4):697–718, 2008.
- [40] Jiawang Nie, Kristian Ranestad, and Bernd Sturmfels. The algebraic degree of semidefinite programming, 2006. URL: <http://www.citebase.org/abstract?id=oai:arXiv.org:math/0611562>.
- [41] Jiawang Nie and Markus Schweighofer. On the complexity of Putinar's Positivstellensatz. *J. Complexity*, 23:135–70, 2007.
- [42] Pablo A. Parrilo. *Structured Semidefinite Programs and Semialgebraic Geometry Methods in Robustness and Optimization*. PhD thesis, California Institute of Technology, Pasadena, CA, 2000. URL: <http://www.mit.edu/~parrilo/>.

- [43] Pablo A. Parrilo. Exploiting algebraic structure in sum of squares programs. In *Positive polynomials in Control*, volume 312 of *Lecture Notes in Control and Information Sciences*, pages 181–194. Springer, 2005.
- [44] Pablo A. Parrilo and Bernd Sturmfels. Minimizing polynomial functions. In *Algorithmic and Quantitative Real Algebraic Geometry*, volume 60 of *DMACS Series in Discrete Mathematics and Theoretical Computer Science*, pages 83–99. AMS, 2003.
- [45] Helfried Peyrl and Pablo A. Parrilo. A Macaulay 2 package for computing sum of squares decompositions of polynomials with rational coefficients. In Verschelde and Watt [58], pages 207–208.
- [46] Stephen Prajna, Antonis Papachristodoulou, Peter Seiler, and Pablo A. Parrilo. *SOSTOOLS: Sum of squares optimization toolbox for MATLAB*, 2004. URL: <http://www.mit.edu/~parrilo/sostools>.
- [47] Bruce Reznick. Extremal PSD forms with few terms. *Duke Mathematical Journal*, 45(2):363–374, 1978.
- [48] Bruce Reznick. Some concrete aspects of Hilbert’s 17th problem. In Charles N. Delzell and James J. Madden, editors, *Real Algebraic Geometry and Ordered Structures*, volume 253 of *Contemporary Mathematics*, pages 251–272. AMS, Providence, RI, USA, 2000.
- [49] Siegfried M. Rump. Structured perturbations part I: Normwise distances. *SIAM J. Matrix Anal. Applic.*, 25(1):1–30, 2003.
- [50] Siegfried M. Rump. Global optimization: a model problem, 2006. URL: <http://www.ti3.tu-harburg.de/rump/Research/ModelProblem.pdf>.
- [51] Siegfried M. Rump and H. Sekigawa. The ratio between the Toeplitz and the unstructured condition number, 2006. To appear. URL: <http://www.ti3.tu-harburg.de/paper/rump/RuSe06.pdf>.
- [52] W. M. Ruppert. Reduzibilität ebener Kurven. *J. reine angew. Math.*, 369:167–191, 1986.

-
- [53] Wolfgang M. Ruppert. Reducibility of polynomials $f(x, y)$ modulo p . *J. Number Theory*, 77:62–70, 1999.
- [54] N. Z. Shor. Class of global minimum bounds of polynomial functions. *Cybernetics and Systems Analysis*, 23(6):731–734, 1987.
- [55] N. Z. Shor and P. I. Stetsyuk. The use of a modification of the r-algorithm for finding the global minimum of polynomial functions. *Cybernetics and Systems Analysis*, 33:482–497, 1997.
- [56] Jos F. Sturm. Using SeDuMi 1.02, a MATLAB toolbox for optimization over symmetric cones. *Optimization Methods and Software*, 11/12:625–653, 1999. URL: <http://sedumi.mcmaster.ca>.
- [57] Lieven Vandenbergh and Stephen Boyd. Semidefinite programming. *SIAM Review*, 38(1):49–95, 1996.
- [58] Jan Verschelde and Stephen M. Watt, editors. *SNC'07 Proc. 2007 Internat. Workshop on Symbolic-Numeric Comput.*, New York, N. Y., 2007. ACM Press.
- [59] Gilles Villard. Certification of the QR factor R and of lattice basis reducedness. In Christopher W. Brown, editor, *ISSAC 2007 Proc. 2007 Internat. Symp. Symbolic Algebraic Comput.*, pages 361–368, New York, N. Y., 2007. ACM Press.
- [60] Hayato Waki, Sunyoung Kim, Masakazu Kojima, and Masakazu Mura-matsu. Sums of squares and semidefinite program relaxations for polynomial optimization problems with structured sparsity. *SIAM Journal on Optimization*, 17(1):218–242, 2006.
- [61] Dongming Wang and Lihong Zhi, editors. *Internat. Workshop on Symbolic-Numeric Comput. SNC 2005 Proc.*, 2005. Distributed at the Workshop in Xi'an, China, July 19–21.

- [62] Henry Wolkowicz, Romesh Saigal, and Lieven (Eds.) Vandenberghe. *Handbook of Semidefinite Programming: Theory, Algorithms, and Applications*. Kluwer Academic, Boston, 2000.
- [63] Ting Zhang, Rong Xiao, and Bican Xia. Real solution isolation based on interval Krawczyk operator. In Sung il Pae and Hyungju Park, editors, *Proc. of the Seventh Asian Symposium on Computer Mathematics*, pages 235–237, Seoul, South Korea, 2005. Korea Institute for Advanced Study. Extended abstract.
- [64] Lihong Zhi. Numerical optimization in hybrid symbolic-numeric computation. In Verschelde and Watt [58], pages 33–35.
- [65] Lihong Zhi, Matu-Tarow Noda, Hiroshi Kai, and Wenda Wu. Hybrid method for computing the nearest singular polynomials. *Japan J. Industrial and Applied Math.*, 21(2):149–162, June 2004.
- [66] Lihong Zhi and Wenda Wu. Nearest singular polynomial. *J. Symbolic Comput.*, 26(6):667–675, 1998. Special issue on Symbolic Numeric Algebra for Polynomials S. M. Watt and H. J. Stetter, editors.

发表文章目录

- [1] Erich Kaltofen, Bin Li, Kartik Sivaramakrishnan, Zhengfeng Yang, and Lihong Zhi. Lower bounds for approximate factorizations via semidefinite programming (extended abstract). In Verschelde and Watt [58], pages 203–204, 2007.
- [2] Bin Li, Jiawang Nie, and Lihong Zhi. Approximate GCDs of polynomials and SOS relaxation. In Verschelde and Watt [58], pages 205–206, 2007.
- [3] Bin Li, Jiawang Nie, and Lihong Zhi. Approximate GCDs of polynomials and sparse SOS relaxations. Revised version submitted to Theoretical Computer Science, 2008.
- [4] Erich Kaltofen, Bin Li, Zhengfeng Yang, and Lihong Zhi. Exact certification of global optimality of approximate factorizations via rationalizing sums-of-squares with floating point scalars. In David Jeffrey, editor, *ISSAC 2008 Proc. 2008 Internat. Symp. Symbolic Algebraic Comput.*, New York, N. Y., 2008. ACM Press.

个人简介

李斌, 男, 河北省, 1983 年出生。 E-mail: bli@mmrc.iss.ac.cn

教育状况

- 2005.9–2008.7 中国科学院数学与系统科学研究院, 系统所, 硕士研究生。
方向: 符号与数值混合计算, 导师: 吴文俊、支丽红。
- 2000.9–2004.7 复旦大学, 数学系理科基地班, 本科。
- 1997.9–2000.7 河北省邯郸市第一中学。

会议活动

- 2007 年 11 月, 数学与系统科学研究院系统所青年学术会议, 北京。
- 2007 年 6 月, The First Chinese-SALSA Workshop, 北京大学。
- 2007 年 3 月, The Second NCSU-China Symbolic Computation Collaboration Workshop, 杭州。
- 2006 年 6 月, 中国科学院第十三次和中国工程院第八次院士大会开幕会, 北京。

获奖经历

- 2006 年中国科学院研究生院数学科学学院院长奖学金。
- 2004 年复旦大学人民奖学金二等奖。
- 2003 年美国大学生数学建模竞赛 (MCM) Honorable Mention 奖。
- 2003 年复旦大学程序设计竞赛一等奖。
- 2002 年全国大学生数学建模竞赛全国二等奖、上海赛区一等奖。
- 2002 年华东地区数学建模竞赛二等奖。
- 2001 年复旦大学人民奖学金三等奖。
- 2000 年中国数学奥林匹克 (CMO、数学冬令营) 三等奖。

致 谢

值此论文完成之际，谨在此向多年来给予我关心和帮助的各位老师、同学、朋友和家人表示衷心的感谢！

首先要特别感谢我的导师支丽红老师！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认真指导下完成的。支老师的严格要求和教诲无论是在学习还是生活上都使我受益良多，她活跃的思维、崇高的敬业精神和严谨的治学态度都深深影响了我并值得我学习。

特别感谢 Erich Kaltofen、杨争峰师兄、聂家旺和 Kartik Sivaramakrishnan 在论文研究讨论中的贡献和帮助！Erich Kaltofen 教授平易近人，在同他的合作研究的过程中，我从他那里学习到了很多知识。在同杨争峰师兄一起学习期间，从他那里我获得了很多启发和热情的帮助。

特别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、王定康副研究员、李子明研究员，从他们那里我学习到了很多的知识并且获得了很多的帮助。同时感谢周代珍老师和王莎莎小姐的热心帮助。

特别感谢现在或曾经在数学机械化中心学习的李冰玉师姐、吴晓丽师姐、孙东霞师妹、郭峰师弟以及其他同学！感谢李冰玉师姐、吴晓丽师姐的帮助和照顾，也感谢一起上讨论班的其他老师和同学，通过讨论班上的讨论交流让我学习到了很多知识。

特别感谢数学与系统科学研究院和中国科学院研究生院的其他老师、同学及各位好友！感谢他们对我在学习和生活上的关心和帮助，同大家一起度过的很多愉快的时光给我留下了许多美好的回忆。

最后还要特别感谢数学与系统科学研究院和中科院研究生院的各位老师！他们的辛勤工作为我们创造了良好的学习和生活环境。