中国科学院大学

University of Chinese Academy of Sciences

博士学位论文

实根理想的计算及多项式全局最优化

作者姓名：杨志红

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：理学博士

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

2018 年 6 月

Computation of Real Radicals and Global Optimization of Polynomials

A dissertation submitted to

University of Chinese Academy of Sciences

in partial fulfillment of the requirement

for the degree of

Doctor of Philosophy

in Applied Mathematics

By

Yang Zhi-Hong

Supervisor: Professor Zhi Lihong

Academy of Mathematics and Systems Science

Chinese Academy of Sciences

June, 2018

中国科学院大学

研究生学位论文原创性声明

本人郑重声明：所呈交的学位论文是本人在导师的指导下独立进行研究工作所取得的成果。尽我所知，除文中已经注明引用的内容外，本论文不包含任何其他个人或集体已经发表或撰写过的研究成果。对论文所涉及的研究工作做出贡献的其他个人和集体，均已在文中以明确方式标明或致谢。

作者签名：

日　　期：

中国科学院大学

学位论文授权使用声明

本人完全了解并同意遵守中国科学院有关保存和使用学位论文的规定，即中国科学院有权保留送交学位论文的副本，允许该论文被查阅，可以按照学术研究公开原则和保护知识产权的原则公布该论文的全部或部分内容，可以采用影印、缩印或其他复制手段保存、汇编本学位论文。

涉密及延迟公开的学位论文在解密或延迟期后适用本声明。

作者签名：　　导师签名：

日　　期：　　日　　期：

摘 要

实根理想的计算是实代数几何中的一个基本问题，它在多项式全局最优化领域中有重要应用。

给定一组有理数域上的 n 元多项式，记这组多项式生成的理想为 I，本文考虑的第一个问题是如何计算 I 的实根理想。假设 I 的复代数簇是光滑的，我们证明 I 的实根理想有一组次数不超过其复代数簇次数的生成元。我们给出一个概率算法计算 I 的实根理想的所有极小素理想的生成元，这个算法的复杂度关于变元个数是单指数的。对于一般的情形，我们采用有理参数化来表示复代数簇和根理想。我们给出一个概率算法计算 I 的实根理想的所有素理想的有理参数化表示，这个算法的复杂度关于 I 的维数是双指数的，如果 I 的维数是固定的，那么这个算法的复杂度关于变元个数是单指数的。

给定一个 n 元实系数多项式 f，考虑其在实代数簇上的全局下确界 f^*。假设可行域是等维的，我们证明如果 f^* 不是 f 的广义关键值，那么这个优化问题的可行域就可以缩小为一个更低维的实代数簇。为了计算 f^*，我们引入一个新的集合。我们证明这个新的集合的测度为零，而且它和 f 的广义关键值集合的并集是一个半代数闭集。我们证明这个并集的测度也为零。最后，我们给出一个算法用于计算任意实代数簇上多项式函数的全局下确界，并将这个算法推广到可行域为基本半代数集的情形。

关键词：多项式，实根理想，算法，复杂度，全局最优化，广义关键值

Abstract

Computation of real radicals is a fundamental problem in real algebraic geometry, and it has important applications in global optimization of polynomials.

Given a sequence of n-variate polynomials with rational coefficients, let I denote the ideal generated by these polynomials. The first problem considered in this thesis is computing the real radical of I. Assume that the complex variety of I is smooth, we prove that the real radical of I has a set of generators with degrees bounded by the degree of the complex variety of I. We give a probabilistic algorithm to compute generators of all minimal primes of the real radical of I. The complexity of this algorithm is singly exponential in the number of variables. For general cases, we use rational parametrizations to represent complex varieties and radical ideals. We give a probabilistic algorithm to compute rational parametrizations for all minimal primes of the real radical of I. The complexity of this algorithm is doubly exponential in the dimension of I, and if the dimension of I is fixed, then the complexity of this algorithm is singly exponential in the number of variables.

Given an n-variate polynomial f with real coefficients, consider its global infimum f^* over some real algebraic variety. Assume that the feasible region is equidimensional, we prove that either f^* is a generalized critical value of f, or the feasible region of the optimization problem can be reduced to a lower dimensional real algebraic variety. In order to compute f^*, we introduce a new set. We prove that this new set has zero measure, and furthermore, the union of this new set and all generalized critical values of f is a closed semi-algebraic set. We show that this union also has zero measure. In the end, we give an algorithm to compute the global infimum of a polynomial function over an arbitrarily given real algebraic variety, and we generalize this algorithm to cases where feasible regions are basic closed semi-algebraic sets.

Key Words: Polynomial, Real Radical Ideal, Algorithm, Complexity, Global Opti-

mization, Generalized Critical Value

目 录

第 1 章 引言 1
1.1 实根理想的计算 1
1.1.1 问题概述与研究现状 1
1.1.2 主要成果 2
1.2 多项式全局最优化 4
1.2.1 问题概述与研究现状 4
1.2.2 主要成果 5
1.3 论文结构 8
第 2 章 预备知识 9
2.1 代数几何基础 9
2.2 实代数几何基础 13
第 3 章 实根理想的计算 17
3.1 问题和背景 17
3.2 预备知识 17
3.2.1 实根理想的基本性质 17
3.2.2 周形式 19
3.3 光滑情形 19
3.3.1 生成元次数上界 19
3.3.2 算法 21
3.4 一般情形 23
3.4.1 有理参数化的定义和性质 23
3.4.2 算法 25

3.5 例子 32
第 4 章 多项式全局最优化 35
4.1 问题和背景 35
4.2 预备知识 35
4.2.1 广义关键值 35
4.2.2 纤维丛 39
4.3 新的集合 $K_1(f, M)$ 及其性质 40
4.4 最优值的表示 44
4.5 算法 48
4.5.1 算法描述 48
4.5.2 算法的正确性 51
4.5.3 例子 53
4.6 半代数情形 56
第 5 章 总结与展望 61
参考文献 63
致谢 69
作者简历及攻读学位期间发表的学术论文与研究成果 71

图目录

图 1.1　例 1.2.1 ……6
图 1.2　例 1.2.2 ……7
图 4.1　例 4.4.1 …… 45
图 4.2　例 4.5.3 …… 53
图 4.3　例 4.5.4 …… 54
图 4.4　例 4.6.2 半代数集 S …… 57
图 4.5　例 4.6.2 对应于 λ_i 的半代数集 …… 59

第 1 章　引言

1.1　实根理想的计算

1.1.1　问题概述与研究现状

令 $\mathbb{Q}$，$\mathbb{R}$ 和 $\mathbb{C}$ 分别表示有理数域，实数域和复数域，令 $X = \{X_1, \ldots, X_n\}$。给定 $\mathbb{Q}[X] = \mathbb{Q}[X_1, \ldots, X_n]$ 中的一组多项式 $\boldsymbol{f} = (f_1, \ldots, f_s)$，记 $f_1, \ldots, f_s$ 在 $\mathbb{Q}[X]$ 中生成的理想为 $\langle \boldsymbol{f} \rangle$。理想 $\langle \boldsymbol{f} \rangle$ 在 $\mathbb{Q}[X]$ 中的实根理想定义为：

$$\sqrt[re]{\langle \boldsymbol{f} \rangle} = \left\{ g \in \mathbb{Q}[X] \mid g^{2m} + \sum_{i=1}^{l} a_i^2 \in \langle \boldsymbol{f} \rangle, \text{ 其中} m, l \in \mathbb{N}, \ a_i \in \mathbb{Q}[X] \right\}.$$

$\boldsymbol{f}$ 的实代数簇 (或实代数集) 定义为：

$$\mathbf{V}_{\mathbb{R}}(\boldsymbol{f}) = \{x \in \mathbb{R}^n \mid f_1(x) = 0, \ldots, f_s(x) = 0\}.$$

实零点定理 (Real Nullstellensatz) 表明，$\boldsymbol{f}$ 的实根理想等于 $\mathbf{V}_{\mathbb{R}}(\boldsymbol{f})$ 的零化理想 (vanishing ideal)。因此，实根理想是表示实代数簇的有力工具，计算实根理想也是实代数几何中的一个基本问题。下面我们从符号计算和数值计算两方面来介绍这一问题的研究现状。

符号计算方面，Becker 和 Neuhaus 在 [1] 中首次给出了计算实根理想的算法。后来 Neuhaus 在 [2] 中将这个算法的思路重新整理了一遍，并给出了实根理想生成元的次数上界 $D^{2^{O(n^2)}}$，其中 D 是输入多项式的次数上界，n 是变元的个数。这个算法主要是基于实代数簇的孤立点的性质，将实根理想的计算转化到零维的情形，然后再通过 Shape Lemma [参见 3] 转化为单个多项式的情形，最后通过因式分解转化为不可约多项式的情形。对于一个不可约多项式 $P \in \mathbb{Q}[X]$，可以通过变号准则 (sign change criterion, [参见 2, Lemma 4.1]) 来判定理想 $\langle P \rangle$ 是否是实的。这样便得到了 [1, 2] 中计算实根理想的算法。此后，Spang [4, 5] 结合极大理想的性质，给出了判定一个极大理想是否为实理想的充分条件，从而可以避免 [1, 2] 算法中的一些坐标变换运算。基于三角列特征集的性质，曾广兴和曾小宁 [6] 给出了判定一个多元多项式是否正定的方法。这

个判定方法也是 Spang 在 Singular 中实现计算实根理想算法的基础之一。肖水晶等 [7] 后续也对这个判定方法进行了改进。另一方面，基于三角列分解，陈长波等 [8-10] 引入正则半代数系统的概念，给出了一个算法用于将一般的半代数系统分解为正则半代数系统。

数值算法方面工作主要是针对 $\mathbb{R}[X] = \mathbb{R}[X_1, \ldots, X_n]$ 中的多项式和理想展开的。Lasserre 等 [11, 12] 基于半正定规划 (Semidefinite Programming, 简称 SDP) 松弛给出了计算零维实根理想的算法。这个算法的前提假设是，输入多项式系统的实代数簇是零维的。之后，应用 Pommaret 基的性质，马玥等 [13] 将这个算法推广到了正维的情形：对于 $\mathbb{R}[X]$ 中的一个理想 I，算出一个理想 J 使得 J 介于 I 和 $\sqrt[re]{I}$ 之间且 $\mathbf{V}_{\mathbb{R}}(J) = \mathbf{V}_{\mathbb{R}}(I)$。类似地，Brake 等 [14] 基于数值代数几何与平方和规划 (sums of squares programming) 提出了一个算法：对于 $\mathbb{R}[X]$ 中的一组多项式 $\boldsymbol{f} = (f_1, \ldots, f_s)$，计算出另一组多项式 $\boldsymbol{g} = (g_1, \ldots, g_m)$ 使得 $\mathbf{V}_{\mathbb{R}}(\boldsymbol{g})$ 包含在 $\mathbf{V}_{\mathbb{R}}(\boldsymbol{f})$ 中，然后判定 $\langle \boldsymbol{g} \rangle$ 是否等于 $\sqrt[re]{\langle \boldsymbol{f} \rangle}$。这个算法的难点在于最后一步，即如何判定等式 $\langle \boldsymbol{g} \rangle = \sqrt[re]{\langle \boldsymbol{f} \rangle}$ 是否成立。需要指出的是，$\mathbb{R}[X]$ 中的实理想与 $\mathbb{Q}[X]$ 中的实理想有区别，比如理想 $I = \langle X_1^3 - 2 \rangle$ 在 $\mathbb{Q}[X]$ 中的实根理想是它本身，但 I 在 $\mathbb{R}[X]$ 中的实根理想是 $X_1 - \sqrt[3]{2}$。对于这个例子，针对 $\mathbb{Q}[X]$ 的符号算法返回的是 I，针对 $\mathbb{R}[X]$ 的数值算法返回的是 $X_1 - \sqrt[3]{2}$ 的近似表达式。

本文从符号计算的角度出发，考虑如何有效地计算 $\mathbb{Q}[X]$ 中的实根理想。正如之前提到的，[1, 2, 4, 5] 中的算法理论上对 $\mathbb{Q}[X]$ 中任给的一组多项式 $\boldsymbol{f} = (f_1, \ldots, f_s)$，都能计算出 $\sqrt[re]{\langle \boldsymbol{f} \rangle}$ 的一组生成元，然而这个算法的复杂度是 $D^{2^{O(n^2)}}$ (其中 $D = \max\{\deg f_1, \ldots, \deg f_s\}$，$n$ 是变元的个数)。本文的第一个工作即是给出复杂度为 $s^{O(1)}(nD)^{O(nr2^r)}$ 的符号算法用于计算 $\boldsymbol{f}$ 在 $\mathbb{Q}[X]$ 中的实根理想，其中 r 是理想 $\langle \boldsymbol{f} \rangle$ 的维数。

1.1.2 主要成果

令 $\boldsymbol{f} = (f_1, \ldots, f_s)$ 是 $\mathbb{Q}[X] = \mathbb{Q}[X_1, \ldots, X_n]$ 中的一组多项式，$\mathbf{V}_{\mathbb{C}}(\boldsymbol{f})$ 是 $\boldsymbol{f}$ 的复代数簇，$D = \max\{\deg f_1, \ldots, \deg f_s\}$。

光滑情形 Blanco 等 [15] 证明如果 $\mathbf{V}_{\mathbb{C}}(\boldsymbol{f})$ 是等维光滑的，那么 $\langle \boldsymbol{f} \rangle$ 的根理想 $\sqrt{\langle \boldsymbol{f} \rangle}$ 有一组次数不高于 $\mathbf{V}_{\mathbb{C}}(\boldsymbol{f})$ 次数的生成元，并且给出了一个概率算法来

计算这样的一组生成元，其复杂度是 $s(nD^n)^{O(1)}$（这里的复杂度是指 $\mathbb{Q}$ 中的算术复杂度，下同）。我们把这个结果推广到实根理想。假设 $\mathbf{V}_{\mathbb{C}}(\boldsymbol{f})$ 是光滑的：

- 我们证明了 $\langle \boldsymbol{f} \rangle$ 的实根理想 $\sqrt[re]{\langle \boldsymbol{f} \rangle}$ 有一组生成元，其次数不高于 $\mathbf{V}_{\mathbb{C}}(\boldsymbol{f})$ 的次数；
- 我们给出第一个概率算法计算 $\sqrt[re]{\langle \boldsymbol{f} \rangle}$ 所有极小素理想的生成元，使得这些生成元都满足上述次数界。算法的复杂度是 $(snD^n)^{O(1)}$。

一般情形 如果 $\mathbf{V}_{\mathbb{C}}(\boldsymbol{f})$ 不是光滑的，那么 $\boldsymbol{f}$ 的实代数簇 $\mathbf{V}_{\mathbb{R}}(\boldsymbol{f})$ 可能包含在 $\mathbf{V}_{\mathbb{C}}(\boldsymbol{f})$ 的奇异轨迹 (singular locus) 中，这时已不能应用 [15] 中的结果。如果直接应用雅可比准则和 Gröbner 基来计算 $\mathbf{V}_{\mathbb{C}}(\boldsymbol{f})$ 的奇异轨迹，然后再对 $\mathbf{V}_{\mathbb{C}}(\boldsymbol{f})$ 的奇异轨迹做递归，那么最后得到的算法复杂度仍然是 $D^{2^{O(n^2)}}$。因此，我们选用另一类表示复代数簇的方法：对于一个等维的复代数簇，使用等式和不等式来表示它的一个 Zariski 开集。这类表示主要有两种，一种是三角列 [16, 17] (也叫正则链 (regular chains)[18], 单扩张塔 (tower of simple extensions)[19], 正则集 (regular set)[20])，另一种是有理参数化 (也叫几何预解式 (geometric resolution)，参见 [21-24])。本文将采用后者。

令 V 是一个等维复代数簇，其维数是 r ($r \geq 0$)，次数是 δ。V 的一个有理参数化表示由如下多项式组成：

- $\mathbb{Q}[T_1, \ldots, T_{r+1}]$ 中的一组多项式 $(w, v_1, \ldots, v_n)$，满足: $T_1, \ldots, T_{r+1}$ 是新的变元；w 无平方，首系数为 1，全次数为 δ；对于 $1 \leq i \leq n$，有不等式 $\deg(v_i, T_{r+1}) < \deg(w, T_{r+1})$。
- $\boldsymbol{\ell} = (\lambda_1, \ldots, \lambda_{r+1})$，其中每个 λ_i 是 $X_1, \ldots, X_n$ 的线性组合，满足 $\lambda_i(v_1, \ldots, v_n) = T_i \frac{\partial w}{\partial T_{r+1}} \mod w$。

我们把这样的有理参数化表示记为 $\mathscr{Q} = ((w, v_1, \ldots, v_n), \boldsymbol{\ell})$，称 $\mathscr{Q}$ 是 $\mathbb{Q}[T_1, \ldots, T_{r+1}]$ 中的一个次数为 δ 的 r 维有理参数化表示。复代数簇 V 是如下集合在 $\mathbb{C}^n$ 中的 Zariski 闭包：

$$\left\{(x_1, \ldots, x_n) \in \mathbb{C}^n \mid \exists \vartheta \in \mathbb{C}^{r+1}, w(\vartheta) = 0, \frac{\partial w}{\partial T_{r+1}}(\vartheta) \neq 0, x_i = \frac{v_i}{\partial w / \partial T_{r+1}}(\vartheta)\right\}.$$

我们也称 $\mathscr{Q}$ 是复代数簇 V 的零化理想的有理参数化表示。

基于上述表示和 [25] 中计算复代数簇等维分解的算法，我们证明：对

于 $\mathbb{Q}[X_1,\ldots,X_n]$ 的一组多项式 $\boldsymbol{f}=(f_1,\ldots,f_s)$，令 r 等于 $\langle \boldsymbol{f}\rangle$ 的维数，存在一个概率算法计算 $\sqrt[re]{\langle \boldsymbol{f}\rangle}$ 所有极小素理想的有理参数化表示，其复杂度是 $s^{O(1)}(nD)^{O(nr2^r)}$。

1.2 多项式全局最优化

1.2.1 问题概述与研究现状

本文考虑的第二个问题是如何计算多项式函数在实代数簇上的全局最优值。多项式全局最优化是实代数几何应用较多的一个领域，而这一问题本身在很多工程领域也有广泛的应用，比如控制论 [26]，运筹优化 [27]，信号处理 [28]，计算机视觉 [29]，等等。

多项式全局最优化的基本形式是：给定多项式 f 和半代数集

$$S=\{x\in\mathbb{R}^n \mid g_1(x)\geq 0,\ldots,g_s(x)\geq 0\},$$

其中 $f,g_1,\ldots,g_s\in\mathbb{R}[X_1,\ldots,X_n]$，求 f 在 S 上的全局下确界：

$$f^*=\inf_{x\in S} f(x). \tag{1-1}$$

Putinar 在 [30] 给出了紧致集上正多项式的有效表示，Lasserre [31] 应用这个结果，对于 S 是紧致集的情形，提出了基于 SDP 求解 (1-1) 的数值算法。此后，对于 S 非紧致的情形，也有一系列的工作。假设 S 是非奇异的，且 f^* 在 S 上是可达的，即存在 $x\in S$ 使得 $f(x)=f^*$，聂家旺等 [32-34] 给出了雅可比 SDP 松弛方法来求解 (1-1)。Bucero 和 Mourrain 在 [35] 中也考虑了这一情形。去掉 f^* 可达的假设，Schweighofer [36] 引入梯度触 (gradient tentacle) 来处理没有限制条件的多项式全局最优化问题，即可行域 $S=\mathbb{R}^n$；Hà 和 Phạm [37, 38] 引入截断切簇 (truncated tangency variety) 来处理可行域 S 非奇异的情形。通过将梯度触和截断切簇替换为极簇 (polar variety)，郭峰等 [39, 40] 改进了 [36-38] 的结果。

此外，也有针对优化问题 (1-1) 的符号算法。一种经典的方法是将 (1-1) 转化为量词消去问题，然后用柱形代数分解 (cylindrical algebraic decomposition) 算法 [41] 求解。这个算法可以处理一般的情形，后续也有很多的工作对这个算法进行改进 (参见 [42-45])。它的复杂度关于变元个数是双指数的。在实际

计算中，它能处理的非平凡问题涉及的变元个数通常不超过 4 个。假设输入满足一定的条件，Hong 和 Safey El Din [46, 47] 对量词消去问题也给出了一个算法，这个算法能求解此前基于柱形代数分解算法实现的软件包无法计算的问题。在 [48, Section 14.2] 中，Basu 等基于量词消去给出了一个求解 (1-1) 的算法，其复杂度是 $s^{2n+1}D^{O(n)}$，其中 $D = \max\{\deg f, \deg g_1, \ldots, \deg g_s\}$。然而这个算法使用了无穷小形变 (infinitesimal deformation) 等技巧，所以在实际计算当中，这个算法在复杂度上的优势并未得到体现。

Kurdyda 等 [49] 证明了 $\mathbb{R}^n$ 上多项式映射的广义关键值集合是零测集。在此基础上，Safey El Din [50] 针对 S 等于 $\mathbb{R}^n$ 的情形，结合极簇的性质，给出了复杂度为 $O(n^7D^{4n})$ 的符号算法求解问题 (1-1)，其中，算法要求目标函数 f 的系数都是有理数。Greuet 和 Safey El Din [51] 推广了上述结果。假设 $f, g_1, \ldots, g_s$ 都是有理系数多项式，集合 S 的定义式中只包含等式，$g_1, \ldots, g_s$ 生成的理想是根理想且其复代数簇只包含有限多个奇异点，Greuet 和 Safey El Din [51] 给出了一个概率算法求解问题 (1-1)，这个概率算法的复杂度本质上是 $(sD)^{3n}$。

1.2.2 主要成果

本文应用多项式映射的广义关键值的性质来求解多项式全局最优化问题。

令 $G = \{g_1, \ldots, g_s\}$ 是 $\mathbb{R}[X] = \mathbb{R}[X_1, \ldots, X_n]$ 中一组多项式，$\mathbf{V}_{\mathbb{R}}(G)$ 是 G 的实代数簇。假设 $V = \mathbf{V}_{\mathbb{R}}(G)$ 是等维的，它的维数是 d。将 V 中所有在 d 维非奇异的点构成的集合记为 $\mathrm{Reg}(V)$，令 $M = \mathrm{Reg}(V)$。

给定多项式映射 $f : V \to \mathbb{R}^m$，记 $f|_M$ 为 f 限制在 M 上的映射，映射 $f|_M$ 的广义关键值集合是：

$$K(f, M) = \{y \in \mathbb{R}^m \mid \exists\, x_l \in M,\ \text{s.t. } f(x_l) \to y \text{ 且 } (1 + \|x_l\|)v(df(x_l), T_{x_l}M) \to 0\}.$$

对于 $y \in \mathbb{R}^m$，如果 f 在 y 的某个开邻域上是一个光滑纤维化 (fibration) (对应的纤维 (fiber) 可以是空集)，则称 y 为 f 的一个典型值 (typical value)，否则称 y 为 f 的非典型值 (atypical value)。用 $B(f)$ 表示 f 的所有非典型值构成的集合。$B(f)$ 称为 f 的分歧集 (bifurcation set)。对于映射 $f|_M$，记 $B(f, M) = B(f|_M)$。如

果 V 是非奇异的，即 $M = V$，那么 $B(f, M)$ 包含在 $K(f, M)$ 中 [52, Theorem 6.1]，这个包含关系为 [50] 中的算法奠定了理论基础。然而，当 V 不等于 M 时，下述例子说明这个包含关系可能不再成立。

例 1.2.1 考虑下面的曲线：

$$V = \left\{(x, y) \in \mathbb{R}^2 \mid x^4(y^2+1) - y^2(1+y) = 0\right\}.$$

令 $f : V \to \mathbb{R}$ 是从 V 到 y 轴的投射，即 $f(x, y) = y$。

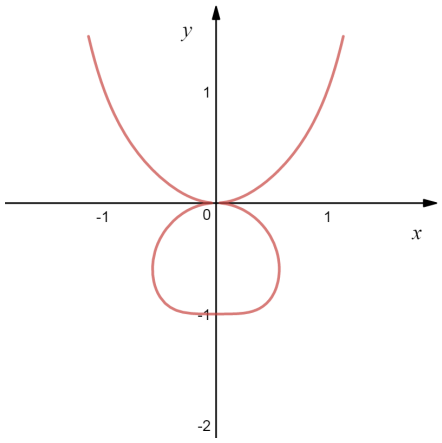


图 1.1　例 1.2.1

这里，$M = \mathrm{Reg}(V) = V \setminus \{(0,0)\}$，$K(f, M) = \{-1\}$，但 $B(f, M) = \{-1, 0\}$。因此 $B(f, M) \not\subset K(f, M)$。

为了刻画集合 $B(f, M)$，我们引入一个新的集合：

$$K_1(f, M) = \{y \in \mathbb{R}^m \mid \exists\, x_l \in M, x \in V \setminus M, x_l \to x \text{ s.t.}$$
$$f(x_l) \to y \text{ 且} v(df(x_l), T_{x_l}M) \to 0\}.$$

例 1.2.1 (续) 显然，$K_1(f, M) = \{0\}$。因此，我们有

$$K(f, M) \cup K_1(f, M) = B(f, M).$$

注意到，$f^* = \inf_{x \in V} f(x) = -1$。

但是，下述例子表明 $K(f, M)$ 与 $K_1(f, M)$ 的并集仍然不足以刻画集合 $B(f, M)$。

例 1.2.2　考虑 $\mathbb{R}^2$ 中的曲线：

$$V = \left\{(x,y) \in \mathbb{R}^2 \mid x^3 + x^2 - y^2 = 0\right\}.$$

令 $f : V \to \mathbb{R}$ 是从 V 到 y 轴的投射，即 $f(x,y) = y$。

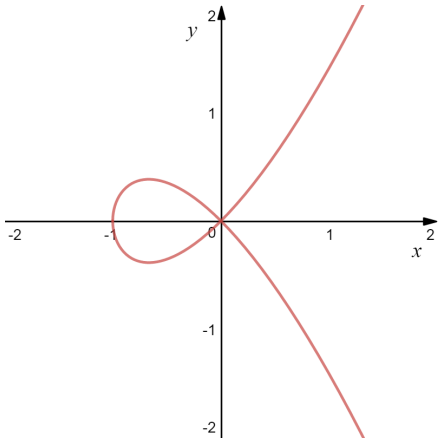


图 1.2　例 1.2.2

这里，$M = \mathrm{Reg}(V) = V \setminus \{(0,0)\}$，

$$K(f,M) \cup K_1(f,M) = \left\{\pm\left(2\sqrt{3}\right)/9\right\}.$$

然而，$B(f,M)$ 等于 $\left\{\pm\left(2\sqrt{3}\right)/9, 0\right\}$，不包含在 $K(f,M) \cup K_1(f,M)$ 中。

尽管如此，我们发现即使不能完全刻画 $B(f,M)$，基于 $K(f,M)$ 和 $K_1(f,M)$ 的性质，多项式全局最优化问题依然可解。

Jelonek 和 Kurdyka [53] 证明如果 $\mathbf{V}_{\mathbb{R}}(G)$ 是等维非奇异的，那么 $K(f, \mathbf{V}_{\mathbb{R}}(G))$ 是 $\mathbb{R}^m$ 中维数小于 m 的半代数闭集，且等于一个有理映射的像的闭包。

去掉非奇异的条件，假设 $\mathbf{V}_{\mathbb{R}}(G)$ 是等维的，令 $M = \mathrm{Reg}(\mathbf{V}_{\mathbb{R}}(G))$，我们证明 $K(f,M) \cup K_1(f,M)$ 是 $\mathbb{R}^m$ 中维数小于 m 的半代数闭集，且仍等于上述 [53] 中定义的一个有理映射的像的闭包。

然后令 $m = 1$，我们证明 $\inf_{x \in \mathbf{V}_{\mathbb{R}}(G)} f(x)$ 包含在 $K(f,M)$ 或 $\mathbf{V}_{\mathbb{R}}(G) \setminus M$ 的像的闭包中。注意到 $\mathbf{V}_{\mathbb{R}}(G) \setminus M$ 也是一个实代数簇且它的维数小于 $\mathbf{V}_{\mathbb{R}}(G)$ 的维数。于是，通过计算 $K(f,M)$，然后对 $\mathbf{V}_{\mathbb{R}}(G) \setminus M$ 的所有等维分支做递归，我

们可以得到一个有限集合使得它包含 $\inf_{x\in\mathbf{V}_{\mathbb{R}}(G)} f(x)$。由此，给出一个算法用于计算多项式函数在任意实代数簇上的全局最优值。

最后，我们证明，一般的基本半代数闭集上的多项式全局最优化问题 (1-1) 可以转化有限个子问题，其中每个子问题的可行域都是实代数簇。因此，通过多次调用上面的算法，即可求解 (1-1)。

1.3 论文结构

第二章，先介绍代数几何中的一些基本概念及其性质，包括理想、复代数簇、奇异点、Zariski 拓扑等。然后介绍实代数几何中特有的一些概念及其性质，包括实代数簇、实根理想、半代数集、半代数映射等。

第三章，给出光滑情形下实根理想生成元的次数上界，分析计算实根理想的复杂度。如果给定的多项式的复代数簇是光滑的，那么计算实根理想的复杂度关于变元个数是单指数的。对于一般的情形，计算实根理想的有理参数化表示的复杂度关于输入多项式系统的维数是双指数的；假定输入多项式系统的维数是固定的，那么这个复杂度关于变元的个数是单指数的。

第四章，引入一个新的集合用于求解多项式全局最优化问题，证明这个集合的勒贝格测度为零。更进一步，证明这个集合与广义关键值的并集是一个勒贝格测度为零的半代数闭集，且等于一个有理映射的像的闭包。然后，给出一个算法用于计算多项式函数在任意实代数簇上的全局最优值，最后把这个算法推广到可行域为基本半代数闭集的情形。

第五章是对全文内容的总结与展望。

第 2 章　预备知识

在这一章，我们首先介绍多项式理想及其基本性质，然后介绍多项式理想与复代数簇之间的对应关系。

2.1　代数几何基础

我们用 $\mathbb{N}$，$\mathbb{Q}$，$\mathbb{R}$ 和 $\mathbb{C}$ 分别表示自然数、有理数域、实数域和复数域。

令 $\mathbb{K}$ 是一个特征为零的数域，$\mathbb{K}$ 上的 n 元多项式环记为 $\mathbb{K}[X_1,\ldots,X_n]$。为简化符号，我们记 $\mathbb{K}[X]=\mathbb{K}[X_1,\ldots,X_n]$。

定义 2.1.1 设 I 是 $\mathbb{K}[X]$ 的一个子集。如果 I 满足：

(i) $0\in I$；

(ii) 若 $f\in I, g\in I$，则 $f+g\in I$；

(iii) 若 $f\in I, g\in I$，则 $fg\in I$，

则称 I 是 $\mathbb{K}[X]$ 的一个理想。

令 F 是 $\mathbb{K}[X]$ 的一个子集，F 在 $\mathbb{K}[X]$ 中生成的理想记作 $\langle F\rangle$，它是 $\mathbb{K}[X]$ 中包含 F 的最小理想。

定义 2.1.2 令 I 是 $\mathbb{K}[X]$ 中的一个理想，I 的根理想定义为：

$$\sqrt{I}=\{f\in\mathbb{K}[X]\mid \exists\, m\in\mathbb{N}\ \text{s.t.}\ f^m\in I\}.$$

定义 2.1.3 令 $I\subsetneq\mathbb{K}[X]$ 是一个理想，如果满足：

(i) $f,g\in\mathbb{K}[X], fg\in I\Rightarrow \exists m\in\mathbb{N}, s.t. f\in I$ 或 $g^m\in I$，则称 I 是 $\mathbb{K}[X]$ 的一个准素理想；

(ii) $f,g\in\mathbb{K}[X], fg\in I\Rightarrow f\in I$ 或 $g\in I$，则称 I 是 $\mathbb{K}[X]$ 的一个素理想；

(iii) $J \supsetneq I$ 且 J 是 $\mathbb{K}[X]$ 的一个理想 $\Rightarrow J = \mathbb{K}[X]$，则称 I 是 $\mathbb{K}[X]$ 的一个极大理想。

定义 2.1.4 令 I 是 $\mathbb{K}[X]$ 中的一个理想，I 的维数定义为

$$\dim I = \max\left\{l \in \mathbb{N} \mid I \subseteq P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_l \subsetneq \mathbb{K}[X],\ P_i \text{ 是素理想}\right\}.$$

对于 $\mathbb{K}[X]$ 中的一个理想 I，如果存在一个有限集合 $G \subset \mathbb{K}[X]$ 使得 $I = \langle G \rangle$，则称理想 I 是有限生成的。

定理 2.1.5 (Hilbert **基定理**) [54, 77 页，Chapter 2 §5, Theorem 4] $\mathbb{K}[X]$ 中的理想都是有限生成的。

对于 $\mathbb{K}[X]$ 中的一个理想 I，将 I 写成一些准素理想的交，即：$I = \bigcap_{i=1}^{r} Q_i$，其中 Q_i 是 $\mathbb{K}[X]$ 中的准素理想，这样的写法称为 I 的一个准素分解。更进一步，如果 $\sqrt{Q_i}$ 都互不相同，且 $Q_i \not\supset \bigcap_{j\neq i} Q_j$，则称这个准素分解是极小的。

定理 2.1.6 [54, 229 页，Chapter 4 §8, Theorem 7] $\mathbb{K}[X]$ 中的每一个理想 I 都有极小准素分解。

假设理想 I 有极小准素分解：$I = \bigcap_{i=1}^{r} Q_i$，如果每个 $\sqrt{Q_i}$ 的维数都相等，则称理想 I 是等维的；假设 I 的维数是 d，对于 $0 \le j \le d$，令 I_j 等于所有 j 维准素理想 Q_i 的交，理想 I_j 称为 I 的 j 维等维部分 [参见 55, 259 页，Definition 4.1.1, 4.4.5]。

定义 2.1.7 令 $f_1, \ldots, f_s$ 是 $\mathbb{K}[X]$ 中的多项式。定义：

$$\mathbf{V}_{\mathbb{C}}(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in \mathbb{C}^n \mid f_i(a_1, \ldots, a_n) = 0,\ \forall 1 \le i \le s\}, \qquad (2\text{-}1)$$

$\mathbf{V}_{\mathbb{C}}(f_1, \ldots, f_s)$ 叫做 $f_1, \ldots, f_s$ 在 $\mathbb{C}^n$ 中的复代数簇[①]。

对于 $\mathbb{C}^n$ 的一个子集 V，如果存在集合 $F \subset \mathbb{K}[X]$ 使得 $V = \mathbf{V}_{\mathbb{C}}(F)$，则称 V 是一个复代数簇。在 $\mathbb{C}^n$ 上定义一个拓扑使得其中的闭集都是复代数簇，这个拓扑称为 *Zariski* 拓扑。

① 很多文献中把 (2-1) 中的集合直接称作代数簇或代数集，即默认代数簇或代数集都是定义在复向量空间中的，于是也会把 $\mathbf{V}_{\mathbb{C}}(\cdot)$ 简写为 $\mathbf{V}(\cdot)$。但本文将在多处涉及到实向量空间中的代数簇，因此为避免混淆，采用记号 $\mathbf{V}_{\mathbb{C}}(\cdot)$ 和“复代数簇”来表示复空间中的代数簇。

定理 2.1.8 (Hilbert **零点定理**) 令 I 是 $\mathbb{K}[X]$ 中的一个理想，则 $\mathbf{I}(\mathbf{V}_{\mathbb{C}}(I)) = \sqrt{I}$。(参见 [54, 179 页，Chapter 4 §1, Theorem 2])

假设 V 是由 $\mathbb{K}[X]$ 中多项式定义的一个复代数簇。如果存在 $\mathbb{K}[X]$ 的两个子集 F_1 和 F_2 满足 $\mathbf{V}_{\mathbb{C}}(F_1) \neq \mathbf{V}_{\mathbb{C}}(F_2)$，使得 V 等于 $\mathbf{V}_{\mathbb{C}}(F_1)$ 和 $\mathbf{V}_{\mathbb{C}}(F_2)$ 的并，则称 V 在 $\mathbb{K}$ 是上可约的，否则称 V 在 $\mathbb{K}$ 上是不可约的。如果多项式环的系数域 $\mathbb{K}$ 是事先明确或固定的，那么也简单地称 V 是可约或不可约的。

定义 2.1.9 令 S 是 $\mathbb{C}^n$ 的一个子集，定义

$$\mathbf{I}(S) = \{f \in \mathbb{K}[X] \mid f(a_1, \ldots, a_n) = 0,\ \forall (a_1, \ldots, a_n) \in S\},$$

$\mathbf{I}(S)$ 称为 S 的零化理想 (vanishing ideal)，或简称为 S 的理想。

定理 2.1.10 [54, 207 页，Chapter 4 §5, Proposition 3] 令 V 是 $\mathbb{K}[X]$ 中多项式定义的一个复代数簇。则 V 在 $\mathbb{K}$ 上不可约当且仅当 $\mathbf{I}(V)$ 是 $\mathbb{K}[X]$ 中的素理想。

令 V 是 $\mathbb{K}[X]$ 中多项式定义的一个复代数簇。将 V 写成一些不可约复代数簇的并，即：

$$V = V_1 \cup \cdots \cup V_r,$$

其中每个 V_i 都是不可约复代数簇。如果对任意 $i \neq j$ 有 $V_i \not\subset V_j$，则称这个分解是 V 的极小不可约分解。

定理 2.1.11 [54, 215 页，Chapter 4 §6, Theorem 4] 每个复代数 V 簇都有极小不可约分解：$V = \bigcup_{i=1}^{r} V_i$，其中 V_i 都是不可约复代数簇。如果不计 $V_1, \ldots, V_r$ 的顺序，则这个分解是唯一的。

定义 2.1.12 对于 $\mathbb{C}^n$ 中的一个复代数簇 V，V 的维数定义为它的零化理想 $\mathbf{I}(V)$ 的维数，即

$$\dim V = \dim \mathbf{I}(V).$$

令 $V = \bigcup_{i=1}^{r} V_i$ 是 V 的极小不可约分解，则每个 V_i 称为 V 的一个不可约分支。如果 V 的所有不可约分支的维数都相等，则称 V 是等维的。

假设一个复代数簇 $V \subset \mathbb{C}^n$ 的维数是 d，将 V 分解为：$V = \bigcup_{i=0}^{d} V_i$，其中 V_i 等于空集或 V_i 是一个 i 维等维的复代数簇，而且对于 $i \neq j$ 有 $V_i \not\subset V_j$，这样的分解称为 V 的极小等维分解，非空的 V_i 称为 V 的（i 维）等维分支。

下面我们定义复代数簇的次数（参见 [56, 165 页] 或 [22, 57]）。令 V 是 $\mathbb{C}^n$ 中的一个不可约复代数簇，V 的维数是 r。V 的（几何）次数定义为：

$$\deg V = \sup\left\{\#(H_1 \cap \ldots \cap H_r \cap V) < \infty \mid H_1, \ldots, H_r \text{是}\mathbb{C}^n \text{中的超平面}\right\},$$

其中 # 表示势函数。如果 V 是可约的，那么它的（几何）次数则定义为它所有不可约分支的次数的和。

定义 2.1.13 [54, 516 页，Chapter 9 §6，Definition 1，Proposition 2] 设 $V \subset \mathbb{C}^n$ 是一个复代数簇，$\mathbf{I}(V) = \langle f_1, \ldots, f_s \rangle$。对于 V 中的一点 p，V 在 p 点的切空间定义为：

$$T_p(V) = \bigcap_{j=1}^{s} \left\{ x \in \mathbb{C}^n \,\Big|\, \sum_{i=1}^{n} \frac{\partial f_j}{\partial X_i}(p) x_i = 0 \right\}. \tag{2-2}$$

定义 2.1.14 [54, 520 页，Chapter 9 §6，Definition 6] 令 $V \subset \mathbb{C}^n$ 是一个复代数簇。对于 $p \in V$，V 在 p 点的维数定义为 V 中包含 p 的不可约分支的最大维数，这个维数记作 $\dim_p V$。

定义 2.1.15 [①] [54, 520 页，Chapter 9 §6，Definition 7] 令 $V \subset \mathbb{C}^n$ 是一个复代数簇。对于 $p \in V$，如果 $\dim T_p(V) = \dim_p V$，则称 p 是 V 的一个非奇异 (nonsingular) 点（或光滑 (smooth) 点）。否则，称 p 为 V 的奇异 (singular) 点。

一个复代数簇 V 的所有奇异点构成的集合称为 V 的奇异轨迹 (singular locus)，记为 $\mathrm{Sing}(V)$[参见 54, 521 页，Chapter 9 §6，Theorem 8]。如果 V 中所有的点都是非奇异的（或光滑的），则称 V 是非奇异的（或光滑的）。

命题 2.1.16 [54, 521 页，Chapter 9 §6，Theorem 8] 令 V 是一个复代数簇，记 $\mathrm{Sing}(V)$ 为 V 的奇异轨迹。则：

① 在文献 [54] 中，定义 2.1.15 并不局限于复代数簇。对于 $\mathbb{R}^n$ 中的实代数簇，只需将定义 2.1.13，定义 2.1.14 和定义 2.1.15 中的 $\mathbb{C}^n$ 替换成 $\mathbb{R}^n$ 即可。然而，这与文献 [58] 中关于非等维实代数簇的非奇异性的定义不一致（见定义 2.2.8）。考虑到文献 [58] 是针对实代数几何的专著，所以对于实代数簇的非奇异性，我们将采用文献 [58] 中的定义。

(i) $\mathrm{Sing}(V)$ 是一个复代数簇；

(ii) 如果 $p \in \mathrm{Sing}(V)$，则 $\dim T_p(V) > \dim_p V$；

(iii) $\mathrm{Sing}(V)$ 不包含 V 的任何一个不可约分支；

(iv) 如果 V_i 和 V_j 是 V 的两个不同的不可约分支，则 $V_i \cap V_j \subset \mathrm{Sing}(V)$。

定理 2.1.17 (**雅可比准则** (Jacobian Criterion)) [59, 405 页，Corollary 16.20] 令 V 是 $\mathbb{C}^n$ 中的一个等维复代数簇。假设 V 的零化理想 $\mathbf{I}(V) = \langle f_1, \ldots, f_s \rangle$，且 $\mathbf{I}(V)$ 的维数是 d。那么 V 中的一点 p 是非奇异的当且仅当 $f_1, \ldots, f_s$ 关于 $X_1, \ldots, X_n$ 的雅可比矩阵在 p 处的秩为 $n - d$。

2.2　实代数几何基础

令 $\mathbb{K}$ 是包含在 $\mathbb{R}$ 中的一个实域，与上一节相同，$\mathbb{K}$ 上的 n 元多项式环记为 $\mathbb{K}[X] = \mathbb{K}[X_1, \ldots, X_n]$。

定义 2.2.1 令 $f_1, \ldots, f_s$ 是 $\mathbb{K}[X]$ 中的多项式。定义：

$$\mathbf{V}_{\mathbb{R}}(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in \mathbb{R}^n \mid f_i(a_1, \ldots, a_n) = 0,\ \forall 1 \le i \le s\}, \tag{2-3}$$

$\mathbf{V}_{\mathbb{R}}(f_1, \ldots, f_s)$ 叫做 $f_1, \ldots, f_s$ 在 $\mathbb{R}^n$ 中的实代数集或实代数簇。

对于 $\mathbb{R}^n$ 的一个子集 V，如果存在集合 $F \subset \mathbb{K}[X]$ 使得 $V = \mathbf{V}_{\mathbb{R}}(F)$，则称 V 是一个实代数集或实代数簇。

上一节中针对复代数簇定义的“不可约、维数、等维”的概念，以及定理 2.1.10 和 2.1.11 都可以直接推广到实代数簇上。此外，在 $\mathbb{C}^n$ 上定义的 Zariski 拓扑也可以直接推广到 $\mathbb{R}^n$ 上。所有推广的细节可参阅 [58, Chapter 2-4]。下面介绍实代数几何特有的概念及其相关性质。

命题 2.2.2 [58, 24 页，Proposition 2.1.3] 实代数集都可由单个多项式定义。

定义 2.2.3 给定 $\mathbb{K}[X]$ 中的一个理想 I，定义 I 的实根理想为 (参见 [1, Definition 2.1] 或 [58, 85 页])：

$$\sqrt[re]{I} = \left\{ g \in \mathbb{K}[X] \mid g^{2m} + \sum_{i=1}^{l} a_i^2 \in \langle \boldsymbol{f} \rangle,\ \text{其中} m, l \in \mathbb{N},\ a_i \in \mathbb{K}[X] \right\}. \tag{2-4}$$

如果 $I = \sqrt[re]{I}$，则称理想 I 是实的。

命题 2.2.4 一个实理想的所有极小素理想都是实的。(参见 [1, Proposition 1] 或 [2, Lemma 2.3])

定理 2.2.5 (**实零点定理** (Real Nullstellensatz)) 令 I 是 $\mathbb{K}[X]$ 中的一个理想，则 $\mathbf{I}(\mathbf{V}_{\mathbb{R}}(I)) = \sqrt[re]{I}$。(参见 [2, Theorem 2.8] 或 [58, 86 页，Corollary 4.1.8])

定义 2.2.6 [58, 65 页，Definition 3.3.3] 令 $V \subset \mathbb{R}^n$ 是一个实代数簇，$\mathbf{I}(V) = \langle f_1, \ldots, f_s \rangle$。对于 V 中的一点 p，V 在 p 处的 Zariski 切空间定义为：

$$T_p^{Zar}(V) = \bigcap_{j=1}^{s} \left\{ x \in \mathbb{R}^n \,\middle|\, \sum_{i=1}^{n} \frac{\partial f_j}{\partial X_i}(p) x_i = 0 \right\}. \tag{2-5}$$

定义 2.2.7 [58, 66 页，Definition 3.3.4] 令 $V \subset \mathbb{R}^n$ 是一个不可约实代数簇。对于 V 中的一点 p，如果 $\dim T_p^{Zar}(V) = \dim V$，则称 p 是 V 的非奇异点。如果 V 中的所有点都是非奇异的，则称 V 是非奇异的。

定义 2.2.8 [①] 令 V 是一个 d 维的实代数簇。对于 $p \in V$，如果 V 有唯一的 d 维不可约分支 V' 包含 p，且 p 是 V' 的非奇异点，则称 p 在 d 维是非奇异的 (nonsingular in dimension d)。如果 V 中所有的点都在 d 维是非奇异的，则称 V 是非奇异的。

令 V 是一个 d 维的实代数簇，V 中所有在 d 维非奇异的点构成就集合记为 $\mathrm{Reg}(V)$[参见 58, 69 页，Notation 3.3.13]。由定义 2.2.8，非奇异的实代数簇都必须是等维的。为了避免混淆，在本文中，对于非奇异的实代数簇，我们仍然强调其等维性，即使用“等维非奇异实代数簇”来表示上述定义中的“非奇异实代数簇”。

雅可比准则 (见定理 2.1.17) 对于等维的实代数簇也成立，为完整起见，我们再次叙述一遍：

定理 2.2.9 (**雅可比准则** (Jacobian Criterion)) [59, 405 页，Corollary 16.20] 令 V 是 $\mathbb{R}^n$ 中的一个等维实代数簇。假设 V 的零化理想 $\mathbf{I}(V)$ 等于 $\langle f_1, \ldots, f_s \rangle$，且

① 在定义 2.1.15 的脚注中我们提到过，定义 2.2.8 与文献 [54] 中关于非等维实代数簇的非奇异性的定义不完全一致。在本文中，对于实代数簇，都将采用定义 2.2.8。需要指出的是，对于等维的实代数簇，这两个定义是等价的。因此，为避免混淆，本文中提到的非奇异实代数簇都只指针对等维实代数簇。

$\mathbf{I}(V)$ 的维数是 d。那么 V 中的一点 p 在 d 维是非奇异的当且仅当 $f_1,\ldots,f_s$ 关于 $X_1,\ldots,X_n$ 的雅可比矩阵在 p 处的秩为 $n-d$。

命题 2.2.10 [58, 69 页，Proposition 3.3.14] 令 V 是 $\mathbb{R}^n$ 中的一个 d 维实代数簇，则 $V \setminus \mathrm{Reg}(V)$ 也是一个实代数簇且其维数小于 d。

定义 2.2.11 [58, 24 页，Definition 2.1.4] 如果 $\mathbb{R}^n$ 的一个子集 S 可写成如下形式：

$$S = \bigcup_{i=1}^{s} \bigcap_{j=1}^{r_i} \left\{ (a_1,\ldots,a_n) \in \mathbb{R}^n \mid f_{i,j} \ *_{i,j} \ 0 \right\},$$

其中 $f_{i,j} \in \mathbb{K}[X]$，$*_{i,j}$ 是 $<$ 或 $=$，则称 S 是 $\mathbb{R}^n$ 中的一个半代数集。

定义 2.2.12 [58, 50 页，Definition 2.8.1] 令 S 是 $\mathbb{R}^n$ 中的一个半代数集，S 的维数定义为它的零化理想 $\mathbf{I}(S)$ 的维数，即：

$$\dim S = \dim \mathbf{I}(S).$$

定理 2.2.13 [58, 26 页，Theorem 2.2.1] 令 S 是 $\mathbb{R}^{n+1}$ 中的一个半代数集，$\pi : \mathbb{R}^{n+1} \to \mathbb{R}^n$ 是投射到前 n 个坐标的映射，则 $\pi(S)$ 也是 $\mathbb{R}^n$ 中的一个半代数集。

命题 2.2.14 [58, 27 页，Proposition 2.2.2] 一个半代数集的闭包和内部都是半代数集。

定义 2.2.15 [58, 28 页，Definition 2.2.5] 令 $A \subset \mathbb{R}^m$ 和 $B \subset \mathbb{R}^n$ 是两个半代数集。如果一个映射 $f : A \to B$ 的图 (graph) 是 $\mathbb{R}^{m+n}$ 中的一个半代数集，则称 f 是从 A 到 B 的半代数映射。

命题 2.2.16 [58, 28-29 页，Proposition 2.2.6(i), 2.2.7] 令 A, B, C 是三个半代数集，$f : A \to B$ 和 $g : B \to C$ 是半代数映射。则 $f \circ g$ 也是一个半代数映射。对于半代数集 $S \subset A$ 和半代数集 $T \subset B$，S 的像 $f(S)$ 和 T 的原像 $f^{-1}(T)$ 都是半代数集。

定义 2.2.17 [58, 29 页，Proposition 2.2.8] 令 A 是 $\mathbb{R}^n$ 中的非空半代数集。对于任一 $x \in \mathbb{R}^n$，x 到 A 的距离定义为：

$$\mathrm{dist}(x, A) = \inf\{ \|x - y\| \mid y \in A \}.$$

距离函数 $\mathrm{dist}: x \mapsto \mathrm{dist}(x, A)$ 是从 $\mathbb{R}^n$ 到 $\mathbb{R}$ 的一个连续的半代数函数。如果 $x \in \mathrm{cl}(A)$，那么 $\mathrm{dist}(x, A) = 0$，否则 $\mathrm{dist}(x, A) > 0$。这里，$\mathrm{cl}(A)$ 表示 A 的闭包。

定理 2.2.18 [58, 38 页, Theorem 2.5.5] 令 A 是 $\mathbb{R}^n$ 中的一个半代数集，$x \in \mathrm{cl}(A)$。存在一个连续的半代数映射 $f: [0,1] \to \mathbb{R}^n$ 使得 $f(0) = x$ 且 $f((0,1]) \subset A$。

定理 2.2.19 (Łojasiewicz **不等式**) [58, 44 页，Corollary 2.6.7] 令 A 是 $\mathbb{R}^n$ 中的一个有界的半代数闭集，f 和 g 是从 A 到 $\mathbb{R}$ 上的连续半代数函数。如果 $f^{-1}(0) \subset g^{-1}(0)$，则存在正整数 L 和常数 $c \in \mathbb{R}$，使得 $|g(x)|^L \leq c|f(x)|, \forall x \in A$。

第 3 章　实根理想的计算

3.1　问题和背景

给定 $\mathbb{Q}[X]=\mathbb{Q}[X_1,\ldots,X_n]$ 中的一组多项式 $\boldsymbol{f}=(f_1,\ldots,f_s)$, 记 $\langle \boldsymbol{f}\rangle$ 为 $\boldsymbol{f}$ 在 $\mathbb{Q}[X]$ 中生成的理想。$\langle \boldsymbol{f}\rangle$ 的实根理想是 (见定义 2.2.3)：

$$\sqrt[re]{\langle \boldsymbol{f}\rangle}=\left\{g\in\mathbb{Q}[X]\mid g^{2m}+\sum_{i=1}^{l}a_i^2\in\langle \boldsymbol{f}\rangle,\ \text{其中}m,l\in\mathbb{N},\ a_i\in\mathbb{Q}[X]\right\}.$$

令 D 为 $\boldsymbol{f}$ 中多项式的最高次数。目前已有的计算实根理想的符号算法 [1, 2]，其输出多项式的次数上界是 $D^{2^{O(n^2)}}$，算术复杂度是关于 $D^{2^{O(n^2)}}$ 的多项式。另一方面，如果假定 $\boldsymbol{f}$ 的复代数簇是等维光滑的，那么存在复杂度为 $s(nd^n)^{O(1)}$ 的符号算法用于计算 $\langle \boldsymbol{f}\rangle$ 的根理想 [15]。

一个自然的问题是：若 $\boldsymbol{f}$ 的复代数簇是等维光滑的，是否也可以找到复杂度关于 n 为单指数的符号算法来计算 $\langle \boldsymbol{f}\rangle$ 的实根理想？

3.2　预备知识

3.2.1　实根理想的基本性质

这一章里，如无特别说明，考虑的多项式都是有理系数多项式，涉及的代数簇也假定是由某些有理系数多项式定义的。在考虑算法复杂度时，如果没有特别强调，所提到的复杂度也是指有理数域 $\mathbb{Q}$ 中的算术复杂度。

记 $\mathbb{Q}[X]=\mathbb{Q}[X_1,\ldots,X_n]$ 为有理数域上的 n 元多项式环。令 I 是 $\mathbb{Q}[X]$ 中的一个理想，S 是 $\mathbb{C}^n$ 中的子集。我们将使用如下记号：

- 理想 I 的复代数簇：$\mathbf{V}_{\mathbb{C}}(I)=\{x\in\mathbb{C}^n\mid f(x)=0,\ \forall f\in I\}$;
- 理想 I 的实代数簇：$\mathbf{V}_{\mathbb{R}}(I)=\mathbf{V}_{\mathbb{C}}(I)\cap\mathbb{R}^n$;
- 理想 I 的根理想：$\sqrt{I}=\{f\in\mathbb{Q}[X]\mid \exists\, m\in\mathbb{N}\ \text{s.t.}\ f^m\in I\}$;
- 集合 S 的零化理想：$\mathbf{I}(S)=\{f\in\mathbb{Q}[X]\mid f(x)=0,\ \forall x\in S\}$;
- 集合 S 在 $\mathbb{C}^n$ 中的 Zariski 闭包：包含 S 的最小的复代数簇，记作 $\mathrm{cl}_{\mathrm{Zar}}(S)$。

在这一章，如无特别声明，一个集合的 Zariski 闭包都指其在复空间中的 Zariski 闭包。

命题 3.2.1 假设 I 和 J 是 $\mathbb{Q}[X]$ 中的两个理想，则有

$$\sqrt[re]{I \cap J} = \sqrt[re]{I} \cap \sqrt[re]{J}.$$

证明 这个式子在 [1, 2] 中是直接给出来的。我们简短地证明一下。

首先，显然有 $\sqrt[re]{I \cap J} \subset \sqrt[re]{I} \cap \sqrt[re]{J}$。

反过来，假设 $f \in \sqrt[re]{I} \cap \sqrt[re]{J}$，则存在 $m, p \in \mathbb{N}$，$a_1 \ldots, a_k, b_1, \ldots, b_l \in \mathbb{Q}[X_1, \ldots, X_n]$ 使得

$$g_1 := f^{2m} + \sum_{i=1}^{k} a_i^2 \in I, g_2 := f^{2p} + \sum_{i=1}^{l} b_i^2 \in J.$$

故 $g_1 g_2 \in I \cap J$，因此 $f \in \sqrt[re]{I \cap J}$。 □

命题 3.2.2 令 I 是 $\mathbb{Q}[X]$ 中的一个素理想。那么 I 是实理想当且仅当 I 有一个非奇异的实零点。

证明 参见 [60, Theorem 12.6.1] 或 [58, 69 页，Proposition 3.3.16]。 □

命题 3.2.3 令 I 和 J 是 $\mathbb{Q}[X]$ 中的两个理想。对于 $\mathbb{K} = \mathbb{C}$ 或 $\mathbb{R}$，下述等式成立:

$$\mathbf{V}_{\mathbb{K}}(I \cap J) = \mathbf{V}_{\mathbb{K}}(I) \cup \mathbf{V}_{\mathbb{K}}(J).$$

证明 参见 [54, 196 页，Chapter 4 §3, Theorem 15]。 □

命题 3.2.4 对于 $\mathbb{C}^n$ 中的一个子集 S，它的 Zariski 闭包 $\mathrm{cl}_{\mathrm{Zar}}(S)$ 等于 $\mathbf{V}_{\mathbb{C}}(\mathbf{I}(S))$，且 S 的零化理想等于它的 Zariski 闭包的零化理想。

证明 参见 [54, 199 页，Chapter 4 §4]。 □

3.2.2　周形式

令 $\mathbb{P}^n$ 是复数域 $\mathbb{C}$ 上的 n 维射影空间，V 是 $\mathbb{P}^n$ 中的一个不可约射影代数簇，V 的维数是 r。对于 $i = 0, \ldots, r$, 记 $U_i = (U_{i0}, \ldots, U_{in})$ 为 $n+1$ 个新的变元，$U = (U_0, \ldots, U_r)$。令

$$L_i = U_{i0}x_0 + \ldots + U_{in}x_n,\ i = 0, \ldots, r.$$

那么存在唯一的（相差一个常数倍）多项式 $\mathcal{F}_V \in \mathbb{Q}[U]$ 使得对任意的 $u_0, \ldots, u_r \in \mathbb{C}^{n+1}$ 有：

$$\mathcal{F}_V(u_0, \ldots, u_r) = 0 \Longleftrightarrow V \cap \{L_0(u_0, x) = 0, \ldots, L_r(u_r, x) = 0\} \neq \emptyset,$$

其中 $L_i(u_i, x) = u_{i0}x_0 + \cdots + u_{in}x_n,\ i = 0, \ldots, r$。这个多项式 $\mathcal{F}_V$ 就称为射影代数簇 V 的周形式 [61, Chapter 3]。

假设 W 是 $\mathbb{P}^n$ 中的一个等维射影代数簇。令 $W = \bigcup_{i=1}^{s} W_i$ 是 V 的极小不可约分解。那么 V 的周形式定义为：

$$\mathcal{F}_W = \prod_{i=1}^{s} \mathcal{F}_{W_i},$$

其中 $\mathcal{F}_{W_i}$ 是 W_i 的周形式。

这个定义也可以推广到 $\mathbb{C}^n$ 中的等维仿射复代数簇。假设我们有 $\mathbb{Q}[X_1, \ldots, X_n]$ 中的一组多项式 $\boldsymbol{f} = (f_1, \ldots, f_s)$。记 f_i^h 为添加变量 X_0 得到的 f_i 的齐次化形式，$\boldsymbol{f}^h = (f_1^h, \ldots, f_s^h)$。那么仿射代数簇 $\mathbf{V}_{\mathbb{C}}(\boldsymbol{f})$ 等同于 $\mathbb{P}^n$ 的一个子集 $\mathbf{V}_{\mathbb{C}}(\boldsymbol{f}^h) \setminus \mathbf{V}_{\mathbb{C}}(X_0)$，并且 $\mathbf{V}_{\mathbb{C}}(\boldsymbol{f})$ 的射影闭包是包含 $\mathbf{V}_{\mathbb{C}}(\boldsymbol{f}^h) \setminus \mathbf{V}_{\mathbb{C}}(X_0)$ 的最小射影代数簇 [54, 418 页，Chapter 8 §4, Proposition 7]。$\mathbf{V}_{\mathbb{C}}(\boldsymbol{f})$ 的周形式就定义为它的射影闭包的周形式 [62, Section 1.1]。

3.3　光滑情形

3.3.1　生成元次数上界

命题 3.3.1　令 V 是 $\mathbb{C}^n$ 中的一个等维光滑复代数簇，记 $m = (n - \dim V)(1 + \dim V)$。则存在一组多项式 $g_1, \ldots, g_m \in \mathbb{Q}[X_1, \ldots, X_n]$ 满足 $\deg g_i \leq \deg V$ 使得 $g_1, \ldots, g_m$ 生成 V 的零化理想 $\mathbf{I}(V)$。

证明　参见 [15, Theorem 10]。　□

定理 3.3.2 令 I 是 $\mathbb{Q}[X_1,\ldots,X_n]$ 中的一个素理想，记 $m=(n-\dim I)(1+\dim I)$。那么 I 的实根理想有一组次数不高于 $\deg V$ 的生成元，且这组生成元的个数不超过 m。

证明 如果 I 的实代数簇 $\mathbf{V}_{\mathbb{R}}(I) = V\cap\mathbb{R}^n$ 是空集，那么 I 的实根理想等于 $\mathbf{I}(\mathbf{V}_{\mathbb{R}}(I))=\langle 1\rangle$。

如果 I 的实代数簇非空，则存 $x\in\mathbf{V}_{\mathbb{R}}(I)\subset V$，因为 V 是光滑的，所以 x 是 V 的一个光滑点。又因为且 I 是素理想，由雅可比准则，可知 x 也是 I 的非奇异点。根据命题 3.2.2，我们知道 I 是实的，即 I 的实根理想等于 I 本身。另一方面，I 是素理想意味着 I 等于 $\mathbf{I}(V)$，故 I 的实根理想等于 $\mathbf{I}(V)$。由命题 3.3.1可知，$\mathbf{I}(V)$ 有一组次数不高于 $\deg V$ 的生成元，且这组生成元的个数不超过 m。

□

定理 3.3.3 令 I 是 $\mathbb{Q}[X_1,\ldots,X_n]$ 中的一个理想。如果 I 的复代数簇 $V=\mathbf{V}_{\mathbb{C}}(I)$ 是光滑的，那么 I 的实根理想有一组次数不高于 $\deg V$ 的生成元。

证明 设 V 的极小不可约分解为 $V=\bigcup_{i=1}^{t}V_i$，记 $I_i=\mathbf{I}(V_i)$，则 $\sqrt{I}=\bigcap_{i=1}^{t}I_i$。此外，$I\subset\sqrt{I}\subset\sqrt[re]{I}$ 可推出 $\sqrt[re]{I}=\sqrt[re]{\sqrt{I}}$。于是由命题 3.2.1，有

$$\sqrt[re]{I}=\bigcap_{i=1}^{t}\sqrt[re]{I_i}. \tag{3-1}$$

根据定理 3.3.2, 每个实根理想 $\sqrt[re]{I_i}$ 都有一组次数不高于 $\deg V_i$ 的生成元，假设是 $\{g_1^{(i)},\ldots,g_{m_i}^{(i)}\}$，其中 $m_i=(n-\dim V_i)(1+\dim V_i)$。另一方面，因为 V 是光滑的，由命题 2.1.16 (iv) 可知，V 的所有不可约分支都两两不相交，即对任意的 $i,j\in\{1,\ldots,s\}, i\neq j$，有 $V_i\cap V_j=\emptyset$，故 $(V_i\cap\mathbb{R}^n)\cap(V_j\cap\mathbb{R}^n)=\emptyset$。因此，若 $i\neq j$ 则 $\sqrt[re]{I_i}+\sqrt[re]{I_j}=\langle 1\rangle$。于是下面的等式成立：

$$\bigcap_{i=1}^{t}\sqrt[re]{I_i}=\left\langle\left\{g_{i_1}^{(1)}\cdots g_{i_t}^{(t)}\mid 1\le i_1\le m_1,\ldots,1\le i_t\le m_t\right\}\right\rangle. \tag{3-2}$$

并且, $\deg(g_{i_1}^{(1)}\cdots g_{i_t}^{(t)})\le\deg V_1+\cdots+\deg V_t=\deg V$。结合 (3-1) 与 (3-2)，定理得证。

□

3.3.2　算法

令 $\boldsymbol{f} = (f_1, \ldots, f_s)$ 是 $\mathbb{Q}[X_1, \ldots, X_n]$ 中的一组多项式，假设 $\boldsymbol{f}$ 的复代数簇 $V = \mathbf{V}_{\mathbb{C}}(\boldsymbol{f})$ 是光滑的，记 $r = \dim V$。将 V 的极小等维分解写为 $V = \bigcup_{i=0}^{r} V_i$，其中 V_i 是 V 的 i-维等维分支或是空集。记 $f_1^h, \ldots, f_s^h$ 为添加变量 X_0 的 $f_1, \ldots, f_s$ 的齐次化形式。我们给出计算 $\sqrt[re]{\langle \boldsymbol{f} \rangle}$ 所有极小素理想的一个概率算法。下面是算法中要用到的几个子程序。

- PointsPerComponents. 输入一组多项式等式：$f_1 = 0, \ldots, f_s = 0$，输出包含有限个实点的集合 S 使得 S 与 $\mathbf{V}_{\mathbb{R}}(f_1, \ldots, f_s)$ 的每一个连通分支的交集都非空 [63-66]。
- Equidim. 输入一组齐次多项式 $f_1^h, \ldots, f_s^h, g \in \mathbb{Q}[X_0, \ldots, X_n]$，输出 $\mathbf{V}_{\mathbb{C}}(f_1^h, \ldots, f_s^h) \setminus \mathbf{V}_{\mathbb{C}}(g)$ 所有等维分支的周形式 [62, Subroutine 11]。
- Generators. 输入某个等维复代数簇 V_i 的周形式 $\mathcal{F}_{V_i}$，输出 $\mathbf{I}(V_i)$ 的一组次数不高于 $\deg V_i$ 的生成元 [15, Section 5]。

令 $V_i \subset \mathbb{C}^n$ 是 V 的一个等维分支，记 $V_i^h \subset \mathbb{P}^n$ 为 V_i 的射影闭包。令 $V_i = \bigcup_{j=1}^{m_i} V_{ij}$ 是 V_i 的极小不可约分解。那么 $V_i^h = \bigcup_{j=1}^{m_i} V_{ij}^h$，其中 V_{ij}^h 是 V_{ij} 的射影闭包。V_i 的周形式 $\mathcal{F}_{V_i}$ 可由 Equidim 计算得到。另外，根据周形式的定义，我们有 $\mathcal{F}_{V_i} = \prod_{j=1}^{m_i} \mathcal{F}_{V_{ij}}$。于是通过在 $\mathbb{Q}$ 上分解 $\mathcal{F}_{V_i}$，我们就能得到 V_i 所有不可约分支的周形式。现在，我们介绍用于计算 $\langle \boldsymbol{f} \rangle$ 的实根理想的所有极小素理想的算法。这里，假定输入的 $\boldsymbol{f}$ 满足条件：$\mathbf{V}_{\mathbb{C}}(\boldsymbol{f})$ 是光滑的复代数簇。

RealRadicalSmooth($\boldsymbol{f}$)

1. $S = \text{PointsPerComponents}(\boldsymbol{f} = 0)$;
2. if $S = \emptyset$, then return {1};
3. $\{\mathcal{F}_{V_0}, \ldots, \mathcal{F}_{V_r}\} = \text{Equidim}(\boldsymbol{f}^h, X_0)$;
4. for $0 \le i \le r$ do

   $\{\mathcal{F}_{V_{i1}}, \ldots, \mathcal{F}_{V_{im_i}}\} \leftarrow$ irreducible factors of $\mathcal{F}_{V_i}$;
5. $\Omega = \{\}$;
6. for $0 \le i \le r$ and $1 \le j \le m_i$ do

$G_{ij} = \mathsf{Generators}(\mathcal{F}_{V_{ij}})$;

if $\mathbf{V}_{\mathbb{C}}(G_{ij}) \cap S \neq \emptyset$ then $\Omega = \Omega \cup \{G_{ij}\}$;

7. return Ω.

定理 3.3.4 设 $\boldsymbol{f} = (f_1, \ldots, f_s)$ 是 $\mathbb{Q}[X_1, \ldots, X_n]$ 中的一组多项式，由一个直线型程序 (straight-line program, 简称 SLP) Γ 表示。记 $D = \max(\deg(f_i), i = 1, \ldots, s)$。假设 $\mathbf{V}_{\mathbb{C}}(\boldsymbol{f})$ 是光滑的，维数是 r，次数是 δ。算法 $\mathsf{RealRadicalSmooth}(\boldsymbol{f})$ 以 Γ 为输入，以概率 1 输出 $\sqrt[re]{\langle \boldsymbol{f} \rangle}$ 的每一个极小素理想的生成元，这些生成元的次数不高于 δ。在成功的情况下，这个算法的复杂度是 $(snD^n)^{O(1)}$。

证明 **概率分析：**这个算法的第 1,3,4,6 步用的是概率算法。整个算法的成功的概率依赖于在 $\mathbb{Q}^{n^{O(1)}}$ 中的随机取值，并且存在 $\mathbb{Q}^{n^{O(1)}}$ 的一个 Zariski 开集使得 RealRadicalSmooth 中涉及的概率算法都得到正确答案，由此 RealRadicalSmooth 将以概率 1 得到正确答案。下面我们假设第 1,3,4,6 步运算得到的结果都是正确的。

正确性：集合 S 中的点也叫作实代数集 $\mathbf{V}_{\mathbb{R}}(\boldsymbol{f})$ 的样本点，即对于 $\mathbf{V}_{\mathbb{R}}(\boldsymbol{f})$ 的任意一个连通分支 C，集合 S 至少包含 C 的一个点。因为 $\mathbf{V}_{\mathbb{C}}(\boldsymbol{f})$ 是光滑的，所以它的所有不可约分支都两两不相交（参见命题 2.1.16），因此 $\mathbf{V}_{\mathbb{R}}(\boldsymbol{f})$ 的所有不可约分支也两两不相交。故对于 $\mathbf{V}_{\mathbb{R}}(\boldsymbol{f})$ 的每一个连通分支 C，$\mathbf{V}_{\mathbb{R}}(\boldsymbol{f})$ 有且仅有一个不可约分支包含 C。令 $V_{ij} = \mathbf{V}_{\mathbb{C}}(G_{ij})$，我们证明 $V_{ij} \cap \mathbb{R}^n$ 非空当且仅当 $V_{ij} \cap S$ 非空。假设 $V_{ij} \cap \mathbb{R}^n$ 不等于空集，那么它至少包含 $\mathbf{V}_{\mathbb{R}}(\boldsymbol{f})$ 的一个连通分支，因此 $V_{ij} \cap S$ 也非空。反过来是显然的。又因为 $\mathbf{I}(V_{ij})$ 是素理想，由定理 3.3.2 可知，$\mathbf{I}(V_{ij})$ 是实的当且仅当 V_{ij} 包含一个实点，即 $V_{ij} \cap S$ 非空。由等式 (3-1) 可知，$\langle \boldsymbol{f} \rangle$ 的实根理想 $\sqrt[re]{\langle \boldsymbol{f} \rangle}$ 等于 $\bigcap_{V_{ij} \cap S \neq \emptyset} \mathbf{I}(V_{ij})$。最后，因为 V_{ij} 是 $\mathbf{V}_{\mathbb{C}}(\boldsymbol{f})$ 的不可约分支，故对于每个满足 $V_{ij} \cap S \neq \emptyset$ 的复代数簇 V_{ij}，$\mathbf{I}(V_{ij})$ 都是 $\sqrt[re]{\langle \boldsymbol{f} \rangle}$ 的一个极小素理想。

复杂度分析：记 Γ 的长度为 L。算法 RealRadicalSmooth 的第 1 步计算一个有限的集合 $S \subset \mathbb{R}^n$ 使得 S 与 $\mathbf{V}_{\mathbb{R}}(\boldsymbol{f})$ 的每一个连通分支的交都不为空。可实现这一步的算法参见 [63-67]。调用已有的 Maple 程序包 Raglib[66]，根据 [65, Theorem 4] 中关于 PointsPerComponents 复杂度的分析，可知第 1 步的复杂度是 $sL(nD^n)^{O(1)}$。

接下来，由 [62, Theorem 1]，计算 $\mathbf{V}_{\mathbb{C}}(f_1^h,\ldots,f_s^h)\setminus\mathbf{V}_{\mathbb{C}}(X_0)$ 所有等维分支的周形式的复杂度是 $sL(nD^n)^{O(1)}$。第 3 步得到的周形式 $\{\mathcal{F}_{V_0},\ldots,\mathcal{F}_{V_r}\}$ 由长度不大于 $sL(nD^n)^{O(1)}$ 的 SLP 表示 [62, Section 3.5]。

设表示 $\mathcal{F}_{V_i}$ 的 SLP 的长度为 L_i，那么在有理数域上分解 $\mathcal{F}_{V_i}$ 的复杂度是关于 L_i 和 $\mathcal{F}_{V_i}$ 的全次数的多项式函数 [68, 69]。注意到 $\mathcal{F}_{V_i}$ 的全次数不超过 $(i+1)D^n$，所以第 4 步的复杂度是 $(sLn(r+1)D^n)^{O(1)}$。又因为 $r\le n-1$，所以 $(sLn(r+1)D^n)^{O(1)}$ 包含在 $(sLnD^n)^{O(1)}$ 中。

以 $\mathcal{F}_{V_{ij}}$ 为输入，计算 $\mathbf{I}(V_{ij})$ 的生成元 G_{ij} 的复杂度不会超过 $(sLnD^n)^{O(1)}$ [15, Section 5.5]。然后，将 G_{ij} 中的多项式在 S 中的所有点上取值，可判定 $\mathbf{V}_{\mathbb{C}}(G_{ij})\cap S$ 是否为空，这一步的复杂度也不会超过 $(sLnD^n)^{O(1)}$。最后，因为 L 不超过 $O(s(nD)^n)$ [见 70]，所以在成功的情况下，算法 RealRadicalSmooth 的整体复杂度是 $(snD^n)^{O(1)}$。

□

算法 RealRadicalSmooth 是蒙特卡罗算法，即无法保证最后得到的结果是正确的。

3.4　一般情形

3.4.1　有理参数化的定义和性质

定义 3.4.1　令 V 是一个等维复代数簇，其维数是 $r\,(r\ge 0)$，次数是 δ。V 的一个有理参数化表示由如下多项式组成：

- $\mathbb{Q}[T_1,\ldots,T_{r+1}]$ 中的一组多项式 $(w,v_1,\ldots,v_n)$，满足：$T_1,\ldots,T_{r+1}$ 是新的变元；w 无平方，首系数为 1，全次数为 δ；对于 $1\le i\le n$，有不等式 $\deg(v_i,T_{r+1})<\deg(w,T_{r+1})$。
- $\boldsymbol{\ell}=(\lambda_1,\ldots,\lambda_{r+1})$，其中每个 λ_i 是 $X_1,\ldots,X_n$ 的线性组合，满足 $\lambda_i(v_1,\ldots,v_n)=T_i\frac{\partial w}{\partial T_{r+1}} \mod w$。

我们把这样的有理参数化表示记为 $\mathcal{Q}=((w,v_1,\ldots,v_n),\boldsymbol{\ell})$，称 $\mathcal{Q}$ 是 $\mathbb{Q}[T_1,\ldots,T_{r+1}]$ 中的一个次数为 δ 的 r 维有理参数化表示。

复代数簇 V 是如下集合在 $\mathbb{C}^n$ 中的 Zariski 闭包：

$$\left\{(x_1,\ldots,x_n)\in\mathbb{C}^n \mid \exists\vartheta\in\mathbb{C}^{r+1}, w(\vartheta)=0, \frac{\partial w}{\partial T_{r+1}}(\vartheta)\neq 0, x_i=\frac{v_i}{\partial w/\partial T_{r+1}}(\vartheta)\right\}.$$

我们也称 $\mathscr{Q}$ 是复代数簇 V 的零化理想的有理参数化表示。

给定一个有理参数化表示 $\mathscr{Q}$，将 $\mathscr{Q}$ 所对应的复代数簇记作 $Z(\mathscr{Q})$。由雅可比准则可知 (见定理 2.1.17)，$Z(\mathscr{Q})$ 是等维的。在映射 $x\to(\lambda_1(x),\ldots,\lambda_{r+1}(x))$ 下，$Z(\mathscr{Q})$ 的像的 Zariski 闭包等于 $\{\vartheta\in\mathbb{C}^{r+1}\mid w(\vartheta)=0\}$。多项式 w 称为 $\mathscr{Q}$ 的消去多项式 (eliminating polynomial)。此外，w 的次数与 $Z(\mathscr{Q})$ 的次数相等 [22, Proposition 1]。另外，我们用 $((1))$ 表示空集。

命题 3.4.2 *令 V 是 $\mathbb{C}^n$ 中的一个等维复代数簇，其维数是 r。存在一个非空的 Zariski 开集 $\mathscr{G}(V)\subset\mathbb{C}^{n\times(r+1)}$ 使得对任意的 $\boldsymbol{\ell}\in\mathscr{G}(V)\cap\mathbb{Q}^{n\times(r+1)}$，下述性质成立：存在 $\mathbb{Q}[T_1,\ldots,T_{r+1}]$ 中的一组多项式 $(w,v_1,\ldots,v_n)$ 使得 $Z(\mathscr{Q})=V$，其中 $\mathscr{Q}=((w,v_1,\ldots,v_n),\boldsymbol{\ell})$.*

证明 参见 [21, Section 7] 或 [71]。 □

令 $\mathscr{Q}=((w,v_1,\ldots,v_n),\boldsymbol{\ell}=(\lambda_1,\ldots,\lambda_{r+1}))$ 是一个有理参数化表示。对于多项式 $\frac{\partial w}{\partial T_{r+1}}\in\mathbb{Q}[T_1,\ldots,T_{r+1}]$，将变量 T_i 替换为 λ_i，得到一个 $\mathbb{Q}[X_1,\ldots,X_n]$ 中的一个多项式，记作 $\sigma_{\mathscr{Q}}$，即

$$\sigma_{\mathscr{Q}}=\frac{\partial w}{\partial T_{r+1}}(\lambda_1,\ldots,\lambda_{r+1}).$$

记 $\mathcal{S}(\mathscr{Q})=Z(\mathscr{Q})\cap\mathbf{V}_{\mathbb{C}}(\sigma_{\mathscr{Q}})$。下面这个命题在 [25] 中的结论部分提到。

命题 3.4.3 *保留上述的记号，复代数簇 $Z(\mathscr{Q})$ 在 $\mathbb{Q}$ 上不可约当且仅当多项式 w 在 $\mathbb{Q}$ 上不可约。*

引理 3.4.4 *假设复代数簇 $Z(\mathscr{Q})$ 的零化理想 I 是素理想。那么，I 是实的当且仅当下述两个等价的条件成立：*

(i) *$Z(\mathscr{Q})$ 包含一个实的非奇异点;*

(ii) *半代数集 $S=\left\{\vartheta\in\mathbb{R}^{r+1}\mid w(\vartheta)=0,\frac{\partial w}{\partial T_{r+1}}(\vartheta)\neq 0\right\}$ 非空。*

特别地，如果 I 不是实的，则 $Z(\mathscr{Q})\cap\mathbb{R}^n$ 等于 $\mathcal{S}(\mathscr{Q})\cap\mathbb{R}^n$。

证明 记 $h=\frac{\partial w}{\partial T_{r+1}}$。由命题 3.2.2可知，素理想 I 是实的当且仅当它有一个非奇异的实零点，这等价于 $Z(\mathscr{Q})$ 包含一个实的非奇异点。

下面我们证明条件 (ii) 成立当且仅当 I 是实理想。不失一般性，假设对于 $i=1,\ldots,r+1$，线性组合 $\lambda_i=X_i$。于是，$T_i=X_i$，其中 $i=1,\ldots,r+1$。

如果半代数集 S 非空，则存在 $\vartheta\in\mathbb{R}^{r+1}$ 使得 $w(\vartheta)=0$ 且 $h(\vartheta)\neq 0$。令 $x=\left(\frac{v_1}{h}(\vartheta),\ldots,\frac{v_n}{h}(\vartheta)\right)$，则 x 属于 $Z(\mathscr{Q})\cap\mathbb{R}^n$。根据 $Z(\mathscr{Q})$ 定义以及 Hilbert 零点定理，多项式 $w,hX_{r+2}-v_{r+2},\ldots,hX_n-v_n$ 都属于 I。此外，因为 $w,hX_{r+2}-v_{r+2},\ldots,hX_n-v_n$ 关于变元 $X_1,\ldots,X_n$ 的雅可比矩阵在 x 处的秩为 $n-r$，故 x 是 I 的非奇异零点。因此理想 I 是实的。

反过来，如果半代数集 S 是空的，那么 $Z(\mathscr{Q})\cap\mathbb{R}^n$ 包含在 $Z(\mathscr{Q})\cap\mathbf{V}_{\mathbb{C}}(\sigma_{\mathscr{Q}})$ 中。另一方面，由于 $Z(\mathscr{Q})$ 不可约，且 $Z(\mathscr{Q})\cap\mathbf{V}_{\mathbb{C}}(\sigma_{\mathscr{Q}})$ 严格包含在 $Z(\mathscr{Q})$ 中，故 $Z(\mathscr{Q})\cap\mathbf{V}_{\mathbb{C}}(\sigma_{\mathscr{Q}})$ 的维数严格小于 $(Z(\mathscr{Q}))$ 的维数。因此，$Z(\mathscr{Q})\cap\mathbb{R}^n$ 的维数也严格小于 $Z(\mathscr{Q})$ 的维数，这就意味着 I 不是实的。

□

从引理 3.4.4的证明中，我们有下述推论。

推论 3.4.5 保留上述的记号，假设复代数簇 $Z(\mathscr{Q})$ 不可约，则 $\mathcal{S}(\mathscr{Q})$ 的维数严格小于 $Z(\mathscr{Q})$ 的维数。

3.4.2　算法

首先介绍一些将在主算法中会用到的子程序。

第一个子程序是 IrreducibleDecomposition，它主要是执行如下任务：输入 $\mathbb{Q}[X_1,\ldots,X_n]$ 中的一组多项式 $\boldsymbol{f}=(f_1,\ldots,f_s)$，然后输出 $\mathbf{V}_{\mathbb{C}}(\boldsymbol{f})$ 的所有不可约分支的有理参数化表示。首先，调用 [25] 中的等维分解算法可得到 $\mathbf{V}_{\mathbb{C}}(\boldsymbol{f})$ 所有等维分支上的一般零点 (generic points) 的参数化表示，这个等维分解算法的复杂度是 $(sLnD^n)^{O(1)}$。接下来，用 Hensel 提升将一般零点的参数化表示恢复成对应的等维分支的参数化表示，这一步的复杂度是 $\left(snD^{n\max(1,r)}\right)^{O(1)}$。最后，通过分解每个等维分支的参数化表示的消去多项式，再做相应的约化计算，得到对应的不可约分支的参数化表示。这一步的算术复杂度不会超过 $\left(snD^{n\max(1,r)}\right)^{O(1)}$（参见 [68, Theorem 6.1] 或 [69, Theorem 1]。

引理 3.4.6 令 $\boldsymbol{f} = (f_1, \ldots, f_s)$ 是 $\mathbb{Q}[X_1, \ldots, X_n]$ 中的一组多项式。记 $D = \max\{\deg f_i \mid 1 \le i \le s\}$，$V$ 是 $\boldsymbol{f}$ 的复代数簇，V 的维数是 r。存在复杂度为 $(snD^{n\max(1,r)})^{O(1)}$ 的概率算法计算 V 的所有不可约分支的参数化表示。

第二个子程序是 IsReal。令 $\mathscr{Q}$ 是 $\mathbb{Q}[T_1, \ldots, T_{r+1}]$ 中次数为 δ 的一个有理参数化表示。假设 $\mathscr{Q}$ 对应的复代数簇 $Z(\mathscr{Q})$ 是不可约的。子程序 IsReal 用来判定 $Z(\mathscr{Q})$ 是否包含一个非奇异的实点，它的复杂度是 $\delta^{O(r)}$。

引理 3.4.7 令 $\mathscr{Q} = (w, v_1, \ldots, v_n, \boldsymbol{\ell})$ 是 $\mathbb{Q}[T_1, \ldots, T_{r+1}]$ 中次数为 δ 的一个有理参数化表示。假设 $\mathscr{Q}$ 对应的复代数簇 $Z(\mathscr{Q})$ 是不可约的。则存在算法 IsReal 可判定 $Z(\mathscr{Q})$ 是否包含一个非奇异的实点，如果包含则返回 true，否则返回 false。这个算法的复杂度是 $\delta^{O(\max(1,r))}$。

证明 由引理 3.4.6，只需判定半代数系统 $w = 0, \frac{\partial w}{\partial T_{r+1}} \neq 0$ 是否有实解。根据 [48, Chapter 14]，存在复杂度为 $\delta^{O(\max(1,r))}$ 的算法来完成上述判定。 □

下一个子程序是 ChangeSeparatingElement。这个子程序的输入是某个复代数簇 Z 的一个有理参数化表示，这个参数化中的线性组合是 $\boldsymbol{\ell}$。这个子程序的输出是：一个新的线性组合 $\boldsymbol{\ell}'$ 以及 $\boldsymbol{\ell}'$ 对应的有理参数化表示 $\mathscr{Q}'$(其中 $\mathscr{Q}'$ 也是 Z 的一个有理参数化表示)。

引理 3.4.8 令 $\mathscr{Q} = ((w, v_1, \ldots, v_n), \boldsymbol{\ell})$ 是 r 维等维复代数簇 Z 的一个有理参数化表示，其次数为 δ，且 $\boldsymbol{\ell}$ 在 Zariski 开集 $\mathscr{G}(Z)$ 中（关于 $\mathscr{G}(Z)$ 的定义，见命题 3.4.2）。那么存在复杂度为 $(r+1)(n\delta)^{O(\max(1,r))}$ 的算法 ChangeSeparatingElement 用于计算有理参数化表示 $\mathscr{Q}' = ((w', v_1', \ldots, v_n'), \boldsymbol{\ell}')$，使得 $\mathscr{Q}'$ 也是 Z 的一个有理参数化表示。

证明 这个算法的原理与 [24, Lemma J.8, electronic Appendix] 类似，需要用到 [72, Lemma 2] 中的完成零维系统本原元变换的算法（其复杂度是 $(n\delta)^{O(1)}$）。

这里，我们需要处理的是正维的情形。在 [24, Lemma J.8, electronic Appendix] 中，一维的情形是通过应用 [72, Lemma 2] 和单变元幂级数环 $\mathbb{Q}[[T_1 - y_1]]$ 中的操作来处理，其中 y_1 是随机选取的。通过模 $(T_1 - y_1)^{\deg(\mathscr{Q})+1}$ 来截断幂级数，就可以将零维情形下的算法在 $\mathbb{Q}[[T_1 - y_1]]$ 中运行，从而得到新的线性组合

及其对应的有理参数化表示。于是，增加的运算量都是由此而来的 $\mathbb{Q}[[T_1 - y_1]]$ 中的运算步骤。

为了处理 r 维等维的情形，使用类似的办法，把幂级数环变为 $\mathbb{Q}[[T_1 - y_1, \ldots, T_r - y_r]]$，其中 $y_1, \ldots, y_r$ 是随机选取的，依然通过模次数为 $\deg(\mathscr{Q})+1$ 的单项式来截断幂级数。这时，增加的运算量都是由此而来的 $\mathbb{Q}[[T_1 - y_1, \ldots, T_r - y_r]]$ 中的运算步骤，这不会超过 $(n\delta)^{O(r)}$（因为计算的多项式次数都不超过 $\deg(\mathscr{Q})+1$，即 $\delta+1$）。

最后，改变 $r+1$ 个线性形式只需要把这个过程执行 $r+1$ 遍。

□

子程序 Intersect。令 $\mathscr{Q} = ((w, v_1, \ldots, v_n), \boldsymbol{\ell})$ 是 $\mathbb{Q}[T_1, \ldots T_{r+1}]$ 中的一个有理参数化表示，其中 $\boldsymbol{\ell} = (\lambda_1, \ldots, \lambda_{r+1})$，$g$ 是 $\mathbb{Q}[T_1, \ldots T_{r+1}]$ 中的一个多项式。用 $g_{\mathscr{Q}}$ 表示多项式 $g(\lambda_1, \ldots, \lambda_{r+1}) \in \mathbb{Q}[X]$。子程序 Intersect 用于计算 $Z(\mathscr{Q}) \cap \mathbf{V}_{\mathbb{C}}(g_{\mathscr{Q}})$ 的有理参数化表示。

引理 3.4.9　令 $\mathscr{Q} = ((w, v_1, \ldots, v_n), \boldsymbol{\ell})$ 是 $\mathbb{Q}[T_1, \ldots T_{r+1}]$ 中的次数为 δ 一个有理参数化表示，$Z(\mathscr{Q}) \subset \mathbb{C}^n$ 是一个 r 维的等维复代数簇，其中 $r \geq 1$。令 g 是 $\mathbb{Q}[T_1, \ldots T_{r+1}]$ 中次数为 δ' 的一个多项式。假设 $Z(\mathscr{Q}) \cap \mathbf{V}_{\mathbb{C}}(g_{\mathscr{Q}})$ 的维数是 $r-1$。则存在算法 Intersect 使得输入 $(\mathscr{Q}, g)$，可得到表示 $Z(\mathscr{Q}) \cap \mathbf{V}_{\mathbb{C}}(g_{\mathscr{Q}})$ 的所有不可约分支的有理参数化表示，且算法 Intersect 的复杂度是 $(n \max(\delta, \delta'))^{O(r)}$。

证明　这个算法的第一步是选取 $r+1$ 个关于 $X_1, \ldots, X_n$ 的线性组合 $\lambda'_1, \ldots, \lambda'_{r+1}$，令 $\boldsymbol{\ell}' = (\lambda'_1, \ldots, \lambda'_{r+1})$，假设 $\boldsymbol{\ell}'$ 属于 Zariski 开集 $\mathscr{G}(Z)$ 中（见命题 3.4.2）。

$Z(\mathscr{Q})$ 是一个 r 维等维的复代数簇，由 Krull 维数定理 [59]，如果交集 $Z(\mathscr{Q}) \cap \mathbf{V}_{\mathbb{C}}(g_{\mathscr{Q}})$ 非空，则它的维数不小于 $r-1$，因此它所有的不可约分支的维数也都不低于 $r-1$。因为已经假定 $\dim(Z(\mathscr{Q}) \cap \mathbf{V}_{\mathbb{C}}(g_{\mathscr{Q}})) = r-1$，故 $Z(\mathscr{Q}) \cap \mathbf{V}_{\mathbb{C}}(g_{\mathscr{Q}})$ 是一个 $r-1$ 维的等维复代数簇。

因此，可以进一步假设 $\boldsymbol{\ell}'$ 的前 r 个线性组合包含在 Zariski 开集 $\mathscr{G}(Z(\mathscr{Q}) \cap \mathbf{V}_{\mathbb{C}}(g_{\mathscr{Q}}))$（见命题 3.4.2）。

下一步，要计算有理参数化表示 $\mathscr{Q}' = ((w', v'_1, \ldots, v'_n), \boldsymbol{\ell}')$ 使得其对应的复代数簇是 $Z(\mathscr{Q})$。为清晰起见，记 $\mathscr{Q}'$ 中涉及到的变元为 $T'_1, \ldots, T'_{r+1}$。引理 3.4.8表明这一步的复杂度是 $(r+1)(n\delta)^{O(r)}$。

现在，要计算表示交集 $Z(\mathscr{Q}') \cap \mathbf{V}_{\mathbb{C}}(g_{\mathscr{Q}})$ 的有理参数化表示。这个过程如下：

1. 将 g 中的变元 $T_1, \ldots, T_{r+1}$ 分别替换为 $\mathscr{Q}$ 中的 $\lambda_1, \ldots, \lambda_{r+1}$，得到 $\mathbb{Q}[X_1, \ldots, X_n]$ 中的多项式 $g_{\mathscr{Q}}$；

2. 将 $g_{\mathscr{Q}}$ 中的变元 $X_1, \ldots, X_n$ 分别替换为 $\mathscr{Q}'$ 中对应的参数化形式，由此得到 $\mathbb{Q}(T'_1, \ldots, T'_{r+1})$ 中的一个有理函数 g'；

3. 通过 [21, Section 2.2] 中的子结式运算，求 g' 和 w' 的分子的零点集的交（在复数域中），并由此得到 $Z(\mathscr{Q}) \cap \mathbf{V}_{\mathbb{C}}(g_{\mathscr{Q}})$ 的有理参数化表示。

然而，直接按上述步骤计算无法得到引理中所给出的复杂度，需要引进一个经典的赋值-插值技巧，这样能更好地控制运算过程中出现的分母的次数。

这里，通过一个直线型程序（straight-line program, 简称 SLP）Γ 来表示 $g_{\mathscr{Q}}$。因为 g 是 $\mathbb{Q}[T_1, \ldots T_{r+1}]$ 中次数为 δ' 的多项式，因此 Γ 的长度不超过 $(r\delta')^{O(r)} + O(nr)$[70]。然后，将 $X_i = \frac{v'_i}{\partial w'/\partial T'_{r+1}}$ 代入 Γ 中，再执行所需的赋值操作，可得到有理函数 g' 的 SLP 表示，这个过程复杂度是 $(n\delta)^{O(r)}$（因为 $\mathscr{Q}'$ 中的多项式的次数不超过 δ 且只涉及 $r+1$ 个变元）。最后，总结起来，计算 g' 的 SLP 表示总的复杂度是 $(r\delta')^{O(r)} + O(nr) + (n\delta)^{O(r)}$。

取 $y = (y_1, \ldots, y_{r-1}) \in \mathbb{Q}^{r-1}$，将 g' 中的变元 $T'_1, \ldots, T'_{r-1}$ 分别取值为 $y_1, \ldots, y_{r-1}$，根据上面计算 g' 的 SLP 表示的过程，可知完成所有的取值的复杂度是 $(r\delta')^{O(r)} + O(nr) + (n\delta)^{O(r)}$。

对于上述的 y，记 g'_y 为新得到的有理函数。类似地，将 $\mathscr{Q}'$ 中的变元 $T'_1, \ldots, T'_{r-1}$ 赋值为 $y_1, \ldots, y_{r-1}$，这样得到有理参数化表示记为 $\mathscr{Q}'_y$。

利用 [21, Section 2.2] 中的计算交集的算法，以 g'_y 的分子和 $\mathscr{Q}'_y$ 为输入，可得到 $Z(\mathscr{Q}) \cap \mathbf{V}_{\mathbb{C}}(g_{\mathscr{Q}}) \cap \mathbf{V}_{\mathbb{C}}(\boldsymbol{\ell}'_y)$ 的一个零维参数化表示。

由 Bézout's 定理，复代数簇 $Z(\mathscr{Q}) \cap \mathbf{V}_{\mathbb{C}}(g_{\mathscr{Q}})$ 的次数不超过 $\delta'\delta$，因此只需将上述过程重复 $(\delta'\delta)^{O(r)}$ 次，再利用插值算法即可得到 $Z(\mathscr{Q}) \cap \mathbf{V}_{\mathbb{C}}(g_{\mathscr{Q}})$ 的参数化表示。最后，再通过分解相应的消去多项式得到 $Z(\mathscr{Q}) \cap \mathbf{V}_{\mathbb{C}}(g_{\mathscr{Q}})$ 的不可约分支的参数化表示。

□

子程序 RemoveRedundantComponents。令 $\mathscr{L}=(\mathscr{Q}_1,\ldots,\mathscr{Q}_t)$ 是一组有理参数化表示，满足：对 $1\le i\le t$，$Z(\mathscr{Q}_i)$ 是不可约的。这个子程序返回 $\mathscr{L}$ 的一个子集 $\mathscr{Q}_{i_1},\ldots,\mathscr{Q}_{i_k}$，使得 $Z(\mathscr{Q}_{i_1})\cup\cdots\cup Z(\mathscr{Q}_{i_k})=Z(\mathscr{Q}_1)\cup\cdots\cup Z(\mathscr{Q}_t)$，且对于 $u\ne v$，有 $Z(\mathscr{Q}_{i_u})\not\subset Z(\mathscr{Q}_{i_v})$。

引理 3.4.10 令 $\mathscr{L}=(\mathscr{Q}_1,\ldots,\mathscr{Q}_t)$ 是一组有理参数化表示，其中 $\mathscr{Q}_i$ 的次数为 δ_i，记 δ 是 $\delta_1,\ldots,\delta_t$ 中的最大值。假设对于 $1\le i\le t$，$Z(\mathscr{Q}_i)$ 是不可约的且它的维数是 r_i。令 r 是 $r_1,\ldots,r_t$ 中的最大值。存在一个算法 RemoveRedundantComponents，对于输入 $\mathscr{L}$，可得到 $\mathscr{L}$ 的一个子集 $\mathscr{Q}_{i_1},\ldots,\mathscr{Q}_{i_k}$ 使得下述条件成立：

- $Z(\mathscr{Q}_{i_1})\cup\cdots\cup Z(\mathscr{Q}_{i_k})=Z(\mathscr{Q}_1)\cup\cdots\cup Z(\mathscr{Q}_t)$；
- 如果 $u\ne v$，则 $Z(\mathscr{Q}_{i_u})\not\subset Z(\mathscr{Q}_{i_v})$。

算法 RemoveRedundantComponents 的复杂度是 $t(r+1)(n\delta)^{O(r)}$。

证明 首先，将 $\mathscr{L}$ 中的有理参数化表示按照其维数的大小进行排序。不妨假设 $\mathscr{Q}_1,\ldots,\mathscr{Q}_t$ 已经是按维数非递减的顺序排列好的，即 $r_i\le r_{i+1}$。随机选取 $r+1$ 个线性组合 $\boldsymbol{\ell}=(\lambda_1,\ldots,\lambda_{r+1})$，然后以 $\mathscr{Q}_i$ 和 $(\lambda_1,\ldots,\lambda_{r_i+1})$ 为输入，调用 ChangeSeparatingElement，得到 $\mathscr{Q}_i'$ 和 $(\lambda_1',\ldots,\lambda_{r_i+1}')$，使得 $\mathscr{Q}_1',\ldots,\mathscr{Q}_t'$ 满足：对任意的 $1\le s_i\le r_i$ 和 $1\le s_j\le r_j$，如果 $s_i=s_j$，则 $\lambda_{s_i}'=\lambda_{s_j}'$。由引理 3.4.8，这一步的复杂度是 $t(r+1)(n\delta)^{O(r)}$。因为已经假定所有的 $Z(\mathscr{Q}_i')$ 都是不可约的，因此最后只需做如下操作：若 $i<j$ 且 $r_i<r_j$，判定 $Z(\mathscr{Q}_i')$ 是否包含在 $Z(\mathscr{Q}_j')$。□

下面我们开始介绍主要的算法 LazyRealRadical。算法的输入是 $\mathbb{Q}[X_1,\ldots,X_n]$ 中的一组多项式 $\boldsymbol{f}=(f_1,\ldots,f_s)$，输出是实根理想 $\sqrt[re]{\langle\boldsymbol{f}\rangle}$ 的所有极小素理想的有理参数化表示（这里我们将素理想等同于其对应的复代数簇）。

首先，调用 IrreducibleDecomposition 来计算复代数簇 $\mathbf{V}_{\mathbb{C}}(\boldsymbol{f})$ 的所有不可约分支的有理参数化表示 $\mathscr{R}_1,\ldots,\mathscr{R}_t$。然后，对于 $1\le i\le t$，记 $Z(\mathscr{R}_i)$ 的零化理想为 I_i，计算 $\sqrt[re]{I_i}$ 的所有极小素理想的有理参数化表示。这需要一个新的算法 LazyRealRadicalRec(随后会详细介绍)。最后，调用 RemoveRedundantComponents 来去掉多余的分支。

LazyRealRadical($\boldsymbol{f}$)

1. $(\mathscr{R}_1,\ldots,\mathscr{R}_t)=\mathsf{IrreducibleDecomposition}(\boldsymbol{f})$;
2. if $t=1$ and $\mathscr{R}_1=((1))$ then return $((1))$;
3. $\mathsf{res}=\{\}$;
4. for $1\le j\le t$ do
   - $\mathrm{res}=\mathrm{res}\cup\mathsf{LazyRealRadicalRec}(\mathscr{R}_i)$;
5. return $\mathsf{RemoveRedundantComponents}(\mathrm{res})$.

现在，我们介绍算法 LazyRealRadicalRec。令 $\mathscr{Q}$ 是一个有理参数化表示，且 $Z(\mathscr{Q})$ 不可约。记 $Z(\mathscr{Q})$ 的零化理想为 I。算法以 $\mathscr{Q}$ 为输入，计算 $\sqrt[re]{I}$ 的所有极小素理想的有理参数化表示。首先，通过 IsReal 来判定 $Z(\mathscr{Q})$ 是否包含一个非奇异的实点，如果包含，则返回 $\mathscr{Q}$，否则计算 $\mathcal{S}(\mathscr{Q})$ 的所有不可约分支的有理参数化表示，最后对这些新的有理参数化表示做递归。

LazyRealRadicalRec($\mathscr{Q}$)

1. if $\mathscr{R}_1=((1))$ then return $((1))$;
2. if $\mathsf{IsReal}(\mathscr{Q})$ then return $(\mathscr{Q})$;
3. let $w\in\mathbb{Q}[T_1,\ldots,T_{r+1}]$ be the eliminating polynomial of $\mathscr{Q}$;
4. $(\mathscr{Q}'_1,\ldots,\mathscr{Q}'_k)=\mathsf{Intersect}(\mathscr{Q},\frac{\partial w}{\partial T_{r+1}})$;
5. for $1\le\ell\le k$ do
   - $\mathrm{res}=\mathrm{res}\cup\mathsf{LazyRealRadicalRec}(\mathscr{Q}'_\ell)$;
6. return $\mathsf{RemoveRedundantComponents}(\mathrm{res})$.

定理 3.4.11 令 $\boldsymbol{f}=(f_1,\ldots,f_s)$ 是 $\mathbb{Q}[X_1,\ldots,X_n]$ 中的一组多项式，$D=\max\{\deg f_1,\ldots,\deg f_s\}$，$r=\max\{1,\dim\mathbf{V}_{\mathbb{C}}(\boldsymbol{f})\}$。算法 LazyRealRadical 以 $\boldsymbol{f}$ 为输入，以概率 1 返回 $\sqrt[re]{\langle\boldsymbol{f}\rangle}$ 的所有极小素理想的有理参数化表示，其复杂度为 $s^{O(1)}(nD)^{O(nr2^r)}$。

证明　概率分析：与定理 3.3.4的证明类似。

正确性：以 $\boldsymbol{f}$ 为输入，LazyRealRadical 首先计算 $\mathbf{V}_{\mathbb{C}}(\boldsymbol{f})$ 所有不可约分支的有理参数化表示 $\mathscr{R}_1,\ldots,\mathscr{R}_t$。下一步，对于 $1 \le i \le t$，计算 $\mathbf{I}(Z(\mathscr{R}_i))$ 的实根理想所有极小素理想的有理参数化表示。这一步是通过调用算法 LazyRealRadicalRec 来完成。因此，只需证明算法 LazyRealRadicalRec 的正确性。假设 $\mathscr{Q}$ 是 LazyRealRadicalRec 的一个输入，$\mathscr{Q}$ 对应的复代数簇 $Z(\mathscr{Q})$ 是不可约的，下面我们通过归纳法证明这个算法的正确性。如果 $Z(\mathscr{Q})$ 是零维的，结论是显然的。现在假设 $Z(\mathscr{Q})$ 的维数 r 大于零，算法 LazyRealRadicalRec 对于维数小于 r 的输入都会在有限步内终止且输出结果是正确的。如果 IsReal 判定 $Z(\mathscr{Q})$ 的理想是实的，则直接返回 $\mathscr{Q}$，算法结束且返回结果正确。否则，由引理 3.4.4, 调用 Intersect 计算 $\mathcal{S}(\mathscr{Q})$ 的不可约分解，得到其不可约分支的有理参数化表示 $\mathscr{Q}'_1,\ldots,\mathscr{Q}'_k$，再对每个 $\mathscr{Q}'_i$ 做递归。由推论 3.4.5和归纳假设，算法的终止性与正确性得证。

复杂度分析：LazyRealRadical 的第一步是调用算法 IrreducibleDecomposition，它的复杂度是 $(snD^{nr})^{O(1)}$(引理 3.4.6)，其中 $r = \max\{1, \dim \mathbf{V}_{\mathbb{C}}(\boldsymbol{f})\}$。由 Bézout's 定理 (可参见 [73])，这一步的输出所表示的不可约分支的次数和不超过 D^n，因此 $t \le D^n$ 且对于 $1 \le i \le t$，$\mathscr{R}_i$ 的次数也不超过 D^n。

下一步，对于 $1 \le i \le t$，以 $\mathscr{R}_i$ 为输入，调用算法 LazyRealRadicalRec。我们将在最后证明如果以次数为 δ 的 ρ 维有理参数化表示 $\mathscr{Q}$ 为输入，满足 $Z(\mathscr{Q})$ 不可约，算法 LazyRealRadicalRec 输出的有理参数化表示的次数和不超过 $(n\delta)^{O(2^\rho)}$，且算法的复杂度也是 $(n\delta)^{O(2^\rho)}$。因此，整个 "for" 循环的复杂度是 $(nD)^{O(n2^r)}$。

LazyRealRadical 的最后一步是调用 RemoveRedundantComponents，由引理 3.4.10可知，整个算法的复杂度是 $s^{O(1)}(nD)^{O(nr2^r)}$。

现在，证明上述关于 LazyRealRadicalRec 的复杂度的声明。这个算法的第一步是以 $\mathscr{Q}$ 为输入，调用 IsReal，其复杂度是 $\delta^{O(\rho)}$(引理 3.4.7)。如果判定 $\mathscr{Q}$ 的理想是实的，那么 $\mathscr{Q}$ 被返回，否则以 $\mathscr{Q}$ 和 $\frac{\partial w}{\partial T_{\rho+1}}$ 为输入，调用 Intersect，其中 w 是 $\mathscr{Q}$ 的消去多项式。由引理 3.4.9，这一步的复杂度是 $(n\delta)^{O(\rho)}$。

输出的有理参数化表示的次数和不高于 δ^2，其维数等于 $\rho - 1$。因此，当输入是次数等于 δ，维数等于 ρ 的一个有理参数化表示时，设 $T(\delta,\rho)$ 为此时

LazyRealRadicalRec 的复杂度，那么就有下面的递归公式：

$$T(\delta,\rho) \le (n\delta)^{O(\rho)} + T(\delta^2, \rho-1).$$

求解这个递归公式即得到算法的复杂度。同样地，对于输出多项式的次数和也有这个递归公式。定理得证。

□

3.5 例子

因为已实现的符号算法大都是基于 Gröbner 基，所以实际计算当中，我们是采用 Gröbner 而不是有理参数化表示来对复代数簇进行操作。因此，计算得到是实根理想的极小素分解。用于算法运行的服务器的参数：Intel(R) Xeon(R) CPU E7-4809 v2 @ 1.90GHz, RAM 756GB。

已有的计算实根理想的符号算法 [1, 2] 是由 Spang[4] 提供的一个 Singular 程序包 realrad。下面给出的例子都是这个程序包无法计算的。

例 3.5.1 (Vor1) 下面的多项式取自 [74]:

$$\begin{aligned}\mathrm{Vor1} =&(\alpha^2+\beta^2+1)a^2\lambda^4 - 2a(2a\beta^2 + ay\beta + a\alpha x - \beta\alpha + 2a + 2a\alpha^2 - \beta\alpha a^2)\lambda^3\\ &+ (\beta^2 + 6a^2\beta^2 - 2\beta x a^3 - 6\beta\alpha a^3 + 6y\beta a^2 - 6a\beta\alpha - 2a\beta x + 6\alpha x a^2 + y^2a^2\\ &- 2a\alpha y + x^2a^2 - 2y\alpha a^3 + 6a^2\alpha^2 + a^4\alpha^2 + 4a^2)\lambda^2\\ &- 2(xa - ya^2 - 2\beta a^2 - \beta + 2a\alpha + \alpha a^3)(xa - y - \beta + a\alpha)\lambda\\ &+ (1+a^2)(xa - y - \beta + a\alpha)^2.\end{aligned}$$

这个多项式是一个平方和 [75]，因此理想 $\langle \mathrm{Vor1}\rangle$ 不是实的。输入 Vor1，得到 $\sqrt[e]{\langle \mathrm{Vor1}\rangle}$ 所有的极小素理想：

$$P_1 = \langle a\alpha - ax + \beta - y, \lambda + 1\rangle, P_2 = \langle a\alpha + ax - \beta - y, \lambda\rangle, P_3 = \langle 2\beta\lambda + \beta + y, a\rangle.$$

运行时间在 9 秒之内。

例 3.5.2 考虑下述对称矩阵的特征多项式：

$$\begin{pmatrix} x & 1 & 1\\ 1 & y & 1\\ 1 & 1 & z\end{pmatrix}.$$

令 $\mathcal{D}$ 是这个特征多项式的判别式，$\mathcal{D}$ 是一个平方和 [76]。以 $\mathcal{D}$ 为输入，得到 $\sqrt[re]{\langle\mathcal{D}\rangle}$ 的极小素理想 $\langle y-z, g\rangle$，其中

$$\begin{aligned}g =& -19y^{12}+228y^{11}z-1254y^{10}z^2+4180y^9z^3-9405y^8z^4+15048y^7z^5-17556y^6z^6+15048y^5z^7\\&-9405y^4z^8+4180y^3z^9-1254y^2z^10+228yz^11-19z^12-606y^10+6060y^9z-27270y^8z^2\\&+72720y^7z^3-127260y^6z^4+152712y^5z^5-127260y^4z^6+72720y^3z^7-27270y^2z^+6060yz^9\\&-606z^10-6732y^8+53856y^7z-188496y^6z^2+376992y^5z^3-471240y^4z^4+376992y^3z^5\\&-188496y^2z^6+53856yz^7-6732z^8-35370y^6+212220y^5z-530550y^4z^2+707400y^3z^3\\&-530550y^2z^4+212220yz^5-35370z^6-116073y^4+464292y^3z-696438y^2z^2+464292yz^3\\&-116073z^4-77760y^2+155520yz-77760z^2+139968x-69984y-69984z.\end{aligned}$$

由此说明 $\sqrt[re]{\langle\mathcal{D}\rangle}$ 是素的。计算这个例子的时间在 4 秒之内。

例 3.5.3 (Homotopy-1) 这个例子取自 [10]:

$$f_1 = x^3y^2+c_1x^3y+y^2+c_2x+c_3,\ f_2 = c_4x^4y^2-x^2y+y+c_5,\ f_3 = c_4-1.$$

输入 $\boldsymbol{f}=(f_1,f_2,f_3)$，计算结果显示 $\sqrt[re]{\langle\boldsymbol{f}\rangle}$ 只有一个极小素理想，且这个素理想是 $\langle\boldsymbol{f}\rangle$。这表明理想 $\langle\boldsymbol{f}\rangle$ 本身就是实的素理想。运行时间在 1 秒之内。

例 3.5.4 (Cinquin-3-4) 这个例子也是取自 [10]:

$$f_1 = s-x_1(1+x_2^4+x_3^4),\ f_2 = s-x_2(1+x_1^4+x_3^4),\ f_3 = s-x_3(1+x_1^4+x_2^4).$$

输入 $\boldsymbol{f}=(f_1,f_2,f_3)$，在 47 秒之内得到 $\sqrt[re]{\langle\boldsymbol{f}\rangle}$ 的极小素理想：

$$\begin{aligned}P_1 &= \left\langle x_3-x_1, x_2-x_1, -x_3^4x_1-x_2^4x_1-x_1+s\right\rangle,\\P_2 &= \left\langle x_3-x_1, x_2^3x_1+x_2^2x_1^2+x_2x_1^3-x_1^4-1, -x_3^4x_1-x_2^4x_1-x_1+s\right\rangle,\\P_3 &= \left\langle x_2-x_1, x_3^3x_1+x_3^2x_1^2+x_3x_1^3-x_1^4-1, -x_3^4x_1-x_2^4x_1-x_1+s\right\rangle,\\P_4 &= \left\langle x_3-x_2, x_2^4-x_2^3x_1-x_2^2x_1^2-x_2x_1^3+1, -x_3^4x_1-x_2^4x_1-x_1+s\right\rangle.\end{aligned}$$

例 3.5.5 (Essential Variety) 这个例子取自 [77]. 令 $\mathcal{E}$ 是按如下定义的一个本质簇:

$$\mathcal{E} = \left\{M\in\mathbb{R}^{3\times3} \mid \det(M)=0,\ 2(MM^T)M-\mathrm{tr}(MM^T)M=0\right\},$$

其中 $\det(M)$ 是 M 的行列式，$\mathrm{tr}(MM^T)$ 是 MM^T 的迹。

将矩阵 M 写为：

$$\begin{pmatrix} a & b & c \\ u & v & w \\ x & y & z \end{pmatrix},$$

则 $\mathcal{E}$ 的定义多项式是 10 个三次多项式:

$$\begin{aligned}
&avz - awy - buz + bwx + cuy - cvx,\\
&(2a^2 + 2b^2 + 2c^2)a + (2au + 2bv + 2cw)u + (2ax + 2by + 2cz)x - ga,\\
&(2a^2 + 2b^2 + 2c^2)b + (2au + 2bv + 2cw)v + (2ax + 2by + 2cz)y - gb,\\
&(2a^2 + 2b^2 + 2c^2)c + (2au + 2bv + 2cw)w + (2ax + 2by + 2cz)z - gc,\\
&(2au + 2bv + 2cw)a + (2u^2 + 2v^2 + 2w^2)u + (2ux + 2vy + 2wz)x - gu,\\
&(2au + 2bv + 2cw)b + (2u^2 + 2v^2 + 2w^2)v + (2ux + 2vy + 2wz)y - gv,\\
&(2au + 2bv + 2cw)c + (2u^2 + 2v^2 + 2w^2)w + (2ux + 2vy + 2wz)z - gw,\\
&(2ax + 2by + 2cz)a + (2ux + 2vy + 2wz)u + (2x^2 + 2y^2 + 2z^2)x - gx,\\
&(2ax + 2by + 2cz)b + (2ux + 2vy + 2wz)v + (2x^2 + 2y^2 + 2z^2)y - gy,\\
&(2ax + 2by + 2cz)c + (2ux + 2vy + 2wz)w + (2x^2 + 2y^2 + 2z^2)z - gz,
\end{aligned}$$

其中 $g = (a^2 + b^2 + c^2 + u^2 + v^2 + w^2 + x^2 + y^2 + z^2)$。将这 10 个多项式生成的理想记为 I。输入这些多项式，结果显示 $\sqrt[re]{I}$ 只有一个极小素理想，且这个素理想是 I 本身。这表明 I 是实的素理想。运行时间在 800 秒之内。

第 4 章　多项式全局最优化

4.1　问题和背景

给定多项式 $f, g_1, \ldots, g_s \in \mathbb{R}[X_1, \ldots, X_n]$，令 $G = (g_1, \ldots, g_s)$。我们把 G 的实代数簇记作

$$\mathbf{V}_{\mathbb{R}}(G) = \{x \in \mathbb{R}^n \mid g_1(x) = 0, \ldots, g_s(x) = 0\}.$$

令 $V = \mathbf{V}_{\mathbb{R}}(G)$。这一章考虑的问题是如何计算 f 在 V 上的全局下确界 f^*：

$$f^* = \inf_{x \in V} f(x). \tag{4-1}$$

正如引言中所提到的，能完全求解上述问题的算法都依赖于量词消去，其他的数值算法或符号算法都对 f 和 V 有一定的假设条件。这一章的目的是，对于一般的 f 和 V，给出基于 Gröbner 基的算法用于求解 (4-1)。

4.2　预备知识

4.2.1　广义关键值

用 $\mathcal{L}(\mathbb{R}^n, \mathbb{R}^m)$ 表示 $\mathbb{R}^n$ 到 $\mathbb{R}^m$ 所有线性映射组成的集合。

对于 $A \in \mathcal{L}(\mathbb{R}^n, \mathbb{R}^m)$，令 $v(A) = \inf_{\|y^*\|=1} \|A^*(y^*)\|$，其中 A^* 表示 A 的伴随映射 (adjoint)。令 H 是 $\mathbb{R}^n$ 的一个线性子空间，$A|_H$ 表示映射 A 在 H 上的限制映射，记 $v(A, H) = v(A|_H)$。

命题 4.2.1 [58, 68 页, Proposition 3.3.11] *令 V 是 $\mathbb{R}^n$ 中的一个等维实代数簇。其维数是 d。如果 $x \in V$ 在 d 维非奇异，那么存在 x 的一个半代数开邻域 $U_x \subset V$ 使得 U_x 是 $\mathbb{R}^n$ 中的一个 d 维光滑流形。*

给定一个等维的实代数簇 $V \subset \mathbb{R}^n$，假设 V 的维数是 d，$\mathrm{Reg}(V)$ 表示 V 中所有在 d 维非奇异的点构成的集合，令 $M = \mathrm{Reg}(V)$。由命题 4.2.1可知，M 是 $\mathbb{R}^n$ 中的一个 d 维光滑流形。

设 $f: V \to \mathbb{R}^m$ 是一个多项式映射，$f|_M$ 表示 f 在 M 上的限制映射。对于 $x \in M$，我们用 df 表示 f 的微分，用 T_xM 表示 M 在 x 处的切空间。令 $y \in \mathbb{R}^m$，如果存在 $x \in M$ 使得 $f(x) = y$ 且 $v(df(x), T_xM) = 0$，则称 y 是映射 $f|_M$ 的关键值 (critical value)。映射 $f|_M$ 所有关键值组成的集合记作 $K_0(f, M)$，即：

$$K_0(f, M) = \{y \in \mathbb{R}^m \mid \exists\, x \in M \text{ s.t. } f(x) = y \text{ 且} v(df(x), T_xM) = 0\}. \tag{4-2}$$

对于 $y \in M$，如果存在 M 中的无穷序列 (x_l) 使得 $\|x_l\| \to \infty$，$f(x_l) \to y$ 且 $\|x_l\| v(df(x_l), T_{x_l}M) \to 0$，则称 y 是映射 $f|_M$ 的渐近关键值 (asymptotic critical value)。映射 $f|_M$ 所有渐近关键值组成的集合记为 $K_\infty(f, M)$，即：

$$\begin{aligned} K_\infty(f, M) = \{y \in \mathbb{R}^m \mid &\exists\, x_l \in M, \|x_l\| \to \infty \text{ s.t. } f(x_l) \to y \text{ 且} \\ &\|x_l\| v(df(x_l), T_{x_l}M) \to 0\}. \end{aligned} \tag{4-3}$$

关键值和渐近关键值统称为广义关键值。将 $f|_M$ 所有广义关键值组成的集合记为 $K(f, M)$，即

$$K(f, M) = K_0(f, M) \cup K_\infty(f, M). \tag{4-4}$$

命题 4.2.2 [49, Proposition 2.2] 令 $A \in \mathcal{L}(\mathbb{R}^n, \mathbb{R}^m)$，$\Sigma \subset \mathcal{L}(\mathbb{R}^n, \mathbb{R}^m)$ 是所有非满的线性映射组成的集合。则 $v(A) = \operatorname{dist}(A, \Sigma)$。

定义 4.2.3 [53] 令 $A \in \mathcal{L}(\mathbb{R}^n, \mathbb{R}^m)$，$H = \{x \in X \mid B_j = \sum_{i=1}^n b_{ji} x_i = 0, j = 1, \ldots, r\}$ 是 $\mathbb{R}^n$ 的一个线性子空间，且 $\dim H = n - r$。记 B 为 $B_1, \ldots, B_r$ 的系数矩阵，为简化记号，A 的矩阵也记作 A，A 和 B 按行拼接得到的新矩阵记为 C。假设 $n \geq m + r$。对于指标集 $I = (i_1, \ldots, i_{m+r}) \subset \{1, \ldots, n\}$，以 I 为列指标，选取 C 中对应的 $((m + r) \times (m + r))$ 阶子式，记为 M_I。令 J 是 I 的一个子集，满足 $|J| = m + r - 1$。对于 $j \in \{1, \ldots, m\}$，去掉 M_I 的第 j 行，然后以 J 为列指标从中选取对应的 $((m + r - 1) \times (m + r - 1))$ 阶子式，记为 $M_I(j)$。定义

$$g'(A, H) = \max_I \left\{ \min_{J \subset I, 1 \leq j \leq m} \frac{|M_I|}{|M_J(j)|} \right\}, \tag{4-5}$$

其中分母仅保留那些满足 $M_J(j) \neq 0$ 的，如果所有的 $M_J(j)$ 都等于零，则令 $g'(A, H) = 0$。

为了符号的简洁，当 A 的定义域明确时，我们将把 $v(A,H), g'(A,H)$ 分别写为 $v(A), g'(A)$。[78, Propostions 2.4，2.5] 表明，$K(f,M)$ 定义中的函数 v 可以被替换为 g'。

例 1.2.1 (续) 令 $g_1 = x^4(y^2+1) - y^2(1+y)$。下面我们用定义 4.2.3中的函数 g' 来计算 $K(f,M)$ 和 $K_1(f,M)$。

f 和 g_1 关于 x,y 的雅可比矩阵是：

$$\mathrm{Jac}(f,g_1) = \begin{pmatrix} 0 & 1 \\ 4x^3(y^2+1) & 2x^4y - 3y^2 - 2y \end{pmatrix}.$$

使用定义 4.2.3中的记号，$A = (0,1), B = (4x^3(y^2+1), 2x^4y - 3y^2 - 2y), C = \mathrm{Jac}(f,g)$，对应的指标集为 $I = (1,2), J = (1)$ 或 $(2), j = 1$。那么

$$g'\left(df(x,y), T_{(x,y)}M\right) = \max_I \left\{ \min_{J\subset I} \frac{|M_I|}{|M_J(1)|} \right\} = \min\left\{1, \frac{|4x^3(y^2+1)|}{|2x^4y - 3y^2 - 2y|}\right\}.$$

可算得 $K_0(f,M) = \{-1\}$，$K_\infty(f,M) = \emptyset$。

例 1.2.2 (续) 记 $g_1 = x^3 + x^2 - y^2$。f 和 g_1 关于 x,y 的雅可比矩阵是：

$$\mathrm{Jac}(f,g_1) = \begin{pmatrix} 0 & 1 \\ 3x^2 + 2x & -2y \end{pmatrix}.$$

仍然使用定义 4.2.3中的记号，$A = (0,1), B = (3x^2+2x, -2y), C = \mathrm{Jac}(f,g_1)$。对应的指标集是 $I = (1,2), J = (1)$ 或 $(2), j = 1$。因此，

$$\begin{aligned} g'\left(df(x,y), T_{(x,y)}M\right) &= \max_I \left\{ \min_{J\subset I} \frac{|M_I|}{|M_J(1)|} \right\} \\ &= \min\left\{1, \frac{|3x^2+2x|}{|2y|}\right\} = \min\left\{1, \frac{|3x^2+2x|}{2\sqrt{x^3+x^2}}\right\}. \end{aligned}$$

于是，可算得：

- $K_0(f,M) = \{y \in \mathbb{R} \mid 3x^2 + 2x = 0, (x,y) \in M\} = \left\{\pm\left(2\sqrt{3}\right)/9\right\}$;
- $K_\infty(f,M) = \emptyset$ (因为对 $(x_l,y_l) \in M$，若 $\|x_l,y_l\| \to \infty$，则 $g' \to \infty$);
- $K_1(f,M) = \emptyset$ (因为对 $(x_l,y_l) \in M$，若 $(x_l,y_l) \to (0,0)$，则 $g' \to 1$)。

故 $K(f,M) \cup K_1(f,M) = \left\{\pm\left(2\sqrt{3}\right)/9\right\}$。

令 $V \subset \mathbb{R}^m$ 是一个等维实代数集，$\mathbf{I}(V)$ 是 V 的 $\mathbb{R}[X]$ 中的零化理想，即

$$\mathbf{I}(V) = \{g \in \mathbb{R}[X] \mid g(x) = 0,\ \forall x \in V\}.$$

假设 $\mathbf{I}(V) = \langle g_1, \ldots, g_s \rangle$。$g_1, \ldots, g_s$ 在 $x \in V$ 处的雅可比矩阵是：

$$J(x) = \begin{pmatrix} \frac{\partial g_1}{\partial X_1}(x) & \cdots & \frac{\partial g_1}{\partial X_n}(x) \\ \vdots & & \vdots \\ \frac{\partial g_s}{\partial X_1}(x) & \cdots & \frac{\partial g_s}{\partial X_n}(x) \end{pmatrix}.$$

下面介绍引自 [53, Section 4] 中的一些记号。我们将在4.3节中看到，这些记号与函数 g' 有关。

假设 V 的维数是 d 且 $d > 0$，令 $f : V \to \mathbb{R}^m$ 是一个支配 (dominant) 多项式映射。对于 $x \in M$，$J(x)$ 的秩为 $n-d$。令 $r = n-d$，B 是 $J(x)$ 的前 r 行构成的一个 $(r \times n)$ 矩阵。不失一般性，假设 B 是行满秩的，即 $\operatorname{rank}(B) = r$。令

$$C = \begin{pmatrix} df(x) \\ B \end{pmatrix} \in \mathbb{R}^{(m+r)\times n}.$$

因为 f 是支配映射，所以 $m \le d$，于是 $m + r \le n$。

给定一个指标集 $I = (i_1, \ldots, i_{m+r}) \subset \{1 \ldots, n\}$，以 I 为列指标，选取 C 中对应的 $((m+r)\times(m+r))$ 阶子式，记为 $M_I(x)$。然后，对于 $j \in I$ 和 $k \in \{1, \ldots, m\}$，去掉 $M_I(x)$ 的第 j 列和第 k 行得到一个新的 $((m+r-1)\times(m+r-1))$ 阶子式，记为 $M_{I(k,j)}(x)$。显然，$M_I(x)$ 和 $M_{I(k,j)}(x)$ 是 V 上的多项式函数。定义

$$W_{I(k,j)}(x) = \frac{M_I(x)}{M_{I(k,j)}(x)}, \tag{4-6}$$

其中，如果 $M_{I(k,j)} \equiv 0$ 则令 $W_{I(k,j)} \equiv 0$。

令 $q = \binom{n}{m+r}$，$M_{I_1}, \ldots, M_{I_q}$ 表示 C 的所有可能的 $((m+r)\times(m+r))$ 阶子式。对于 $l \in \{1, \ldots, q\}$，取 $k_l \in \{1, \ldots, m\}$ 和 $j_l \in I_l$，那么 (k_l, j_l) 可以确定一个 M_{I_l} 的一个 $((m+r-1)\times(m+r-1))$ 阶子式 $M_{I_l(k_l,j_l)}$。记

$$(k, j) = ((k_1, j_1), \ldots, (k_1, j_q)),$$

存在 l 和 (k_l, j_l)，使得 $W_{I_l(k_l,j_l)} \not\equiv 0$ (否则，g' 在 M 上恒等于 0，但这是不可能的)。换句话说，存在序列 (k, j) 使得如下有理映射的最后 $(n+1)\times q$ 个分量不

恒为零：

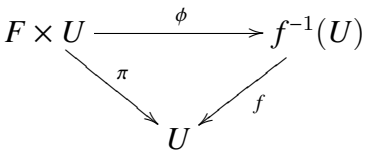
$$\begin{aligned}\Phi_{(k,j)} : M- \to & \mathbb{R}^m \times \mathbb{R}^{(n+1)\times q} \\ x \longmapsto & (f(x), W_{I_1(k_1,j_1)}(x), x_1 W_{I_1(k_1,j_1)}(x), \ldots, x_n W_{I_1(k_1,j_1)}, \ldots, \\ & W_{I_q(k_q,j_q)}(x), x_1 W_{I_q(k_q,j_q)}(x), \ldots, x_n W_{I_q(k_q,j_q)}(x)).\end{aligned} \tag{4-7}$$

如果某个序列 $(k,j) = ((k_1,j_1)\ldots,(k_q,j_q))$ 使得所有的 $W_{I_l(k_i,j_i)} \equiv 0\,(i = 1,\ldots,q)$，则令 $\Phi_{(k,j)} \equiv 0$。如果 $\Phi_{(k,j)} \not\equiv 0$，那么 $\Phi_{(k,j)}(M)$ 在欧氏拓扑下的闭包的维数等于 V 的维数。我们把欧氏拓扑下的闭包记为 $\mathrm{cl}\,(\cdot)$。定义

$$\Gamma(k,j) = \mathrm{cl}\left(\Phi_{(k,j)}(M)\right). \tag{4-8}$$

4.2.2　纤维丛

定义 4.2.4 [79] 令 E，B 是两个拓扑空间，b 是 B 中的一个点。设 $f : E \to B$ 是一个连续的满射，$F = f^{-1}(b)$ 是 f 的一个纤维 (fiber)。如果满足：对于任一 $x \in B$，存在 x 的一个开邻域 $U \subset B$ 和一个同胚 $\phi : F \times U \to f^{-1}(U)$ 使得下面的图交换：



则称映射 $f : E \to B$ 是一个纤维丛 (fiber bundle) 或局部平凡的纤维化 (locally trivial fibration)。这里，π 是从 $F \times U$ 到 U 的典范投射 (canonical projection)。

下面的定理是 [52, Theorem 6.1] 的一种特殊情形。

定理 4.2.5 [52, Theorem 6.1] 令 $S \subset \mathbb{R}^n$ 是一个完备的光滑流形，S' 是 S 的一个开子集，$f : S \to \mathbb{R}^m$ 是一个支配多项式映射。设 $W \subset \mathbb{R}^m$ 是 $\mathbb{R}^m \setminus K\,(f,S)$ 的一个连通分支。如果映射 f 满足下述条件：

$$\text{不存在序列}(x_l) \subset S' \text{ 使得} \lim_{l\to\infty} x_l \in \partial S' \text{ 且} \lim_{l\to\infty} f(x_l) \in \mathbb{R}^m, \tag{4-9}$$

则 $f^{-1}(W) = \emptyset$ 或 $f : f^{-1}(W) \to W$ 是一个纤维丛。这里，$\partial S'$ 表示 S' 在 S 中的边界。

定理 4.2.6 ([53, Theorem 3.3],[49, Theorem 3.1]) 令 V 是 $\mathbb{R}^n$ 中的一个等维非奇异实代数簇，$f : V \to \mathbb{R}^m$ 是一个支配多项式映射。则集合 $K(f,V)$ 是 $\mathbb{R}^m$ 中的闭半代数集，且它的维数小于 m。

4.3 新的集合 $K_1(f,M)$ 及其性质

令 V 是 $\mathbb{R}^n$ 中的一个等维实代数簇，它的维数是 d，$\mathrm{Reg}(V)$ 表示 V 中所有在 d 维非奇异的点构成的集合，记 $M = \mathrm{Reg}(V)$。令 $f : V \to \mathbb{R}^m$ 是一个多项式映射。我们在第一章中提到过分歧集的概念，这里简单回忆一下。对于 $y \in \mathbb{R}^m$，如果 f 在 y 的某个开邻域上是一个光滑纤维化，则称 y 为 f 的一个典型值，否则称 y 为 f 的非典型值。用 $B(f)$ 表示 f 的所有非典型值构成的集合。$B(f)$ 称为 f 的分歧集。对于映射 $f|_M$，记 $B(f,M) = B(f|_M)$。

如果 V 是非奇异的，即 $V = M$，那么它就是 $\mathbb{R}^n$ 的一个完备光滑子流形(见命题 4.2.1)，此时，由定理 4.2.5 可知，$B(f,V)$ 包含在 $K(f,V)$。如果 $V \neq M$ 那么 V 可能就不是一个光滑流形。这时，尽管 V 的子集 M 仍然是 $\mathbb{R}^n$ 中的一个光滑流形，但 M 不完备。例 1.2.1 已说明在这种情形下，$B(f,M)$ 未必包含在 $K(f,M)$ 中。

为了能刻画 $f|_M$ 的分歧集 $B(f,M)$，我们引入下列集合：

$$\begin{aligned} K_1(f,M) = \{y \in \mathbb{R}^m \mid \exists\, x_l \in M, x \in V \setminus M, x_l \to x \text{ s.t.} \\ f(x_l) \to y \text{ 且} v(df(x_l), T_{x_l}M) \to 0\}. \end{aligned} \tag{4-10}$$

在例 1.2.1中，计算可得 $K(f,M) = \{0\}$，因此对于这个例子有：$K(f,M) \cup K_1(f,M) = B(f,M)$。遗憾的是，这个等式并非总是成立。事实上，例 1.2.2 就表明 $K(f,M)$ 与 $K_1(f,M)$ 的并集仍然不足以刻画 $B(f,M)$。尽管如此，$K_1(f,M)$ 仍然有助于求解优化问题，这将在 4.4 节中分析。下面先介绍 $K_1(f,M)$ 的性质。

我们先约定一些记号。$\mathbb{Z}_+$ 表示正整数集合。令 $\mathbf{I}(V) = \langle g_1, \ldots, g_s \rangle$ 是 V 在 $\mathbb{R}[X_1, \ldots, X_n]$ 中的零化理想。由命题 2.2.10 可知，$V \setminus M$ 是 $\mathbb{R}^n$ 中的一个实代数集，因此假设

$$V \setminus M = \{x \in \mathbb{R}^n \mid h_1(x) = \ldots, = h_p(x) = 0\},$$

其中 $h_1,\ldots,h_p \in \mathbb{R}[X_1,\ldots,X_n]$。于是，

$$M = \{x \in \mathbb{R}^n \mid x \in V,\ \exists\, h_i(x) \neq 0, 1 \leq i \leq p\}. \tag{4-11}$$

对于 $i = 1,\ldots,p$ 和 $k \in \mathbb{Z}_+$，令

$$V_i^k = \left\{(x,t) \in \mathbb{R}^{n+1} \mid g_1(x) = 0,\ldots,g_s(x) = 0, h_i(x)t^k = 1\right\}. \tag{4-12}$$

那么对于每一个 $k \in \mathbb{Z}_+$，有

$$M = \bigcup_{i=1}^{p} \pi(V_i^k), \tag{4-13}$$

其中 $\pi : \mathbb{R}^{n+1} \to \mathbb{R}^n$ 是到前 n 个坐标的投射，即 $\pi(x,t) = x$。

引理 4.3.1 *如果 V_i^k (见 (4-12)) 非空，那么它是 $\mathbb{R}^{n+1}$ 中的一个 d 维等维非奇异实代数簇。*

证明 只需证明上述对 V_1^1 和 V_1^2 成立。

记 $W = V_1^1$，假设 $V_1^1 \neq \emptyset$。那么半代数集 $S = V \cap \{x \in \mathbb{R}^n \mid h_1(x) \neq 0\}$ 是 V 的一个非空子集。因为 S 中的每一个点 x 都在 d 维非奇异，由命题 4.2.1，可知 $\dim S = \dim V = d$。定义映射：

$$\begin{aligned} \phi : S &\longrightarrow W \\ x &\longmapsto (x, h_1(x)^{-1}). \end{aligned}$$

显然，ϕ 是从 S 到 W 的半代数双射，因此 W 的维数和 S 的维数相等，故 $\dim W = d$ [58, 52 页，Theorem 2.8.8]。

现在用反证法证明 W 是等维的。假设 W 有一个维数小于 d 的不可约分支 W_1。令 W_2 是 $W \setminus W_1$（$\mathbb{R}^n$ 中的的 Zariski 闭包，则 $W = W_1 \cup W_2$ 且 $W_1 \not\subset W_2$。因此，$W_1 \setminus W_2$ 是 W_1 的一个开子集，故对于 $W_1 \setminus W_2$ 中的任意一个点 $z = (x,t)$，存在 z 的一个开邻域 $U_z \subset W_1$ 使得 $U_z \subset W_1 \setminus W_2$。另一方面，因为映射 ϕ 是连续的，因此存在 x 的一个开邻域 $U_x \subset S$，使得 $\phi(U_x) \subset U_z$。此外，U_x 的维数等于 S 的维数，故 $\dim U_x = d$。于是就得到以下矛盾：

$$d = \dim U_x = \dim \phi(U_x) \leq \dim U_z \leq \dim W_1 < d.$$

最后，还需证明 W 是非奇异的。令 (x,t) 是 W 中的任意一个点，T 是一个新的变元。$g_1,\dots,g_s,h_1T-1$ 关于 $X_1,\dots,X_n,T$ 的雅可比矩阵在 (x,t) 处的取值是：

$$J(x,t)=\begin{pmatrix} \frac{\partial g_1}{\partial X_1}(x) & \dots & \frac{\partial g_1}{\partial X_n}(x) & 0 \\ \vdots & & \vdots & 0 \\ \frac{\partial g_s}{\partial X_1}(x) & \dots & \frac{\partial g_s}{\partial X_n}(x) & 0 \\ \frac{\partial h_1}{\partial X_1}(x)t & \dots & \frac{\partial h_1}{\partial X_n}(x)t & h_1(x) \end{pmatrix}.$$

因为 $x\in V$ 在 d 维非奇异，由雅可比准则 (见定理 2.2.9) 可知，矩阵 $J(x,t)$ 前 s 行的秩为 $n-d$。又因为 $h_1(x)\neq 0$，故矩阵 $J(x,t)$ 的秩为 $n-d+1$。由于 $g_1,\dots,g_s,h_1T-1\in\mathbf{I}(V_1^1)=\mathbf{I}(W)$，再由雅可比准则可知 (x,t) 在 d 维非奇异。因为 (x,t) 是 W 中的任意一个点，故 W 也是非奇异的。

对于 V_1^2，假设 $V_1^2\neq\emptyset$，令 $S'=V\cap\{x\in\mathbb{R}^n\mid h_1(x)>0\}$。考虑下面两个单射：

$$\begin{aligned} \phi_1: S' &\longrightarrow V_1^2 & \qquad \phi_2: S' &\longrightarrow V_1^2 \\ x &\longmapsto (x,h_1(x)^{-\frac{1}{2}}), & x &\longmapsto (x,-h_1(x)^{-\frac{1}{2}}). \end{aligned}$$

于是 $V_1^2=\phi_1(S')\cup\phi_2(S')$，因此 $\dim V_1^2=\max\{\dim\phi_1(S'),\dim\phi_2(S')\}=\dim S'$。与上述针对 V_1^1 的证明类似，可证得 V_1^2 也是 $\mathbb{R}^{n+1}$ 中的一个 d 维等维的非奇异实代数簇。 □

命题 4.3.2 令 $f:V\to\mathbb{R}^m$ 是一个多项式映射。如果 $\mathbb{R}^n$ 和 $\mathbb{R}^m$ 上的范数是半代数的，则函数 $x\mapsto v(df(x))$ 是从 M 到 $\mathbb{R}$ 上的一个连续半代数函数。

证明 与 [49, Proposition 2.4] 的证明类似。 □

注释 4.3.3 对于多项式映射 $f:V\to\mathbb{R}^m$，如果 V 不是非奇异的，那么函数 $x\mapsto v(df(x))$ 在 V 上可能不连续。在例 1.2.2 中，函数 $x\mapsto v(df(x))$ 在 $(0,0)\in V$ 处就是不连续的。

引理 4.3.4 令 $f:V\to\mathbb{R}^m$ 是一个多项式映射，$\pi:\mathbb{R}^{n+1}\to\mathbb{R}^n$ 是到前 n 个坐标的投射，记 $\tilde{f}$ 为 f 和 π 的复合：$f\circ\pi:V_i^k\to\mathbb{R}^m$。那么对每一个 $y\in K_1(f,M)$ (见 (4-10)), 存在 $i\in\{1,\dots,p\}$ 和 $L\in\mathbb{Z}_+$ 使得 $y\in K_\infty(\tilde{f},V_i^L)$。

证明 令 $y \in K_1(f, M)$，存在序列 M 中的 (x_l) 和 $\bar{x} \in V \setminus M$ 使得 $x_l \to \bar{x}$，$f(x_l) \to y$ 且 $v(df(x_l)) \to 0$。由 (4-13), 不失一般性，假设对于 $k \in \mathbb{Z}_+$，(x_l) 有一个无穷子序列 (x_j) 包含在 $\pi(V_1^k)$ 中，于是得到无穷序列 $(x_j, t_j) = (x_j, h_1(x_j)^{-\frac{1}{k}}) \in V_1^k$ 使得

$$\text{当} j \to \infty \text{ 时，} \|(x_j, t_j)\| \to \infty, \tilde{f}(x_j, t_j) \to y. \tag{4-14}$$

记 $M_1^k = \pi(V_1^k)$，则 $\bar{x} \in \mathrm{cl}(M_1^k)$。由定理 2.2.18，存在一个连续的半代数映射 $\gamma : [0,1] \to \mathbb{R}^n$ 使得 $\gamma(0) = \bar{x}$ 且 $\gamma((0,1]) \subset M_1^k$。根据命题 2.2.16 和命题 4.3.2，函数 $t \mapsto v(df(\gamma(t)))$ 是从 $[0,1]$ 到 $\mathbb{R}$ 的连续半代数函数。因此，

$$v(df(\gamma(0))) = v(df(\bar{x})) = 0.$$

所以，$t = 0$ 是函数 $v(df(\gamma(t)))$ 的零点。另一方面，h 和 γ 复合 $h_1 \circ \gamma : [0,1] \to \mathbb{R}$ 也是一个连续的半代数函数，于是有

$$h_1 \circ \gamma(0) = h_1(\bar{x}) = 0.$$

更进一步，因为 $h_1(\gamma((0,1]))$ 包含在 $h_1(M_1^k)$ 中且 $0 \notin h_1(M_1^k)$，故 $t = 0$ 是 $h_1 \circ \gamma$ 在 $[0,1]$ 上唯一的零点。于是，在区间 $[0,1]$ 上，$h_1 \circ \gamma(t)$ 的零点集包含在 $v(df(\gamma(t)))$ 的零点集中。由 Łojasiewicz 不等式 (见定理 2.2.19)，存在正整数 L_1 和常数 $c > 0$ 使得在 $[0,1]$ 上，有下列不等式：

$$|v(df(\gamma(t)))|^{L_1} \le c \cdot |h_1 \circ \gamma(t)|.$$

令 $L = L_1 + 1$，可得

$$\text{当} t \to 0 \text{ 时，} |h_1 \circ \gamma(t)|^{-\frac{1}{L}} v(df(\gamma(t))) \to 0.$$

又因为 $h_1 \circ \gamma(t)$ 和 $v(df(\gamma(t)))$ 是连续的，所以

$$\text{当} j \to \infty \text{ 时，} |h_1(x_j)|^{-\frac{1}{L}} v(df(x_j)) \to 0. \tag{4-15}$$

令 $z_j = (x_j, h_1(x_j)^{-\frac{1}{L}}) \in V_1^L$，因为 (x_j) 是有界的，(4-15) 等价于：

$$\text{当} j \to \infty \text{ 时，} \|z_j\| v(df(x_j)) \to 0. \tag{4-16}$$

再根据 (4-14) 可得 当 $j \to \infty$ 时，$\|z_j\| \to \infty, \tilde{f}(z_j) \to y$。

下面证明 $v(d\tilde{f}(z_j)) \leq v(df(x_j))$。将 $\mathbb{R}^n$ 看作 $\mathbb{R}^{n+1}$ 的一个子空间。因为 $g_1,\ldots,g_s \in \mathbf{I}(V_1^L)$，所以 V_1^L 在 z_j 的切空间包含在 M 在 x_j 的切空间，即 $T_{z_j}(V_1^L) \subset T_{x_j}(M)$。分别记 Σ_1 和 Σ_2 为 $T_{z_j}(V_1^L)$ 到 $\mathbb{R}^m$ 和 $T_{x_j}(M)$ 到 $\mathbb{R}^m$ 的非满线性映射组成的集合。于是 Σ_2 包含在 Σ_1 中，由命题 4.2.2，有 $v(d\tilde{f}(z_j)) \leq v(df(x_j))$。

最后，结合 (4-16) 与不等式 $v(d\tilde{f}(z_j)) \leq v(df(x_j))$，有

$$\|z_j\| v(d\tilde{f}(z_j)) \to 0 \text{ as } j \to \infty.$$

注意到 $y = \lim_{j\to\infty} \tilde{f}(z_j)$，所以 $y \in K_\infty(\tilde{f}, V_1^L)$。 □

定理 4.3.5 令 $f : V \to \mathbb{R}^m$ 是一个多项式映射。集合 $K_1(f,M)$ 的勒贝格测度为零。

证明 由引理 4.3.1，每一个非空的实代数簇 V_i^k 都是等维非奇异的，于是由定理 4.2.6，每一个 $K(\tilde{f}, V_i^k)$ 的勒贝格测度都为零。此外，由引理 4.3.4，$K_1(f,M)$ 包含在 $\bigcup_{i,k} K_\infty(\tilde{f}, V_i^k)$ 中。又因为可数个零测度集的并仍然是一个零测度集，故 $K_1(f,M)$ 的勒贝格测度为零。

□

4.4 最优值的表示

保留上一节的符号。我们先证明 $K(f,M)$ 和 $K_1(f,M)$ 的并是 $\mathbb{R}^m$ 的一个半代数闭集。然后令 $m=1$，考虑 f 是多项式函数的情形，证明：如果 f 在 V 上的全局下确界 f^* 存在，那么它一定包含在 $K(f,M)$ 和 $\mathrm{cl}(f(V \setminus M))$ 的并集中。

如果 V 是等维非奇异的，那么下面的等式是 [53, Lemma 4.3] 的一个直接推论：

$$K(f,V) = K_0(f,V) \cup K_\infty(f,V) = \bigcup_{(k,j)} (\Gamma(k,j) \cap \mathbb{R}^m), \tag{4-17}$$

如果 V 不是非奇异的，那么考虑映射 $f|_M$，则 $\Gamma(k,j) = \mathrm{cl}\left(\Phi_{(k,j)}(M)\right)$ (见 (4-8))，把 V 替换为 M，此时等式 (4-17) 不一定成立。

例 4.4.1 考虑 $\mathbb{R}^2$ 中的曲线：

$$V = \left\{(x,y) \in \mathbb{R}^2 \mid x^2 - y^3 = 0\right\},$$

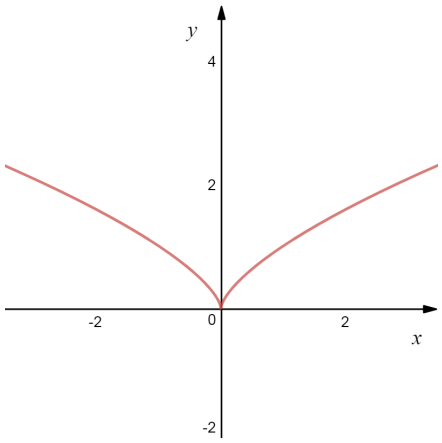


图 4.1　例 4.4.1

令 f 是从 V 到 x 轴的投射，即 $f(x,y)=x$。

记 $g_1=x^2-y^3$。此时，$M=V\setminus\{(0,0)\}$。f 和 g_1 关于 x,y 的雅可比矩阵是：

$$\mathrm{Jac}(f,g_1)=\begin{pmatrix}1 & 0\\ 2x & -3y^2\end{pmatrix}.$$

使用定义 4.2.3中的记号，$A=(1,0),B=(2x,-3y^2),C=\mathrm{Jac}(f,g_1)$，相应的指标集为：$I=(1,2),J=(1)\text{ or }(2),j=1$。于是，

$$g'\left(df(x,y),T_{(x,y)}M\right)=\max_I\left\{\min_{J\subset I}\frac{|M_I|}{|M_J(1)|}\right\}=\min\left\{1,\frac{3y^2}{|2x|}\right\}=\min\left\{1,\frac{3y^2}{2\sqrt{y^3}}\right\}.$$

计算可得：

- $K_0(f,M)=\emptyset$ (因为对任意的 $(x,y)\in M$，有 $g'>0$)。
- $K_\infty(f,M)=\emptyset$ (对于 M 中的序列 (x_l,y_l)，若 $\|(x_l,y_l)\|\to\infty$，则 $g'\to 1$)。

因此，$K(f,M)=\emptyset$。但 $\Gamma((1,2))\cap\mathbb{R}=\{0\}$。

对于例 4.4.1，进一步计算可得 $\Gamma((1,1))\cap\mathbb{R}=\emptyset$，$K_1(f,M)=\{0\}$。于是在这个例子中，$K(f,M)\cup K_1(f,M)=\bigcup_{(k,j)}(\Gamma(k,j)\cap\mathbb{R}$。下面我们证明这个等式在一般的情形下也成立。

定理 4.4.2 令 $\Gamma(k,j)$ 是 (4-8) 中定义的集合，则下面的等式成立：

$$K(f,M)\cup K_1(f,M)=\bigcup_{(k,j)}(\Gamma(k,j)\cap\mathbb{R}^m),\tag{4-18}$$

这里，我们将 $\mathbb{R}^m$ 等同于 $\mathbb{R}^m \times (0,\ldots,0)$。

证明 由 [78, Propostions 2.4，2.5]，可将 $K(f,M)$ 和 $K_1(f,M)$ 的定义中的函数 v 替换为 g'。

先证明对于每个 (k,j)，集合 $\Gamma(k,j)\cap\mathbb{R}^m$ 包含在 $K(f,M)\cup K_1(f,M)$。如果 $y\in\Gamma(k,j)\cap\mathbb{R}^m$, 那么存在 M 中的序列 (x_l) 使得

$$\text{当} l\to\infty \text{ 时，}\ \frac{M_{I_i}(x_l)}{M_{I_i(k_i,j_i)}(x_l)}\to 0,\ \|x_l\|\frac{M_{I_i}(x_l)}{M_{I_i(k_i,j_i)}(x_l)}\to 0,\ \forall I_i.$$

假设 (x_l) 有一个收敛的子序列，且这个子序列收敛到 V 中的一点 $\bar{x}$，那么 $y=f(\bar{x})$，且对于所有的 I_i 有 $M_{I_i}(\bar{x})=0$。因此，$y\in K_0(f,M)\cup K_1(f,M)$ (如果 $\bar{x}\in M$，则 $y\in K_0(f,M)$, 或者 $\bar{x}\in V\setminus M$ 则 $y\in K_1(f,M)$)。否则，有

$$\text{当} l\to\infty \text{ 时，}\ \|x_l\|\to\infty,\ f(x_l)\to y,\ \|x_l\|g'(df(x_l))\to 0,$$

这意味着 $y\in K_\infty(f,M)$。

反过来，如果 $y\in K(f,M)\cup K_1(f,M)$，那么分两种情形讨论：

情形 I: 假设 $y\in K_0(f,M)\cup K_1(f,M)$, 则存在 M 中的序列 (x_l) 使得 $\lim_{l\to\infty}x_l\in V$，$\lim_{l\to\infty}f(x_l)=y$ 且 $\lim_{l\to\infty}g'(df(x_l))=0$。因此对于所有的指标集 I_i，都存在 (k_i,j_i) 使得

$$\frac{M_{I_i}(x_l)}{M_{I_i(k_i,j_i)}(x_l)}\to 0.$$

于是，$y\in \mathrm{cl}\left(\Phi_{(k,j)}(M)\right)\cap\mathbb{R}^m=\Gamma(k,j)\cap\mathbb{R}^m$，其中 (k,j) 表示序列 $((k_1,j_1),\ldots,(k_q,j_q))$。

情形 II: 假设 $y\in K_\infty(f,M)$，那么存在 M 中的序列 (x_l) 使得

$$\text{当} l\to\infty \text{ 时，}\ \|x_l\|\to\infty,\ f(x_l)\to y,\ \|x_l\|g'(df(x_l))\to 0.$$

由此，$y\in \mathrm{cl}\left(\Phi_{(k,j)}(M)\right)\cap\mathbb{R}^m=\Gamma(k,j)\cap\mathbb{R}^m$。

□

推论 4.4.3 令 $f:V\to\mathbb{R}^m$ 是一个多项式映射。那么 $K_1(f,M)\cup K(f,M)$ 是 $\mathbb{R}^m$ 中半代数闭集，且它的勒贝格测度为零。特别地，$K_1(f,M)\cup K(f,M)$ 的维数小于 m。

证明 由定理 4.4.2 可知 $K_1(f,M)\cup K(f,M)$ 是一个半代数闭集。另一方面，[53, Theorem 3.3] 的证明可直接推广到映射 $f|_M$ 上，由此得出 $K(f,M)$ 是 $\mathbb{R}^m$ 中勒贝格测度为零的半代数集。最后，定理 4.3.5 表明 $K_1(f,M)$ 在 $\mathbb{R}^m$ 中的勒贝格测度也为零。命题得证。

□

注释 4.4.4 如果把实数域 $\mathbb{R}$ 替换成复数域 $\mathbb{C}$，实代数簇 V 替换成一个复代数簇，M 替换为 $V\setminus \mathrm{Sing}(V)$，那么定理 4.3.5，定理 4.4.2 和推论 4.4.3 仍然成立 (见 [52, Lemma 8.1])。

现在，令 $f: V\to\mathbb{R}$ 是一个多项式函数。其他的设定和符号保持不变。

定理 4.4.5 令 $f\in\mathbb{R}[X_1,\dots,X_n]$，$V\subset\mathbb{R}^n$ 是一个等维的实代数簇，记 $d=\dim V$。假设 $d>0$，则 $\inf_{x\in V} f(x)>-\infty$ 当且仅当 $\inf_{x\in V} f(x)$ 包含在 $K(f,M)\cup \mathrm{cl}(f(V\setminus M))$。

证明 记 $f^*=\inf_{x\in V} f(x)$，假设 $f^*>-\infty$。我们用反证法证明 f^* 包含在 $K(f,M)\cup \mathrm{cl}(f(V\setminus M))$。

反设 $f^*\notin K(f,M)\cup \mathrm{cl}(f(V\setminus M))$。将 V 看成 $\mathbb{R}^n$ 的子拓扑空间，因为 $V\setminus M$ 在 V 中是闭的 (见命题 2.2.10)，所以 M 是 V 的一个开子集。因此 ∂M 包含在 $V\setminus M$ 中。由定理 4.2.5，存在 f^* 的一个开邻域 $U=(f^*-\epsilon,f^*+\epsilon)\subset\mathbb{R}$，使得 $f: f^{-1}(U)\to U$ 是一个平凡纤维丛，即存在同胚 $\phi: f^{-1}(f^*)\times U\to f^{-1}(U)$ 使得下面的图交换：

$$\begin{array}{ccc} f^{-1}(f^*)\times U & \xrightarrow{\ \phi\ } & f^{-1}(U) \\ & {\scriptstyle\pi}\searrow \quad \swarrow{\scriptstyle f} & \\ & U & \end{array}$$

此外，因为 $f^*\notin \mathrm{cl}(f(V\setminus M))$，我们可以将 ϵ 取得足够小使得 $U\cap \mathrm{cl}(f(V\setminus M))=\emptyset$。于是，$f^{-1}(U)\cap(V\setminus M)=\emptyset$，故 $f^{-1}(U)\subset M$。因此对于 $y=f^*-\frac{\epsilon}{2}\in U$，存在 $x\in f^{-1}(U)\subset M$ 使得 $f(x)=y$。这与 f^* 是全局下确界矛盾。

□

由定理 4.4.2 和推论 4.4.3，可以看出 $K(f,M)\cup K_1(f,M)$ 等于 $\bigcup_{(k,j)}(\Gamma(k,j)\cap\mathbb{R})$，且它是一个有限集。这就意味着 $\Gamma(k,j)\cap\mathbb{R}$ 是 $\mathbb{R}$ 中的一个实代数集，即它

是 Zariski 闭的。于是它可以用 Gröbner 基计算 [参见 54, 138 页, Chapter 3 §3, Theorem 2]。这样，我们就可以得到包含 $K(f, M)$ 的一个有限集。因为 $V \setminus M$ 也是一个实代数簇 (命题 2.2.10)，且它的维数小于 V 的维数，所以可以对 $V \setminus M$ 的每个等维分支做递归，由此就能得到包含 f^* 的一个有限集。下一节我们给出详细的算法。

4.5 算法

4.5.1 算法描述

现在我们回到本章开篇提到的问题：给定多项式 f 和实代数簇 V，计算 f 在 V 上的全局下确界：

$$f^* = \inf_{x \in V} f(x).$$

在这一节，我们给出求解上述问题的一个符号算法。因为计算机代数系统中计算 Gröbner 基的算法大都是针对有理系数多项式，所以我们假设所有的计算都是在有理系数多项式环中执行。因为 $\mathbb{Q} \subset \mathbb{R}$ 而且有理系数多项式的实代数簇是指其所有的实根，因此 4.3 节和 4.4 节中的结论对有理系数多项式都成立。当然，如果下面提到的算法都能在实系数多项式环中执行，那么上述假设便可去掉。

令 f 是 $\mathbb{Q}[X] = \mathbb{Q}[X_1, \ldots, X_n]$ 中的一个多项式，$G = (g_1, \ldots, g_s)$ 是 $\mathbb{Q}[X]$ 的一组多项式。令 V 是 G 的实代数簇，即 $V = \{x \in \mathbb{R}^n \mid g_1(x) = 0, \ldots, g_s(x) = 0\}$，算法的目的是计算 $f^* = \inf_{x \in V} f(x)$。

首先介绍算法中需要用到的几个子程序。

计算实根理想：RealRadical. 输入 $\mathbb{Q}[X]$ 中的一组多项式 $G = (g_1, \ldots, g_s)$，输出 $\sqrt[re]{\langle G \rangle}$ 的一组生成元。由实零点定理 (见定理 2.2.5)，$\sqrt[re]{\langle G \rangle}$ 等于 $\mathbf{I}(\mathbf{V}_{\mathbb{R}}(G))$，所以这个算法输出的是 $\mathbf{V}_{\mathbb{R}}(G)$ 零化理想的一组生成元。对于这个算法的细节，可参考 [1, 2, 4, 5]。

计算等维分解：EquidimensionalDecomposition. 输入 $\mathbb{Q}[X]$ 中的一组多项式 $G = (g_1, \ldots, g_s)$，假设 $\langle G \rangle$ 满足条件：对于 $\langle G \rangle$ 的任一极小准素分解 $\langle G \rangle = \bigcap_i Q_i$，若 $i \neq j$，则 $\sqrt{Q_i} \not\subset \sqrt{Q_j}$。注意到根理想都满足这个条件。算法输出 $\langle G \rangle$ 的所有等维部分的生成元 (参见 [55, 280 页，Algorithm 4.4.9] 或 [80, Chapter 8])。

计算有理映射像的 Zariski 闭包：Image. 输入定义有理映射 $\Phi : V \to \mathbb{R}^q$ 的多项式以及理想 $\mathbf{I}(V)$ 的一组生成元，输出 $\Phi(V)$ 的 Zariski 闭包的一组定义多项式。这个算法是基于消元理论 (elimination theory)[参见 54, 138 页, Chapter 3 §3, Theorem 2]。

计算广义关键值：GenCritValues. 输入 $f \in \mathbb{Q}[X]$ 和 $\mathbb{Q}[X]$ 中的一组多项式 $G = (g_1, \ldots, g_s)$。假设 $\langle G \rangle$ 是等维实理想。输出如下形式的一个有限集：

$$\mathscr{H} = \{\Psi \mid \Psi \text{ 是有限多个单变元多项式构成的集合}\}, \tag{4-19}$$

使得 $\bigcup_{\Psi \in \mathscr{H}} \mathbf{V}_{\mathbb{R}}(\Psi)$ 包含 $K(f, M)$ 和 $K_1(f, M)$，其中 $M = \mathrm{Reg}(\mathbf{V}_{\mathbb{R}}(G))$。这是通过计算集合 $\Gamma(k, j) \cap \mathbb{R}$ 来实现的，而集合 $\Gamma(k, j) \cap \mathbb{R}$ 可以通过 Gröbner 基计算 (参见 [54, 138 页，Chapter 3 §3, Theorem 2])。算法的原理与 [53, Section 5.1] 中的类似，但这里所有的计算都针对有理系数多项式，而非复系数多项式。

从一个有限集中找到最优值：FindInfimum. 这个算法来自 [51, Section 3.3]，我们对它做一点调整使得它适合我们的优化问题。输入 $f \in \mathbb{Q}[X]$ 和 $\mathbb{Q}[X]$ 中的一组多项式 $G = (g_1, \ldots, g_s)$，以及形如 (4-19) 的一个集合 $\mathscr{H}$。令 V 是 G 的实代数簇，假设 $f|_V$ 所有的局部极值包含在 $\bigcup_{\Psi \in \mathscr{H}} \mathbf{V}_{\mathbb{R}}(\Psi)$ 中。输出：

- 如果 f 在 V 上没有下界，输出 $-\infty$；
- 如果 f^* 存在，输出 f^* 的一个隔离区间 U。

在 [51, Section 3.3]，要求 $\langle G \rangle$ 是根理想且其复代数簇只有有限多个奇异点。但这不影响我们的使用，因为涉及到这个要求的步骤是判定一个实代数集是否为空，而对于一般的情形，有很多算法都可以用来处理这一步 [参见 64, 65, 67, 81]。

现在，我们介绍这一节的主要算法。输入 $f \in \mathbb{Q}[X]$ 和 $\mathbb{Q}[X]$ 中的一组多项式 $G = (g_1, \ldots, g_s)$。第一步是计算 $\langle G \rangle$ 实根理想。简单期间，我们仍然用 G 表示这一步得到的多项式集合。这时，如果理想 $\langle G \rangle$ 是零维的，那么调用 Image 计算一个单变元多现实使得它的实根包含 $\mathbf{V}_{\mathbb{R}}(G)$ 的像 $f(\mathbf{V}_{\mathbb{R}}(G))$。否则，调用 EquidimensionalDecomposition 计算 $\langle G \rangle$ 的所有等维部分的生成元。令 $d = \dim\langle G \rangle$，对于 $i = 0, \ldots, d$，记 $\langle G_i \rangle$ 为 $\langle G \rangle$ 的 i 维等维部分 (如果 $\langle G \rangle$ 没有 i 维等维部分，则令 $G_i = (1)$)。由命题 2.2.4 和命题 3.2.1，$\langle G \rangle$ 的每个等维部分 $\langle G_i \rangle$ 都是实的，因此 $\langle G_i \rangle$ 是 V 的一个等维分支的零化理想。所以，这里以 G 为输入，调用算法 EquidimensionalDecomposition 得到的是 V 的极小等

维分解。下一步，计算 f 限制在 $\mathbf{V}_{\mathbb{R}}(G_i)$ 的所有局部极值。这一步是通过调用算法 LocalExtEquidim 来实现的，这个算法会在后面介绍。最后一步，调用 FindInfimum，从此前得到单变元多项式的实根中找到 f^*。

Optimize(f, G)

1. res $= \{\}$;
2. $G =$ RealRadical(G);
3. if $1 \in G$ then return $+\infty$;
4. if $\dim\langle G\rangle = 0$ then
   - res $=$ Image(f, G);
   - return FindInfimum$(f, G,$ res$)$;
5. $\{G_0, \ldots, G_d\} =$ EquidimensionalDecomposition(G);
6. for $0 \le i \le d$ do
   - res $=$ res $\cup$ LocalExtEquidim(f, G_i);
7. return FindInfimum$(f, G,$ res$)$.

计算局部极值：LocalExtEquidim. 输入 $f \in \mathbb{Q}[X]$ 和 $\mathbb{Q}[X]$ 中的一组多项式 $G = (g_1, \ldots, g_s)$，假设 $\langle G\rangle$ 是等维实理想。记 V 为 G 的实代数簇。输出如下形式的一个有限集：

$$\text{res} = \{\Psi \mid \Psi \text{ 是有限多个单变元多项式构成的集合}\} \tag{4-20}$$

使得 $f|_V$ 所有的局部极值都包含在 $\bigcup_{\Psi\in\text{res}} \mathbf{V}_{\mathbb{R}}(\Psi)$ 中。记 $M = \text{Reg}(V)$。在定理 4.4.5 的证明中，我们看到 $f|_V$ 所有的极值都包含在 $K(f, M)$ 和 $\text{cl}(f(V \setminus M))$ 的并集中。而且，由推论 4.4.3，$K(f, M)$ 和 $K_1(f, M)$ 的并是一个有限集。它可以由 GenCritValues 计算得到。因此，通过对 $V \setminus M$ 的所有等维分支做递归，我们就能得到 $f|_V$ 的所有局部极值。对于 $V \setminus M$ 的计算，我们用 Jac(G) 表示 G 关于 $X_1, \ldots, X_n$ 的雅可比矩阵，用 Minors(Jac$(G), r)$ 表示 Jac(G) 所有的 $r \times r$ 阶子式。

LocalExtEquidim(f, G)

1. $d = \dim\langle G\rangle$;
2. if $d \le 0$ then return $\mathsf{Image}(f, G)$;
3. $K_G = \mathsf{GenCritValues}(f, G)$;
4. $\mathsf{res} = \mathsf{res} \cup K_G$;
5. $S_G = \mathsf{RealRadical}(\mathsf{Minors}(\mathsf{Jac}(G), n-d))$;
6. if $\dim S_G \le 0$, then $\mathsf{res} = \mathsf{res} \cup \mathsf{Image}(f, S_G)$;
7. else,
   - $\{G'_0, \ldots, G'_l\} = \mathsf{EquidimensionalDecomposition}(S_G)$;
   - for $0 \le i \le l$ do
     - $\mathsf{res} = \mathsf{res} \cup \mathsf{LocalExtEquidim}(f, G'_i)$;
8. return res.

4.5.2　算法的正确性

定理 4.5.1　令 f 是 $\mathbb{Q}[X] = \mathbb{Q}[X_1, \ldots, X_n]$ 中的一个多项式，$G = (g_1, \ldots, g_s)$ 是 $\mathbb{Q}[X]$ 中的一组多项式。记 V 为 G 的实代数簇，$f^* = \inf_{x\in V} f(x)$。算法 Optimize 将在有限步终止且，它的输出是：

- 如果 V 是空集，则输出 $+\infty$；
- 如果 f 在 V 上没有下界，则输出 $-\infty$；
- 如果 f^* 是有限的，则输出 f^* 的一个隔离区间。

证明　保留算法 Optimize 中的记号。

令 V 的极小等维分解为：$V = \bigcup_{i=0}^{d} V_i$，其中 V_i 等于空集或 V_i 是一个等维的实代数簇且维数是 i。那么 $\mathrm{cl}\,(f(V))$ 等于 $\bigcup_{i=0}^{d} \mathrm{cl}\,(f(V_i))$。另一方面，因为 f^* 包含在 $\mathrm{cl}\,(f(V))$ 中，所以 f^* 包含在某个 $\mathrm{cl}\,(f(V_i))$ 中，故 f^* 也是某个 $f|_{V_i}$ 的全局下确界。另一方面，由命题 2.2.4 和命题 3.2.1 可知，$\langle G\rangle$ 的每个等维部分 $\langle G_i\rangle$ 都是实的，所以 G_i 满足算法 LocalExtEquidim 对输入的假设条件。此外，因为 $\langle G_i\rangle$ 是实的，根据实零点定理 (见定理2.2.5)，$\langle G_i\rangle$ 等于 V_i 的零化理想。因此算法 Optimize 的正确性依赖于 LocalExtEquidim 和 FindInfimum 的正确性。

下面，我们证明 LocalExtEquidim 的正确性，对于 FindInfimum 的正确性，参见 [51, Section 4.2]。

现在假设理想 $\langle G\rangle$ 是等维实理想。我们证明 LocalExtEquidim(f,G) 将在有限步终止，且返回形如 (4-20) 的一个有限集 res，使得 $f|_V$ 所有的局部极值都包含在 $\bigcup_{\Psi\in\text{res}}\mathbf{V}_{\mathbb{R}}(\Psi)$ 中。

保留算法 LocalExtEquidim(f,G) 中的记号。由雅可比准则 (见定理 2.2.9) 和实零点定理 2.2.5，可知 $\langle S_G\rangle$ 是 $V\setminus M$ 的零化理想，因此 $\langle S_G\rangle$ 的维数小于 $\langle G\rangle$ 的维数。此外，命题 2.2.4 和命题 3.2.1 表明 $\langle S_G\rangle$ 的每个等维部分 $\langle G_i'\rangle$ 都是实的，所以 G_i' 满足算法 LocalExtEquidim 对输入的假设条件。另一方面，因为 $\langle S_G\rangle$ 的维数小于 $\langle G\rangle$ 的维数，所以于是对于递归调用中的每一个 G_i'，它生成的理想的维数都小于 $\langle G\rangle$ 的维数。又因为 $\langle G\rangle$ 是有限维的，因此算法的终止性得证。

接下来我们用归纳法证明算法的正确性。对于 $\langle G\rangle$ 是零维的情形，正确性是显然的。记 $d=\dim\langle G\rangle$，$d>0$。假设算法对于可行域维数小于 d 的情形都是正确的。

令 $y\in\mathbb{R}$ 是 $f|_V$ 的一个局部极值，记 $M=\text{Reg}(V)$。由定理 4.4.5 的证明可知，y 包含在 $K(f,M)$ 和 $\text{cl}(f(V\setminus M))$ 的并集中。如果 $y\in K(f,M)$，那么证明完成 (参见算法 GenCritValues 的描述和定理 4.4.2)。否则，对于 $i=1,\ldots,l$，令 V_i' 是 G_i' 是实代数簇，那么 $V\setminus M=\bigcup_{i=0}^{l}V_i'$，因此 y 包含在某个 $\text{cl}\left(f(V_i')\right)$ 中。又因为 $\langle G_i'\rangle$ 的维数小于 d，由归纳假设，定理得证。

□

注释 4.5.2 根据注释 4.4.4，定理 4.3.5，定理 4.4.2和推论 4.4.3对复代数簇也成立，因此可以将上述算法中计算实根理想的步骤都都替换为计算根理想，这样仍然能得到形如 (4-20) 的一个集合。此时，如果 f 在这个复代数簇上有最小实值，那么这个最小实值也包含在 $\bigcup_{\Psi\in\text{res}}\mathbf{V}_{\mathbb{R}}(\Psi)$ 中。目前，一般情况下，计算根理想比计算实根理想简单，但存在如下情况：一组多项式生成的理想是实根理想，且它的实代数簇是等维非奇异的，但其复代数簇有奇异点。这种情况下，计算根理想则需要对其复代数簇的奇异轨迹进行递归运算。而如果只考虑实代数簇和实根理想，则不需要进行递归运算。

例 4.5.3 [58, 63 页, Example 3.2.8, a)] 考虑 $\mathbb{R}^3$ 中的环面：

$$T = \left\{(x,y,z) \in\in \mathbb{R}^3 \mid 16(x^2+y^2) - (x^2+y^2+z^2+3)^2 = 0\right\}.$$

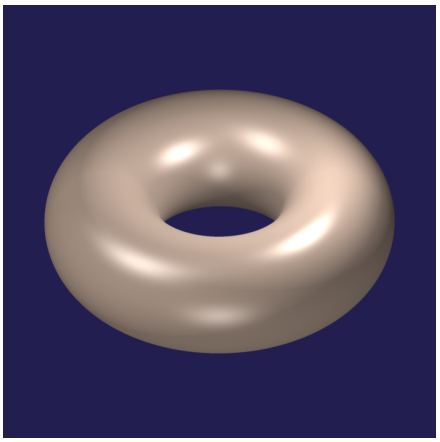


图 4.2　例 4.5.3

显然，T 是 $\mathbb{R}^3$ 中的等维非奇异曲面。记 $g_1 = 16(x^2+y^2)-(x^2+y^2+z^2+3)^2$，$g_1$ 的复代数簇 $\mathbf{V}_{\mathbb{C}}(g_1)$ 有两个奇异点 $(0,0,\pm\sqrt{-3}) \in \mathbb{C}^3$。

4.5.3　例子

例 4.5.4 考虑下述曲面：

$$V = \left\{(x_1,x_2,x_3) \in \mathbb{R}^3 \mid x_1^2 + (x_2^2+x_3)^3 = 0\right\}.$$

令 $f : V \to \mathbb{R}$ 是从多项式函数：$f(x_1,x_2,x_3) = -x_3$，要计算 f 在 V 上的全局下确界 $\inf_{x\in V} f(x)$。

记 $g = x_1^2 + (x_2^2+x_3)^3$。注意到 V 在 $\mathbb{Q}$ 上不可约。取 $G = \{g\}$，应用算法 Optimize(f,G)，我们得到

- $V_0 = V, M_0 = V_0 \setminus \left\{(x_1,x_2,x_3) \in \mathbb{R}^3 \mid x_1 = 0, x_2^2 + x_3 = 0\right\}$,

$$\mathrm{Jac}(f,G) = \begin{pmatrix} 0 & 0 & -1 \\ 2x_1 & 6x_2(x_2^2+x_3)^2 & 3(x_2^2+x_3)^2 \end{pmatrix},$$

$$I_1 = (1,2), M_{I_1} = 0, W_{I_1(1,1)} = W_{I_1(1,2)} = 0;$$

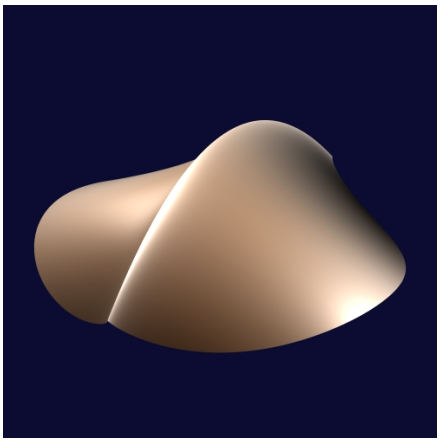


图 4.3　例 4.5.4

$$I_2 = (1,3), M_{I_2} = 2x_1, W_{I_2(1,1)} = 2x_1/3(x_2^2 + x_3)^2, W_{I_2(1,3)} = 1;$$
$$I_3 = (2,3), M_{I_3} = 6x_2(x_2^2 + x_3)^2, W_{I_3(1,2)} = 2x_2, W_{I_3(1,3)} = 1.$$

于是相应的 $\bigcup_{(k,j)} \Gamma(k,j) \cap \mathbb{R} = \emptyset$，故 $K_1(f, M_0) \cup K(f, M_0) = \emptyset$。

- $V_1 = V_0 \setminus M_0,\ M_1 = V_1,$

$$\mathrm{Jac}(f,G) = \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & 0 \\ 0 & 2x_2 & 1 \end{pmatrix},$$

$$I_1 = (1,2,3), M_{I_1} = -2x_2, W_{I_1(1,1)} = 0, W_{I_1(1,2)} = -2x_2, W_{I_1(1,3)} = -1.$$

此时，对应的 $\bigcup_{(k,j)} \Gamma(k,j) \cap \mathbb{R} = \{0\}$，因此 $K_1(f, M_1) \cup K(f, M_1) = \{0\}$. 最后，因为 $\{x \in \mathbb{R}^3 \mid f(x) = 0\} \cap V = \{(0,0,0)\}$，所以 $\inf_{x \in V} f(x) = 0$。

下面是 [51, Appendix] 中的两个例子。目前，因我们我们的算法复杂度太高 (定理 4.5.7)，暂时还不能计算 [51, Appendix] 中的例 3 和例 5。

例 4.5.5 (Greuet 2014 Example 1) $f = (x_1x_2 - 1)^2 + x_2^2 + x_3^2 + 42$, $g = x_3$。计算得到 $\mathsf{res} = \{\Psi = \{(a-42)(a-43)\}\}$，最后的结果是 42，即 $\inf_{x \in \mathbb{R}^2}\{f(x) \mid g(x) = 0\} = 42$。

例 4.5.6 (Greuet 2014 Example 2)　$f=(x_1^2+x_2^2-2)(x_1^2+z_2^2), g=(x_1^2+x_2^2-1)(x_1-3)$。计算得到 res $=\{\Psi=\{(a+1)(a-63)\}\}$，最后的结果是 -1，即 $\inf_{x\in\mathbb{R}^2}\{f(x)\mid g(x)=0\}=-1$。

定理 4.5.7　令 f 是 $\mathbb{Q}[X]=\mathbb{Q}[X_1,\ldots,X_n]$ 中的一个多项式，$G=\{g_1,\ldots,g_s\}$ 是 $\mathbb{Q}[X]$ 的一个子集。令 $D=\max\{\deg f,\deg g_1,\ldots,\deg g_s\}$，$d=\dim\langle G\rangle$。那么算法 Optimize$(f,G)$ 执行完第 6步得到的所有单变元多项式的次数不高于 $(nD)^{2^{O(dn^2)}}$。

证明　令 V 是 G 的实代数簇。如果 V 是有限集，即 $d=0$，那么 V 的像 $f(V)$ 也是有限集且它的元素个数不超过 D^n。下面我们假设 $d>0$，保留算法 Optimize 中的所有记号。

算法 Optimize 一开始调用 RealRadical 来计算 $\sqrt[re]{\langle G\rangle}$ 的生成元。由 [2, Theorem 5.9]，$\langle G\rangle$ 的生成元的次数不高于 $D^{2^{O(n^2)}}$。

接下来，调用算法 EquidimensionalDecomposition，这一步得到的多项式的次数不超过 $(D^{2^{O(n^2)}})^{2^{O(n)}}=D^{2^{O(n^2)}}$ (可参见 [82]).

然后，对于 $0\le i\le d$，以 f,G_i 为输入，调用算法 LocalExtEquidim。下面分析算法 LocalExtEquidim 输出的单变元多项式的次数。

假设 (f,G') 是算法 LocalExtEquidim 的输入，其中 $\langle G'\rangle$ 是等维实理想，且它的维数是 $r>0$。记 δ 为 G' 中多项式的最高次数。算法 LocalExtEquidim 的第一步调用 GenCritValues，得到的单变元多项式的次数不超过 $(D+(\delta-1)(n-r))^r\delta^{n-r}$ [53, Corollary 4.1]。下一步应用雅可比准则 (见定理 2.2.9) 和 RealRadical 来计算 $\mathbf{V}_{\mathbb{R}}(G')\setminus\mathrm{Reg}(\mathbf{V}_{\mathbb{R}}(G'))$。这一步得到的多项式的次数不超过 $((\delta-1)(n-r))^{2^{O(n^2)}}$。假设 $\mathbf{V}_{\mathbb{R}}(G')\setminus\mathrm{Reg}(\mathbf{V}_{\mathbb{R}}(G'))$ 的维数仍然大于零，那么需要调用 EquidimensionalDecomposition，这样将得到次数不高于 $((\delta-1)(n-r))^{2^{O(n^2)}}$ 的多项式 (参见上述关于 EquidimensionalDecomposition 的分析)。然后，对 $\mathbf{V}_{\mathbb{R}}(G')\setminus\mathrm{Reg}(\mathbf{V}_{\mathbb{R}}(G'))$ 的每个等维分支做递归。令 $T(D,\delta,r)$ 表示 LocalExtEquidim(f,G') 输出多项式的次数上界，那么有下述递归公式：

$$T(D,\delta,r)\le\max\left\{(D+(\delta-1)(n-r))^r\delta^{n-r},T\left(D,((\delta-1)(n-r))^{2^{O(n^2)}},r-1\right)\right\}.$$

求解这个递归公式，得到

$$T(D,\delta,d)\le(n\delta)^{2^{O(dn^2)}}.$$

最后，将 δ 替换为 $D^{2^{O(n^2)}}$ 即得到定理中的次数上界。

□

注释 4.5.8 这里的复杂度依赖于实根理想生成元的次数上界。在上一章中，我们给出了如下结果 (或参见 [83])：如果 G 的复代数簇是光滑的，那么它的实根理想有一组次数不超过其复代数簇次数的生成元。将这个结果应用到上述分析中，可以得到：当 G 的复代数簇等维且光滑时，定理 4.5.7 结论中的复杂度可降低为 $(D+(D^n-1)(n-r))^r D^{n(n-r)}$。

4.6 半代数情形

算法 Optimize 还可以应用到更一般的情形。给定基本半代数闭集：

$$S = \{x \in \mathbb{R}^n \mid g_1(x) \geq 0, \ldots, g_s(x) \geq 0\}$$

其中 $g_1, \ldots, g_s \in \mathbb{Q}[X_1, \ldots, X_n]$。令 $f : S \to \mathbb{R}$ 是 S 上的一个有理系数多项式函数。考虑下述优化问题：

$$\inf_{x \in S} f(x). \tag{4-21}$$

下面的定理表明 (4-21) 中的最优值可通过重复调用算法 Optimize 进行求解。我们需要引入下述符号：

- $\Lambda = \{\lambda \mid \lambda \subset \{1, \ldots, s\}\}$;
- 对于每个非空的指标集 $\lambda \in \Lambda$，令 $V_0^\lambda = \{x \in \mathbb{R}^n \mid g_i(x) = 0, i \in \lambda\}$，如果 $\lambda = \emptyset$ 则取 $V_0^\lambda = \mathbb{R}^n$。
- 对于 $i \geq 0$ 和 $\lambda \in \Lambda$，令 $M_{il}^\lambda = \mathrm{Reg}(V_{il}^\lambda)$，$V_{i+1}^\lambda = \bigcup_l \left(V_{il}^\lambda \setminus M_{il}^\lambda\right)$，其中 V_{il}^λ 是 V_i^λ 的 l 维等维分支；
- 对于每个 V_{il}^λ，令 $S_{il}^\lambda = M_{il}^\lambda \cap \{x \in \mathbb{R}^n \mid g_j(x) > 0, j \notin \lambda\}$ (如果 $\lambda = \{1, \ldots, s\}$ 则取 $S_{il}^\lambda = M_{il}^\lambda$)。

定理 4.6.1 *在上述记号下，有*

$$f^* = \inf_{x \in S} f(x) \in \bigcup_{\lambda,i,l} \left(K\left(f, M_{il}^\lambda\right) \cup f(V_{i0}^\lambda)\right). \tag{4-22}$$

证明 因为 $S = \bigcup_{\lambda,i,l} S_{il}^{\lambda}$，所以存在固定的某个 $i, l \geq 0$ 和 $\lambda \in \Lambda$，使得 $f^* = \inf\left\{f(x) \mid x \in S_{il}^{\lambda}\right\}$。和定理 4.4.5的证明类似，可证得

$$f^* \in K\left(f, S_{il}^{\lambda}\right) \cup \mathrm{cl}\left(f(\partial S_{il}^{\lambda})\right). \tag{4-23}$$

又因为 $S_{il}^{\lambda} = M_{il}^{\lambda} \cap \{x \in \mathbb{R}^n \mid g_j(x) > 0, j \notin \lambda\}$ 且 $\{x \in \mathbb{R}^n \mid g_j(x) > 0, j \notin \lambda\}$ 是 $\mathbb{R}^n$ 的一个开子集，所以对于 $l > 0$，直接验证可得

$$K\left(f, S_{il}^{\lambda}\right) \subset K\left(f, M_{il}^{\lambda}\right). \tag{4-24}$$

如果 $l = 0$，那么 $S_{i0}^{\lambda} = V_{i0}^{\lambda}$。因此，如果 f^* 包含在 $K\left(f, S_{il}^{\lambda}\right)$ 或 $f(V_{i0}^{\lambda})$ 中，则证明完成。

现在假设 $f^* \in \mathrm{cl}\left(f(\partial S_{il}^{\lambda})\right)$，那么存在 $\lambda_1 \supsetneq \lambda$ 和 $i_1, l_1 \geq 0$，使得 $f^* \in \mathrm{cl}\left(f(\partial M_{il}^{\lambda})\right)$ 或 $f^* \in \mathrm{cl}\left(f(S_{i_1 l_1}^{\lambda_1})\right)$。如果 $f^* \in \mathrm{cl}\left(f(\partial M_{il}^{\lambda})\right)$，则存在 $i_2 > i$ 和 $l_2 < l$ 使得 $f^* \in K\left(f, M_{i_2 l_2}^{\lambda}\right)$ (因为把 V_{il}^{λ} 看作 $\mathbb{R}^n$ 的子拓扑空间时，$\partial M_{il}^{\lambda} \subset V_{il}^{\lambda} \setminus M_{il}^{\lambda}$)。否则，将 S_{il}^{λ} 替换成 $S_{i_1 l_1}^{\lambda_1}$，重复上述过程直到指标集 λ 等于 $\{1, \ldots, s\}$，定理得证。□

例 4.6.2 给定多项式 $g_1 = (x-1)^2(x^2+y^2) - 4x^2$ 和 $g_2 = (x-1)y^2 - 1$。考虑半代数集 $S = \{(x,y) \in \mathbb{R}^2 \mid g_1(x,y) \leq 0,\ g_2(x,y) \leq 0\}$ (见图 4.4)。令 f 是从 S 到 x 轴的投射，即 $f(x,y) = x$。结合定理 4.6.1 和算法 Optimize，计算 $f^* = \inf_{x \in S} f(x)$。

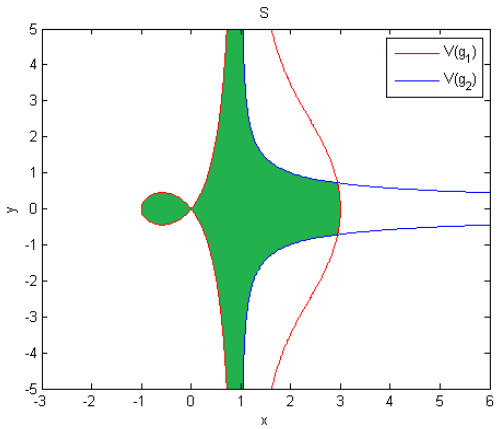


图 4.4　例 4.6.2半代数集 S

令 $\lambda_1=\emptyset,\lambda_2=\{1\},\lambda_3=\{2\},\lambda_4=\{1,2\}$，图 4.5 是对应的半代数集 $S_{il}^{\lambda_i}$。下面给出计算的细节。

- $\lambda_1=\emptyset$, $V_0^{\lambda_1}=\mathbb{R}^2$, $M_{02}^{\lambda_1}=\mathbb{R}^2$, $S_{02}^{\lambda_1}=\{(x,y)\in\mathbb{R}^2 \mid g_1(x,y)<0,\ g_2(x,y)<0\}$。经计算，得到

$$K\left(f,M_{02}^{\lambda_1}\right)\cup K_1\left(f,M_{02}^{\lambda_1}\right)=\emptyset.$$

- $\lambda_2=\{1\}$, $V_0^{\lambda_2}=\{(x,y)\in\mathbb{R}^2 \mid g_1(x,y)=0\}$, $V_{01}^{\lambda_2}=V_0^{\lambda_2}$, $M_{01}^{\lambda_2}=V_{01}^{\lambda_2}\setminus\{(0,0)\}$, $S_{01}^{\lambda_2}=\{(x,y)\mid g_1=0,\ g_2<0\}\setminus\{(0,0)\}$. 计算可得：

$$\begin{aligned}&K\left(f,M_{01}^{\lambda_2}\right)\cup K_1\left(f,M_{01}^{\lambda_2}\right)=\{-1,1,3\},\\&V_1^{\lambda_2}=V_{01}^{\lambda_2}\setminus M_{01}^{\lambda_2}=\{(0,0)\},\ f\left(V_1^{\lambda_2}\right)=\{0\}.\end{aligned}$$

- $\lambda_3=\{2\}$, $V_0^{\lambda_3}=\{(x,y)\in\mathbb{R}^2 \mid g_2(x,y)=0\}$, $V_{01}^{\lambda_3}=V_0^{\lambda_3}$, $M_{01}^{\lambda_3}=V_{01}^{\lambda_3}$, $S_{01}^{\lambda_3}=\{(x,y)\mid g_1<0,\ g_2=0\}$. 计算可得：

$$K\left(f,M_{01}^{\lambda_3}\right)\cup K_1\left(f,M_{01}^{\lambda_3}\right)=\{1\}.$$

- $\lambda_4=\{1,2\}$, $V_0^{\lambda_4}=\{(x,y)\in\mathbb{R}^2 \mid g_1(x,y)=0,g_2(x,y)=0\}$, $M_{00}^{\lambda_4}=V_0^{\lambda_4}$, $S_{00}^{\lambda_4}=V_0^{\lambda_4}$。因为 $V_0^{\lambda_4}$ 是一个有限集，所以我们只需计算它的像 $f(V_0^{\lambda_4})$。这一步输出的单变元多项式是：

$$\psi=a^4-2a^3-3a^2+a-1.$$

令 $\psi=0$，得到两个实根，其中一个小于 -1。然而，最后应用算法 FindInfimum，得到 $f^*=-1$。这是因为所有的计算都是在有理系数多项式环中进行，所以尽管理想 $\langle g_1,g_2\rangle$ 是 $\mathbb{Q}[x,y]$ 中的实理想，但方程组 $g_1=0,g_2=0$ 仍然有复根，所以 $\mathbf{V}_{\mathbb{R}}(\psi)\supsetneq f(V_0^{\lambda_4})$，故出现上述情况：方程 $\psi=0$ 的最小实根不包含在 $f(V_0^{\lambda_4})$ 中。

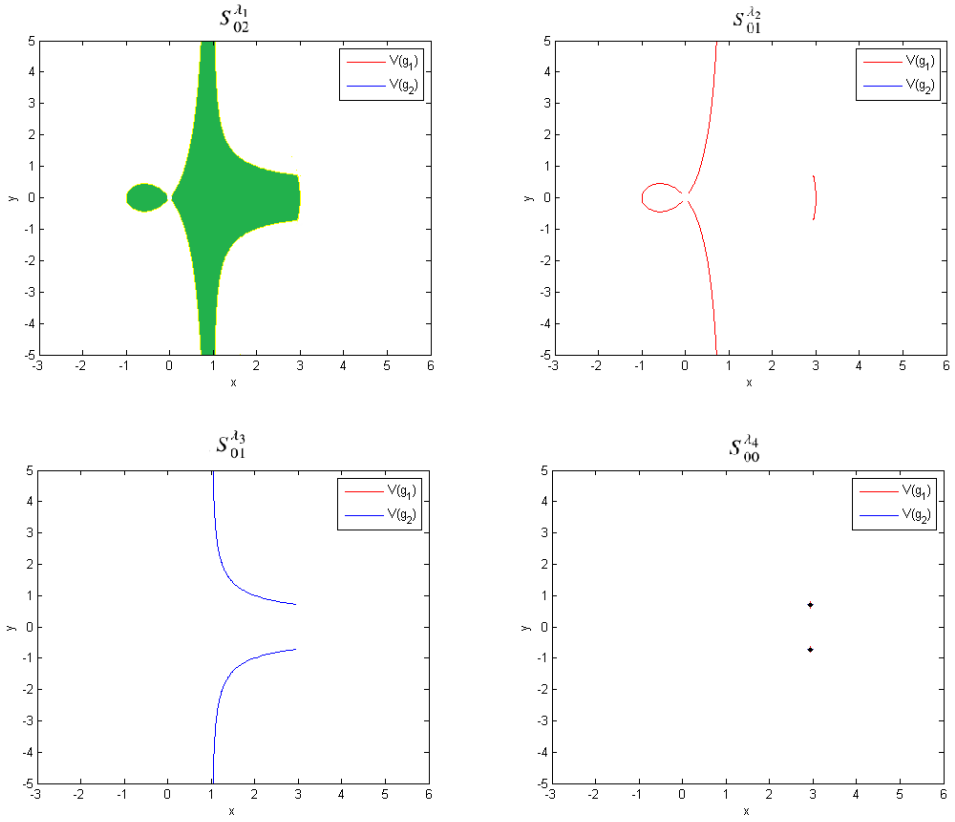


图 4.5　例 4.6.2对应于 λ_i 的半代数集

第 5 章　总结与展望

本文的第一部分旨在分析计算实根理想的复杂度。利用实代数几何中的判定准则：一个素理想是实的当且仅当它有一个非奇异的实零点，将根理想生成元次数上界的成果：一个光滑复代数簇的零化理想有一组次数不高于其几何次数的生成元，推广到实根理想。在此基础上，结合计算实代数簇样本点的算法和利用周形式计算复代数簇等维分解的算法，给出光滑情形下计算实根理想的复杂度，此时的复杂度关于变元个数是单指数的。对于一般的情形，考虑到如果直接应用雅可比准则和 Gröbner 基计算，会导致计算复杂度仍然是双指数的（关于变元个数），于是采用有理参数化来表示实根理想。在已有的应用几何预解式计算复代数簇等维分解算法的基础上，结合插值的技巧，给出一般情形下计算实根理想有理参数化表示的复杂度，这个复杂度关于输入多项式系统的维数是双指数的，如果输入多项式系统的维数是固定的，那么这个复杂度关于变元个数是单指数的。对于已有的计算实根理想的符号算法，其复杂度关于变元个数是双指数的，所以无论是光滑情形还是一般情形，与已有的符号算法相比，我们的结果在复杂度上都有改进。然而，因为在目前的计算机代数系统中，有较为高效的算法用于计算 Gröbner 基，所以最后在实现算法的过程中，我们是通过 Gröbner 基而非周形式或有理参数化表示来实现复代数簇之间的交、并、差等操作。这就意味着我们实现的算法并未达到本文中给出的理论复杂度。尽管如此，我们实现的算仍然法能计算已有算法无法完成的一些例子。下一步可以考虑如何通过周形式或有理参数化表示来实现本文中给出的算法。

对于多项式全局最优化问题，我们将其最优值与多项式函数的广义关键值联系起来。对于可行域是等维实代数簇的情形，我们证明：或者这个问题的最优值是其目标函数的广义关键值，或者这个问题的可行域可以缩小为一个更低维的实代数簇。为了计算实代数簇上多项式函数的全局下确界，在广义关键值的基础上，我们引入一个新的集合。我们证明这个新的集合的勒贝格测度为零。更进一步，我们证明它和广义关键值集合的并集是一个半代数闭集，而且这个半代数闭集的勒贝格测度也为零。基于上述结论，我们给出一个算法计算

多项式函数在任意实代数簇上的全局下确界。如果多项式优化问题的可行域是一个基本半代数闭集，通过划分这个半代数集，我们将这个问题转化为若干个子问题，使得每个子问题的可行域都是实代数簇，这样通过重复调用前面给出的算法，就能处理可行域是基本半代数闭集的情形。

这两个工作的联系之处在于，当多项式优化的可行域是实代数簇时，我们就需要实根理想来表示这个实代数簇。正如我们在第四章中提到的，如果应用光滑情形下计算实根理想的复杂度，那么我们能得到相应的多项式优化问题的计算复杂度关于变元个数是单指数的。对于一般的情形，如何将实根理想的有理参数化表示应用于多项式优化问题，可作为下一步的工作。

参考文献

[1] BECKER E, NEUHAUS R. Computation of real radicals of polynomial ideals[C] // EYSSETTE F, GALLIGO A. Computational Algebraic Geometry. Vol. 109. Boston, MA: Birkhäuser, 1993: 1-20.

[2] NEUHAUS R. Computation of real radicals of polynomial ideals – II[J]. Journal of Pure and Applied Algebra, 1998, 124(1): 261-280.

[3] BECKER E, MORA T, MARINARI M G, TRAVERSO C. The Shape of the Shape Lemma[C]// Proceedings of the International Symposium on Symbolic and Algebraic Computation. ISSAC '94. Oxford, United Kingdom: ACM, 1994: 129-133.

[4] SPANG S J. On the computation of the real radical[D]. Technische Universität Kaiserslautern, 2007.

[5] SPANG S J. A zero-dimensional approach to compute real radicals.[J]. The Computer Science Journal of Moldova, 2008, 16(1): 64-92.

[6] ZENG G, ZENG X. An effective decision method for semidefinite polynomials[J]. Journal of Symbolic Computation, 2004, 37(1): 83-99.

[7] XIAO S, ZENG X, ZENG G. An improved algorithm for deciding semi-definite polynomials[J]. Journal of Algebra, 2014, 417: 72-94.

[8] CHEN C, DAVENPORT J H, MAY J P, MAZA M M, XIA B, XIAO R. Triangular decomposition of semi-algebraic systems[C]// Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation. ISSAC'10. Munich, Germany: ACM, 2010: 187-194.

[9] CHEN C, DAVENPORT J H, MORENO MAZA M, XIA B, XIAO R. Computing with semi-algebraic sets represented by triangular decomposition[C]// Proceedings of the 36th International Symposium on Symbolic and Algebraic Computation. ISSAC'11. San Jose, California, USA: ACM, 2011: 75-82.

[10] CHEN C, DAVENPORT J H, MAY J P, MAZA M M, XIA B, XIAO R. Triangular decomposition of semi-algebraic systems[J]. Journal of Symbolic Computation, 2013, 49: 3-26.

[11] LASSERRE J B, LAURENT M, ROSTALSKI P. Semidefinite characterization and computation of zero-dimensional real radical ideals[J]. Foundations of Computational Mathematics, 2008, 8(5): 607-647.

[12] LASSERRE J B, LAURENT M, MOURRAIN B, ROSTALSKI P, TRÉBUCHET P. Moment matrices, border bases and real radical computation[J]. Journal of Symbolic Computation, 2013, 51: 63-85.

[13] MA Y, WANG C, ZHI L. A certificate for semidefinite relaxations in computing positive-dimensional real radical ideals[J]. Journal of Symbolic Computation, 2016, 72: 1-20.

[14] BRAKE D A, HAUENSTEIN J D, LIDDELL A C Jr. Validating the Completeness of the Real Solution Set of a System of Polynomial Equations[C]/ / Proceedings of the 2016 International Symposium on Symbolic and Algebraic Computation. ISSAC'16. Waterloo, ON, Canada: ACM, 2016: 143-150.

[15] BLANCO C, JERONIMO G, SOLERNÓ P. Computing generators of the ideal of a smooth affine algebraic variety[J]. Journal of Symbolic Computation, 2004, 38(1): 843-872.

[16] WU W T. Basic principles of mechanical theorem proving in elementary geometries[J]. Journal of Systems Science and Mathematical Sciences, 1984, 4: 207-235.

[17] WANG D. Decomposing polynomial systems into simple systems[J]. Journal of Symbolic Computation, 1998, 25(3): 295-314.

[18] KALKBRENER M. Three contributions to elimination theory[D]. Johannes Kepler University, Linz, 1991.

[19] LAZARD D. A new method for solving algebraic systems of positive dimension[J]. Discrete Applied Mathematics, 1991, 33(1-3): 147-160.

[20] MORENO MAZA M. Calculs de pgcd au-dessus des tours d'extensions simples et résolution des systèmes d'équations algébriques[D]. Université Paris 6, 1997.

[21] GIUSTI M, LECERF G, SALVY B. A Gröbner free alternative for polynomial system solving[J]. Journal of complexity, 2001, 17(1): 154-211.

[22] LECERF G. Computing the equidimensional decomposition of an algebraic closed set by means of lifting fibers[J]. Journal of Complexity, 2003, 19(4): 564-596.

[23] SCHOST É. Computing parametric geometric resolutions[J]. Applicable Algebra in Engineering, Communication and Computing, 2003, 13(5): 349-393.

[24] SAFEY EL DIN M, SCHOST É. A Nearly Optimal Algorithm for Deciding Connectivity Queries in Smooth and Bounded Real Algebraic Sets[J]. Journal of the ACM, 2017, 63(6): 48:1-48:37.

[25] LECERF G. Computing an equidimensional decomposition of an algebraic variety by means of geometric resolutions[C]/ / Proceedings of the 2000 International Symposium on Symbolic and Algebraic Computation. ISSAC'00. St. Andrews, Scotland: ACM, 2000: 209-216.

[26] KAMYAR R, PEET M. Polynomial optimization with applications to stability analysis and control-Alternatives to sum of squares[J]. Discrete and Continuous Dynamical Systems-Series B, 2015, 20(8): 2383-2417.

[27] AHMADI A A, MAJUMDAR A. Some applications of polynomial optimization in operations research and real-time decision making[J]. Optimization Letters, 2016, 10(4): 709-729.

[28] QI L, TEO K L. Multivariate polynomial minimization and its application in signal processing[J]. Journal of Global Optimization, 2003, 26(4): 419-433.

[29] KAHL F, HENRION D. Globally optimal estimates for geometric reconstruction problems[J]. International Journal of Computer Vision, 2007, 74(1): 3-15.

[30] PUTINAR M. Positive polynomials on compact semi-algebraic sets[J]. Indiana University Mathematics Journal, 1993, 42(3): 969-984.

[31] LASSERRE J B. Global optimization with polynomials and the problem of moments[J]. SIAM Journal on Optimization, 2001, 11(3): 796-817.

[32] NIE J, DEMMEL J, STURMFELS B. Minimizing polynomials via sum of squares over the gradient ideal[J]. Mathematical programming, 2006, 106(3): 587-606.

[33] DEMMEL J, NIE J, POWERS V. Representations of positive polynomials on noncompact semialgebraic sets via KKT ideals[J]. Journal of pure and applied algebra, 2007, 209(1): 189-200.

[34] NIE J. An exact Jacobian SDP relaxation for polynomial optimization[J]. Mathematical Programming, 2013, 137(1-2): 225-255.

[35] BUCERO M A, MOURRAIN B. Exact relaxation for polynomial optimization on semi-algebraic sets[Z]. working paper or preprint. 2014.

[36] SCHWEIGHOFER M. Global optimization of polynomials using gradient tentacles and sums of squares[J]. SIAM Journal on Optimization, 2006, 17(3): 920-942.

[37] HÀ H V, PHẠM T S. Solving polynomial optimization problems via the truncated tangency variety and sums of squares[J]. J. Pure Appl. Algebra, 2009, 213(11): 2167-2176.

[38] HÀ H V, PHẠM T S. Representations of positive polynomials and optimization on noncompact semialgebraic sets[J]. SIAM Journal on Optimization, 2010, 20(6): 3082-3103.

[39] GUO F, SAFEY EL DIN M, ZHI L. Global optimization of polynomials using generalized critical values and sums of squares[C]/ / Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation. ACM. [S.l.]: [s.n.], 2010: 107-114.

[40] GREUET A, GUO F, SAFEY EL DIN M, ZHI L. Global optimization of polynomials restricted to a smooth variety using sums of squares[J]. Journal of Symbolic Computation, 2012, 47(5): 503-518.

[41] COLLINS G E. Quantifier elimination for real closed fields by cylindrical algebraic decompostion[C]/ / Automata Theory and Formal Languages 2nd GI Conference Kaiserslautern, May 20–23, 1975. Springer. [S.l.]: [s.n.], 1975: 134-183.

[42] COLLINS G E, HONG H. Partial Cylindrical Algebraic Decomposition for quantifier elimination[J]. Journal of Symbolic Computation, 1991, 12(3): 299-328.

[43] HONG H. Simple Solution Formula Construction in Cylindrical Algebraic Decomposition Based Quantifier Elimination[C]/ / Papers from the International Symposium on Symbolic and Algebraic Computation. ISSAC '92. Berkeley, California, USA: ACM, 1992: 177-188.

[44] MCCALLUM S. An Improved Projection Operation for Cylindrical Algebraic Decomposition[C]/ / CAVINESS B F, JOHNSON J R. Quantifier Elimination and Cylindrical Algebraic Decomposition. Vienna: Springer Vienna, 1998: 242-268.

[45] BROWN C W. SOLUTION FORMULA CONSTRUCTION FOR TRUTH INVARIANT CAD'S[D]. University of Delaware, 1999.

[46] HONG H, SAFEY EL DIN M. Variant Real Quantifier Elimination: Algorithm and Application[C]/ / Proceedings of the 2009 International Symposium on Symbolic and Algebraic Computation. ISSAC'09. Seoul, Republic of Korea: ACM, 2009: 183-190.

[47] HONG H, SAFEY EL DIN M. Variant quantifier elimination[J]. Journal of Symbolic Computation, 2012, 47(7): 883-901.

[48] BASU S, POLLACK R, ROY M F. Algorithms in Real Algebraic Geometry[M]. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006.

[49] KURDYKA K, ORRO P, SIMON S, et al. Semialgebraic Sard theorem for generalized critical values[J]. Journal of differential geometry, 2000, 56(1): 67-92.

[50] SAFEY EL DIN M. Computing the Global Optimum of a Multivariate Polynomial over the Reals[C]/ / Proceedings of the Twenty-first International Symposium on Symbolic and Algebraic Computation. ISSAC'08. Linz/Hagenberg, Austria: ACM, 2008: 71-78.

[51] GREUET A, SAFEY EL DIN M. Probabilistic algorithm for polynomial optimization over a real algebraic set[J]. SIAM Journal on Optimization, 2014, 24(3): 1313-1343.

[52] RABIER P J. Ehresmann fibrations and Palais-Smale conditions for morphisms of Finsler manifolds[J]. Annals of Mathematics, 1997: 647-691.

[53] JELONEK Z, KURDYKA K. Quantitative generalized Bertini-Sard theorem for smooth affine varieties[J]. Discrete and Computational Geometry, 2005, 34(4): 659-678.

[54] COX D, LITTLE J, O'SHEA D. Ideals, varieties, and algorithms[M]. 4th. Vol. 3. [S.l.]: Springer, 2007.

[55] GREUEL G M, PFISTER G. A Singular Introduction to Commutative Algebra[M]. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008.

[56] 吴文俊. 数学机械化[M]. 北京: 科学出版社, 2003.

[57] JERONIMO G, SABIA J. Effective equidimensional decomposition of affine varieties[J]. Journal of Pure and Applied Algebra, 2002, 169(2): 229-248.

[58] BOCHNAK J, COSTE M, ROY M F. Real algebraic geometry[M]. Vol. 36. [S.l.]: Springer, Berlin, Heidelberg, 1998.

[59] EISENBUD D. Commutative Algebra: with a View Toward Algebraic Geometry[M]. Vol. 150. New York, NY: Springer New York, 1995.

[60] MARSHALL M. Positive polynomials and sums of squares[M]. 146. [S.l.]: American Mathematical Soc., 2008.

[61] GELFAND I M, KAPRANOV M, ZELEVINSKY A. Discriminants, resultants, and multidimensional determinants[M]. [S.l.]: Springer Science & Business Media, 2008.

[62] JERONIMO G, KRICK T, SABIA J, SOMBRA M. The computational complexity of the Chow form[J]. Foundations of Computational Mathematics, 2004, 4(1): 41-117.

[63] SAFEY EL DIN M, SCHOST É. Polar varieties and computation of one point in each connected component of a smooth real algebraic set[C]/ / Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation. ISSAC'03. Philadelphia, PA, USA: ACM, 2003: 224-231.

[64] SAFEY EL DIN M, SCHOST É. Properness defects of projections and computation of at least one point in each connected component of a real algebraic set[J]. Discrete & Computational Geometry, 2004, 32(3): 417-430.

[65] SAFEY EL DIN M. Finding sampling points on real hypersurfaces is easier in singular situations[J]. MEGA (Effective Methods in Algebraic Geometry) Electronic proceedings, 2005.

[66] SAFEY EL DIN M. RAGLib (Real Algebraic Geometry Library), Maple package. 2007.

[67] SAFEY EL DIN M. Testing sign conditions on a multivariate polynomial and applications[J]. Mathematics in Computer Science, 2007, 1(1): 177-207.

[68] KALTOFEN E. Factorization of polynomials given by straight-line programs[J]. Randomness and Computation. Advances in Computing Research 5 1989: 375-412.

[69] KALTOFEN E, TRAGER B M. Computing with polynomials given by black boxes for their evaluations: greatest common divisors, factorization, separation of numerators and denominators[J]. Journal of Symbolic Computation, 1990, 9(3): 301-320.

[70] KRICK T. Straight-line programs in polynomial equation solving[J]. Foundations of computational mathematics: Minneapolis, 2002, 312: 96-136.

[71] DURVYE C, LECERF G. A concise proof of the Kronecker polynomial system solver from scratch[J]. Expositiones Mathematicae, 2008, 26(2): 101-139.

[72] POTEAUX A, SCHOST É. On the complexity of computing with zero-dimensional triangular sets[J]. Journal of Symbolic Computation, 2013, 50(Supplement C): 110-138.

[73] HEINTZ J. Definability and fast quantifier elimination in algebraically closed fields[J]. Theoretical Computer Science, 1983, 24(3): 239-277.

[74] EVERETT H, LAZARD D, LAZARD S, SAFEY EL DIN M. The Voronoi diagram of three lines[J]. Discrete & Computational Geometry, 2009, 42(1): 94-130.

[75] KALTOFEN E, LI B, YANG Z, ZHI L. Exact certification of global optimality of approximate factorizations via rationalizing sums-of-squares with floating point scalars[C]/ / Proceedings of the Twenty-first International Symposium on Symbolic and Algebraic Computation. ISSAC'08. Linz/Hagenberg, Austria: ACM, 2008: 155-164.

[76] LAX P. On the discriminant of real symmetric matrices[J]. Selected Papers Volume II, 2005: 577-586.

[77] FLØYSTAD G, KILEEL J, OTTAVIANI G. The Chow form of the essential variety in computer vision[J]. Journal of Symbolic Computation, 2017.

[78] JELONEK Z. On asymptotic critical values and the Rabier theorem[J]. Banach Center Publications, 2004, 1(65): 125-133.

[79] COHEN R L. The Topology of Fiber Bundles Lecture Notes[J]. Standford University, 1998.

[80] BECKER T, WEISPFENNING V. Gröbner Bases: A Computational Approach to Commutative Algebra[M]. New York, NY: Springer New York, 1993.

[81] AUBRY P, ROUILLIER F, SAFEY EL DIN M. Real Solving for Positive Dimensional Systems[J]. Journal of Symbolic Computation, 2002, 34(6): 543-560.

[82] KRICK T, LOGAR A. An algorithm for the computation of the radical of an ideal in the ring of polynomials[C]/ / International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes. [S.l.]: Springer, Berlin, Heidelberg, 1991: 195-205.

[83] SAFEY EL DIN M, YANG Z H, ZHI L. On the complexity of computing real radicals of polynomial systems[C]/ / Proceedings of the 2018 International Symposium on Symbolic and Algebraic Computation. ISSAC'18. Philadelphia, PA, USA: ACM, 2018: 1-8.

致 谢

衷心地感谢我的恩师支丽红研究员。在支老师的指导下，我开始学习实代数几何，然后研究这个领域中待解决的问题。当我在研究中遇到困难时，支老师总是耐心地给予指导，为我打开新的思路。这让我得以跨过重重障碍，完成本文的工作。此外，在支老师的帮助下，我曾两度出国学习交流，这为我拓宽了学术视野，提升了科研能力，也让我的博士生涯更加丰富多彩。为了培养我成为一个合格的博士，支老师付出了很大的心力。对于所有的这一切，我都不胜感谢。

承蒙 Mohab Safey El Din 教授的指导，本文第三章关于有理参数化表示的成果才有了完善的复杂度分析。在实现这一章的算法时，Yue Ren 给予了极大的帮助。关于分解多元多项式算法的复杂度，Erich L. Kaltofen 教授提供了参考与指导。关于多项式插值算法的复杂度以及多项式的 SLP 表示，我在学习过程中向黄巧龙同学请教了很多相关问题。在学习几何预解式的过程中，我得到了袁春明老师的指导。本文第四章关于多项式全局最优化的工作得益于王础师兄的长期指导和帮助。在完成这个工作的过程中，我也向陈煜同学和毛媛媛同学请教过相关的问题。我由衷地感谢以上所有的老师、师兄和同学。

在西班牙塞维利亚大学的三个月期间，Justo Puerto 教授百忙之中仍然每个星期抽出时间指导我的学习和研究，在此特地感谢。也感谢这期间所有帮助过我的老师和同学。

感谢数学机械化重点实验室的各位老师，尤其感谢李子明老师、王定康老师和袁春明老师在授课期间对我的指导。感谢数学机械化重点实验室的师兄师姐和师弟师妹们，尤其感谢王础师兄对我学习实代数几何的指导和帮助，还有郝志伟师兄、郭峰师兄、李楠师兄、陈绍示师兄、李应弘师姐、荆瑞娟师姐对我学习上的指导和帮助。以及姜文嵘师妹、葛京通师弟、闫斯卓师妹对我的帮助和支持。感谢数学机械化重点实验室的黄巧龙、周义满、白剑、宓振鹏、窦孝杰、付仕辉、陈勇等同学对我的学习和生活上的帮助。

感谢我的朋友谭屯子，感谢她对我的包容、关心、支持和信任，感谢她在这五年当中带给我的阳光与欢乐，希望与色彩。感谢我的朋友李秋萍对我的信

任和陪伴。感谢我的朋友肖许曼在这篇论文的撰写过程中对我的鼓励、支持与陪伴。感谢我的朋友孙书成和柳梅，感谢她们这些年的惦念、倾听、鼓励、分享和督促。

感谢我亲爱的奶奶和外婆，感谢我可爱的弟弟和妹妹，感谢他们对我的关爱、信任、支持和鼓励。

最后，我对父母的感激之情无以言表，在我的整个求学生涯中，父母都是我最坚强的后盾，正是父母对我的支持，让我有了面对一切困难的勇气和不断前行的动力。

作者简历及攻读学位期间发表的学术论文与研究成果

作者简历：

2009 年 9 月——2013 年 7 月，中南大学数学与统计学院，应用数学专业，理学学士。
2013 年 9 月——现在，中国科学院数学与系统科学研究院，数学机械化重点实验室，硕博连读。

已发表（或正式接受）的学术论文：

[1] Mohab Safey El Din, Zhi-Hong Yang, Lihong Zhi, On the complexity of computing real radicals of polynomial systems, accepted by ISSAC'18.

学术交流：

2015.9– 2015.12　加拿大多伦多大学 Fields 研究所，Thematic Program on Computer Algebra
2015.3– 2015.5　西班牙塞维利亚大学数学研究所，DOC-COURSE: Applied Mathematics and Optimization

获奖情况：

2017　中国科学院数学与系统科学研究院三好学生
2013　湖南省优秀毕业生，中南大学优秀毕业生，中南大学荣誉生，中南大学优秀学生干部
2012　国家奖学金，中南大学一等奖学金

2011 中南大学钻石奖学金，中南大学一等奖学金，中南大学优秀学生，湖南省高校大学生数学竞赛（数学专业组）二等奖，中南大学数学竞赛（数学类）三等奖

2010 国家励志奖学金，中南大学一等奖学金，中南大学优秀学生