密级 _____

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

博士学位论文

线性矩阵不等式精确求解的符号计算方法

作者姓名 郭庆东

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

2014 年 5 月

Symbolic Algorithm for Computing Exact Solutions of Linear Matrix Inequalities

By

Qingdong Guo

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

Academy of Mathematics and Systems Science

May, 2014

摘　要

线性矩阵不等式有理数解及精确实数解的存在性判定和计算是半正定规划、计算实代数几何、多项式优化、凸几何等交叉学科领域面临的一个重要问题，其中线性矩阵不等式有理数解的判定与计算对于多项式有理系数平方和计算具有重要意义。

给定$(D \times D)$ 对称线性矩阵$\mathsf{A} = \mathsf{A}_0 + X_1\mathsf{A}_1 + \cdots + X_k\mathsf{A}_k \succeq 0$，它的元素为$\mathbb{Q}[X_1, \ldots, X_k]$ 中的有理系数线性多项式，这些多项式系数二进制表示的位长不超过τ。线性矩阵不等式$\mathsf{A} \succeq 0$的可行域记为$\mathfrak{S}(\mathsf{A})$，它包含了使得$\mathsf{A}(\mathbf{x}) = \mathsf{A}_0 + x_1\mathsf{A}_1 + \cdots + x_k\mathsf{A}_k$ 的所有特征值非负的全部实数解$\mathbf{x} \in \mathbb{R}^k$，这是一个闭的凸半代数集。

借助计算实代数几何中的一些判定方法和工具，我们在第三章给出了一个算法RationalLMI来判定$\mathfrak{S}(\mathsf{A})$是否包含有理数解，在有理数解存在时给出有理数解。算法RationalLMI的运行时间控制在$(k\tau)^{O(1)}2^{O(\min(k,D)D^2)}D^{O(D^2)}$位操作，并且在$\mathfrak{S}(\mathsf{A})$非空情形，输出解坐标的位长控制在$\tau^{O(1)}2^{O(\min(k,D)D^2)}$以内。作为一般凸半代数集的特殊形式，它显著改进了Safey El Din与支丽红之前给出的算法复杂度。

给定多项式$f \in \mathbb{Q}[X_1, \ldots, X_n]$ 次数为$2d$，系数位长不超过τ。我们的算法可判定f 是否存在有理系数多项式平方和分解，并在分解存在时给出相应表示形式，算法复杂度为$\tau^{O(1)}2^{O(\mathsf{M}(d,n)^3)}$，其中$\mathsf{M}(d,n) = \min(d^n, n^d)$。输出表示形式中系数位长的界为$\tau^{O(1)}2^{O(\mathsf{M}(d,n)^3)}$。这也是目前多项式有理系数平方和判定和计算的复杂度最好的算法。第四章中，我们给出了在Maple软件中演算的一些例子。Sturmfels曾提出一个问题：如果一个有理系数多项式存在实系数多项式平方和表示形式，其是否存在有理系数多项式平方和表示？2012年，Scheiderer给出了Sturmfels 问题的第一个反例，我们的算法给出了该反例的第一个计算机验证。

第五章中，我们设计了新算法RealLMI，给出了$\mathfrak{S}(\mathsf{A})$ 上精确实数解的计算方法并给出了Scheiderer反例精确实系数平方和分解的计算机实现。

关键词： 线性矩阵不等式，多项式有理系数平方和，精确求解，算法复杂度

Abstract

Certification and computation of rational or exact real solutions of linear matrix inequalities is an important question to the intersection discipline of semidefinite programming, computational real algebraic geometry, polynomial optimization and convex geometry. Computing rational solutions of linear matrix inequalities has the vital significance for computing polynomial sums of squares decompositions over the rationals.

Consider a $(D \times D)$ symmetric matrix A whose entries are linear forms in $\mathbb{Q}[X_1, \ldots, X_k]$ with coefficients of bit size $\leq \tau$. The feasible region of the linear matrix inequality $\mathsf{A} \succeq 0$ is $\mathfrak{S}(\mathsf{A})$, which contains all the real solutions $\mathbf{x} \in \mathbb{R}^k$ such that all the eigenvalues of $\mathsf{A}(\mathbf{x}) = \mathsf{A}_0 + x_1\mathsf{A}_1 + \cdots + x_k\mathsf{A}_k$ are nonnegative.

In Chapter 3, by certification methods and tools from computational real algebraic geometry, we provided a symbolic algorithm RationalLMI, which can be used to decide if $\mathfrak{S}(\mathsf{A})$ has rational solutions and return rational points in $\mathfrak{S}(\mathsf{A})$ in the case of non-emptiness. Our algorithm RationalLMI runs within $(k\tau)^{O(1)}2^{O(\min(k,D)D^2)}D^{O(D^2)}$ bit operations; the bit size of the output solution is dominated by $\tau^{O(1)}2^{O(\min(k,D)D^2)}$. As this is a special case of general convex set, the upper complexity bounds dramatically improve over the previously one by Safey El Din and Zhi.

Let $f \in \mathbb{Q}[X_1, \ldots, X_n]$ of degree $2d$ with coefficients of bit size $\leq \tau$. Our algorithm can decide the existence of a sum of squares decomposition of f over the rationals and compute such a decomposition whenever it exists within $\tau^{O(1)}2^{O(\mathsf{M}(d,n)^3)}$ bit operations where $\mathsf{M}(d,n) = \min(d^n, n^d)$. The bit size of the output is also dominated by $\tau^{O(1)}2^{O(\mathsf{M}(d,n)^3)}$. This leads to the best complexity bounds for deciding the existence of sums of squares with rational coefficients of a given polynomial. In Chapter 4, we implemented our algorithm and ran it on several examples. Sturmfels' conjecture asking whether all polynomials with coefficients in $\mathbb{Q}$ and which are sums of squares of polynomials with coefficients in $\mathbb{R}$ can be written as a sum of squares of polynomials with coefficients in $\mathbb{Q}$. In

2012, Scheiderer gave an example showing that Sturmfels' conjecture is not true, we provide the first computer validation of this counter-example to Sturmfels' conjecture.

In Chapter 5, we designed a new algorithm RealLMI，which can be used to compute exact real solutions of $\mathfrak{S}(\mathsf{A})$, and give the exact sum of squares representation over the reals for Scheiderer's example.

Keywords: Linear matrix inequality, rational sum of squares, exact solution, complexity

目　　录

插　　图

第一章　引言

线性矩阵不等式有理数解及精确实数解的存在性判定和计算是半正定规划、计算实代数几何、多项式优化、凸几何等交叉学科领域面临的一个重要问题，其中线性矩阵不等式有理数解的判定与计算对于多项式有理系数平方和计算具有重要意义。我们先从三个方面介绍相关的研究问题、历史发展和目前研究状况，最后我们给出本文主要贡献和结构。

1.1　多项式非负性判定与平方和表示

判定多项式的全局非负性是数学很多领域涉及到的一个基本问题，具体来说，就是给出某种有效的方法来判断多项式 $f(x_1,\cdots,x_n)\in\mathbb{R}[x_1,\ldots,x_n]$是否满足

$$f(x_1,\cdots,x_n)\geq 0,\ \forall(x_1,\cdots,x_n)\in\mathbb{R}^n。\tag{1.1}$$

系统和控制科学领域中的许多具体问题都可转化为对多项式全局非负性的判定 [26]。通常情况下，判定多项式的半正定性是非常困难的任务。如果存在多项式 $u_i(x_1,\ldots,x_n)\in\mathbb{R}[x_1,\ldots,x_n]$ 使得

$$f(x_1,\ldots,x_n)=\sum_j {u_j}^2(x_1,\ldots,x_n)$$

成立，则称 $f(x_1,\ldots,x_n)$ 具有平方和表示。如果能将一个多项式表示成一组多项式的平方和，则可判定该多项式的全局非负性。例如 [23]，

$$\begin{aligned} f(w,x,y,z) &= w^6+2z^2w^3+x^4+y^4+z^4+2x^2w+2x^2z+3x^2+w^2+2zw \\ &\quad +z^2+2z+2w+1 \\ &= (y^2)^2+(x^2+w+z+1)^2+x^2+(w^3+z^2)^2, \end{aligned}$$

$f(w,x,y,z)\geq 0$恒成立。

关于多项式的平方和表示与非负性判定，可以追溯到Hilbert的第十七问题和相关研究，以下是一些相关研究工作的历史进程。

1888年，Hilbert [27]证明半正定多项式 $f(x)$ 具有平方和分解，如果$f(x)$为下列情形之一：

1. $f(x)$ 为双变元多项式；

2. deg $f(x)=2$；

3. $f(x)$ 为三元四次多项式。

1893年，Hilbert [28]又对三元多项式形式作了进一步的研究，得到如下结论：半正定三元m次齐次多项式可以表示为两个多项式平方和之商，并猜想这一结论对一般的半正定多项式也是对的。

在1900年法国巴黎的国际数学家大会上，Hilbert提出了对以后的数学发展产生重大影响的23个数学问题 [29]，其中第17个问题可叙述如下：对于任意非负多项式 $f \in \mathbb{R}[x_1,\ldots,x_n]$，是否存在有理函数 $g_1,\ldots,g_s \in \mathbb{R}(x_1,\ldots,x_n)$ 使得 $f=\sum_{i=1}^{s} g_i^2$?

1906年，Landau [39]给出了如下结论：设 $f(x)\in\mathbb{Q}[x]$为半正定多项式，则$f(x)$可以表示为八项有理系数多项式平方和形式。

1927 年，Artin [2] 运用Tarski转移原理及序域理论对Hilbert的问题给出了肯定的证明并以此为实代数理论的发展奠定了基础。

1928年，Polya [53]证明了如果一个n元偶次多项式$f(x_1,\ldots,x_n)$ 是正定的，那么对充分大的自然数r，$(x_1^2+x_2^2+\ldots+x_n^2)^r f(x_1,\ldots,x_n)$是$\mathbb{R}[x_1,\ldots,x_n]$ 上单项式的平方和。

1940年，Habicht [22]将Polya的结果推广为任意一个正定多项式可写为两个单项式平方和的商。

1964年，Krivine [38]首次提出了基于Hilbert 17问题的Positivstellensatz：任意$\mathbb{R}[x_1,\ldots,x_n]$ 中的多项式f，f在$\mathbb{R}^n$ 中任意点的计值是正的，当且仅当存在多项式平方和s,t满足$s\cdot f=1+t$。

1967年，Pfister [52]证明了$f \in \mathbb{R}[x_1,\ldots,x_n]$是正定的，那么一定能写成$\mathbb{R}(x_1,\ldots,x_n)$中$2^n$个有理函数的平方和。

1971年，Pourchet [55]证明了$f(x)\in\mathbb{Q}[x]$是半正定的，则可写成$\mathbb{Q}[x]$中5个多项式的平方和。

但并不是所有的多项式都存在多项式平方和分解。1967年，Motzkin [44]给出了第一个齐次多项式，它可以表示为有理函数的平方和，但不能表示为多项式的平方和。这个多项式是

$$f(x,y,z)=z^6+x^4y^2+x^2y^4-3x^2y^2z^2。$$

随后Robinson [65]找到了一个完全对称的例子：

$$x^6+y^6+z^6-(x^4\,y^2+x^4\,z^2+y^4\,x^2+y^4\,z^2+z^4\,x^2+z^4\,y^2)+3x^2\,y^2\,z^2,$$

它具有同样的性质。

Cassier [12]在1986年将Krivine定理推广为：对多项式 $f\in\mathbb{R}[x_1,\ldots,x_n]$ 及 $R\in\mathbb{R}$，在以原点为中心以 R 为半径的球上，$f\geq 0$，当且仅当对任意 $\epsilon>0$，存在多项式平方和 $s,t\in\mathbb{R}[x_1,\ldots,x_n]^2$ 使得$f+\epsilon=s+t(R^2-\Sigma_{i=1}^n x_i^2)$。

Reznick [63] 于1995 年证明了：假设 $f(x)$ 是$\mathbb{R}[x_1,\ldots,x_n]$ 中次数为 m 的齐次正定多项式，$\epsilon(f)$ 是 f 在单位球上的下确界和上确界的比。如果 $r\geq \frac{nm(m-1)}{4\log 2\epsilon(f)}-\frac{n+m}{2}$，那么 $(\Sigma_{i=1}^n x_i^2)^r f$ 是 $\mathbb{Q}[x_1,\ldots,x_n]$ 上线性形的 $(m+2r)$ 次幂的非负$\mathbb{R}$-线性组合。

1995年，Choi、Lam和Reznick [14]给出了多项式的Gram矩阵表示法。随后Powers和Wormann [57]在1998年得到了一个将非负多项式表示为多项式平方和的算法，于是判定一个实系数多项式是否存在实系数多项式平方和表示等价于判定其Gram 矩阵半正定是否有实数解。

Parrilo [48]和Lasserre [40] 于 2000 年分别提出了基于Cassier定理的用半定规划来计算多项式的全局最优解。Papachristodoulou, Anderson, Valmorbida, Prajna, Seiler 和Parrilo在Matlab平台上开发了程序包SOSTOOLS [47]，实现了上面提到的Powers和Wormann的算法。

Blekherman在文献 [9]中指出,在所有次数大于或等于4 的多元多项式集合中，能够分解为平方和的多项式与非负多项式的比例随着变元数的增加而趋向于0。关于多项式非负性判定和平方和的更多相关介绍可参见文献 [43, 56, 58, 59, 64, 75]。

1.2　多项式平方和表示的精确验证

Sturmfels曾提出一个问题：如果一个有理系数多项式$f\in\mathbb{Q}[x_1,\ldots,x_n]$ 存在实系数多项式平方和表示形式，其是否存在有理系数多项式平方和表示？

如果对于有理系数多项式$f\in\mathbb{Q}[x_1,\ldots,x_n]$，存在一个可逆的Gram矩阵，那么多项式$f$存在一个有理系数的Gram矩阵 [30, 定理1.2]。更进一步，如果有理系数多项式f可以表示为$\mathbb{K}[x_1,\ldots,x_n]$上$m$个多项式的平方和, 其中$\mathbb{K}$ 为一个Galois闭包为L的完全实域, 那么f可以表示为$\mathbb{Q}[x_1,\ldots,x_n]$上$4m\cdot 2^{[L:\mathbb{Q}]+1}\binom{[L:\mathbb{Q}]+1}{2}$

个多项式的平方和 [30, 定理1.4]。更有趣的是平方和的个数还可以减少到m（参见 [34]）。

Peyrl和Parrilo在文章 [50, 51]中介绍了通过使用 Macaulay 2软件包从一个有理系数非负多项式的数值平方和分解开始计算其精确的平方和分解的方法。Kaltofen、李斌、杨争峰及支丽红 [32, 33] 利用有理化正交投影，Gauss-Newton 迭代等工具，将多项式近似平方和分解转化为准确有理系数平方和分解。但他们的算法失效时，无法验证多项式是否存在有理系数平方和表示。

Khachiyan和Porkolab [35, 36]给出了一般凸半代数集上整数解的计算方法。2010年，Safey El Din与支丽红 [73]给出了一般凸半代数集上有理点的存在性判定和计算方法，线性矩阵不等式的可行域是凸的闭半代数集，应用该算法判定

$$\mathsf{A} = \mathsf{A}_0 + X_1\mathsf{A}_1 + \cdots + X_k\mathsf{A}_k \succeq 0$$

的可行域是否包含有理数解的算法复杂度为$\tau^{O(1)}D^{O(k^3)}$，其中k为变元个数，D为矩阵$\mathsf{A}_0, \ldots, \mathsf{A}_k$的阶数，$\tau$为矩阵$\mathsf{A}_0, \ldots, \mathsf{A}_k$ 中有理系数二进制表示位长的上界。

判定一个有理系数多项式是否存在有理系数多项式平方和分解等价于判定多项式的Gram矩阵半正定的可行域是否包含有理数解，给定一个$2d$次有理系数多项式$f \in \mathbb{Q}[Y_1, \ldots, Y_n]$，其系数位长不超过$\tau$，它的Gram矩阵的阶数为$D = \binom{n+d}{n}$，变元个数为$k \leq \frac{1}{2}D(D+1) - \binom{n+2d}{n}$。通过计算可得$\frac{1}{2}D(D+1) - \binom{n+2d}{n} \simeq O(\min(n^{2d}, d^{2n}))$，$\binom{n+d}{n} \simeq O(\min(n^d, d^n))$。用$\mathsf{M}(d,n)$来表示$\min(n^d, d^n)$，该算法判定一个有理系数多项式是否存在有理系数多项式平方和分解的算法复杂度为$\tau^{O(1)}\mathsf{M}(d,n)^{\mathsf{M}(d,n)^6}$。

2012年，郭峰、Kaltofen和支丽红给出了实系数多项式平方和的存在性判定 [21]，但是当实系数平方和存在而有理系数平方和不存在时，他们无法给出验证。

2012年，Scheiderer给出了Sturmfels问题的第一个反例 [74]

$$f = x^4 + x\,y^3 + y^4 - 3\,x^2\,y\,z - 4\,x\,y^2\,z + 2\,x^2\,z^2 + x\,z^3 + y\,z^3 + z^4。$$

它可以表示为实系数多项式的平方和，但不能表示为有理系数多项式的平方和。

1.3　半正定规划准确对偶与可行性判定

标准的半正定规划问题具有下面形式:

$$\begin{aligned} p^* := \min_{\mathbf{x}\in\mathbb{R}^k} \quad & \mathbf{c}^\star\mathbf{x} \\ s.t. \quad & \mathsf{A}(\mathbf{x}) \succeq 0, \end{aligned} \tag{1.2}$$

其中向量 $\mathbf{c}\in\mathbb{R}^k$，矩阵 $\mathsf{A}(x) := \mathsf{A}_0 + \sum_{i=1}^k x_i\mathsf{A}_i$ 为实对称矩阵 $\mathsf{A}_0, \mathsf{A}_1, \ldots, \mathsf{A}_k$ 的线性组合。限制条件 $\mathsf{A}(\mathbf{x}) \succeq 0$ 叫做线性矩阵不等式 (Linear Matrix Inequality), 表示矩阵 $\mathsf{A}(\mathbf{x})$ 是半正定矩阵 (即 $\mathbf{z}^\star\mathsf{A}(\mathbf{x})\mathbf{z} \geq 0$ 对于任意实向量 $\mathbf{z}$ 成立)。半正定规划的目标函数和限制条件都满足凸性质，所以它的可行解集为凸集，半正定规划问题是凸最优化问题，可以通过Matlab 中基于内点法 (Interior-point Method) 的软件包高效求解，例如 SeDuMi [76]，SDPT3 [78]，DSDP [8]，SDPNAL [82]。然而由于 Matlab 只能进行有限精度的计算，所得结果往往带有较大的数值误差。半正定规划包含线性规划并且很多问题也可以转化为半正定规划求解 [1, 11, 13, 18, 19]。关于半正定规划的介绍, 可以参见文献 [10, 46, 60, 77, 79, 81]。

半正定规划 (1.2) 的对偶问题为

$$\begin{aligned} d^* := \max_{S} \quad & -\mathbf{Tr}(\mathsf{A}_0 S) \\ s.t. \quad & \mathbf{Tr}(\mathsf{A}_i S) = c_i,\ i = 1, \ldots, k, \\ & S \succeq 0, \end{aligned} \tag{1.3}$$

其中变量 $S = S^\star$ 为实对称矩阵，c_i 为向量 $\mathbf{c}$ 中的相应元素。记号 $\mathbf{Tr}(\cdot)$ 表示矩阵的迹，即矩阵主对角线上所有元素的和。对于任意半正定矩阵 A, B，可以设 $B = VV^\star$，则 $\mathbf{Tr}(AB) = \mathbf{Tr}(V^\star AV) \geq 0$，等号成立当且仅当 $AB = 0$。半正定规划 (1.2) 和 (1.3) 对任意可行解 $\mathbf{x}, S$ 成立

$$\mathbf{c}^\star\mathbf{x} + \mathbf{Tr}(\mathsf{A}_0 S) = \sum_{i=1}^k \mathbf{Tr}(x_i\mathsf{A}_i S) + \mathbf{Tr}(\mathsf{A}_0 S) = \mathbf{Tr}(\mathsf{A}(\mathbf{x})S) \geq 0,$$

由此可知弱对偶 $p^* \geq d^*$ 成立，并且 $p^* = d^*$ 时它们的任意最优解 $\mathbf{x}^*, S^*$ 满足 $\mathsf{A}(\mathbf{x}^*)S^* = 0$。如下强对偶定理的证明可参见 [46]。

定理 1.1. *如果以下条件之一成立, 那么 $p^* = d^*$。*

1. 原始问题 (1.2) 存在严格可行解，即存在 $\mathbf{x}$ 满足 $\mathsf{A}(\mathbf{x}) \succ 0$。

2. 对偶问题 (1.3) 存在严格可行解，即存在 $S = S^\star \succ 0$ 满足 $\mathbf{Tr}(\mathsf{A}_i S) = c_i$, $i = 1, ..., k$。

如果两个条件都成立，那么两个对偶问题的最优解集都非空。

Ramana给出了半正定规划的拓展的Lagrange-Slater对偶 [45]，

$$\begin{aligned} d^* := \max_{U} \quad & -\mathbf{Tr}(\mathsf{A}_0(U + W_k)) \\ s.t. \quad & \mathbf{Tr}(\mathsf{A}_i(U + W_k)) = c_i,\ i = 1, \ldots, k, \\ & \mathbf{Tr}(\mathsf{A}_i(U_j + W_{j-1})) = 0,\ i = 0, \ldots, k,\ j = 1, \ldots, k, \\ & U_j \succeq W_j W_j^\star,\ j = 1, \ldots, k, \\ & U \succeq 0, \\ & W_0 = \mathbf{0}, \end{aligned} \tag{1.4}$$

更进一步，Ramana给出了如下的弱形式的拓展的Lagrange-Slater对偶 [45]，

$$\begin{aligned} d^* := \max_{U} \quad & -\mathbf{Tr}(\mathsf{A}_0(U + W_{k-1})) \\ s.t. \quad & \mathbf{Tr}(\mathsf{A}_i(U + W_{k-1})) = c_i,\ i = 1, \ldots, k, \\ & \mathbf{Tr}(\mathsf{A}_i(U_j + W_{j-1})) = 0,\ i = 0, \ldots, k,\ j = 1, \ldots, k-1, \\ & U_j \succeq W_j W_j^\star,\ j = 1, \ldots, k-1, \\ & U \succeq 0, \\ & W_0 = \mathbf{0}, \end{aligned} \tag{1.5}$$

Ramana [45]证明了如果原始问题 (1.2)和拓展的Lagrange-Slater对偶问题 (1.4) （或弱形式的拓展的Lagrange-Slater对偶 (1.5)）同时可行，则它们的最优值相等。利用这一强对偶特性，Ramana给出了如下的半正定规划的Farkas引理。

定理 1.2. （半正定规划的*Farkas*引理）给定线性矩阵$\mathsf{A}(x) := \mathsf{A}_0 + \sum_{i=1}^{k} x_i \mathsf{A}_i$，下面的两个半正定系统有且仅有一个成立

1. $\mathsf{A}(\mathbf{x}) \succeq 0$。

2.

$$\begin{aligned}
&\mathbf{Tr}(\mathsf{A}_0(U+W_k)) = -1\\
&\mathbf{Tr}(\mathsf{A}_i(U+W_k)) = 0,\ i=1,\ldots,k,\\
&\mathbf{Tr}(\mathsf{A}_i(U_j+W_{j-1})) = 0,\ i=0,\ldots,k,\ j=1,\ldots,k,\\
&W_0 = \mathbf{0},\\
&U \succeq 0,\\
&\begin{bmatrix} I & W_j^\star \\ W_j & U_j \end{bmatrix} \succeq 0,\ j=1,\ldots,k。
\end{aligned}$$

Klep与Schweighofer将实代数理论与半正定规划对偶理论相结合给出了半正定规划的如下平方和对偶 [37]。

$$\begin{aligned}
d^* := \max\quad & a\\
s.t.\quad & [x]_1^\star U_i [x]_1 + [x]_2^\star W_{i-1}[x]_1 + \mathbf{Tr}(\mathsf{A}S_i) = 0,\ i=1,\ldots,k,\\
& U_j \succeq W_j^* W_j,\ j=1,\ldots,k,\\
& c^\star x - a + [x]_2^\star W_k [x]_1 - \mathbf{Tr}(\mathsf{A}S) = 0,\ i=1,\ldots,k,\\
& S \succeq 0, a \in \mathbb{R}\\
& S_i = \sum_{i=1}^{D} \mathbf{u}_i \mathbf{u}_i^\star, \mathbf{u}_i \in \mathbb{R}[x_1,\ldots,x_k]^D\\
& s(1) = \binom{k+1}{k},\ s(2) = \binom{k+2}{k},\\
& U_i \in \mathbb{R}^{s(1)\times s(1)},\ i=1,\ldots,k,\\
& W_i \in \mathbb{R}^{s(2)\times s(1)},\ i=1,\ldots,k,\\
& W_0 = \mathbf{0} \in \mathbb{R}^{s(2)\times s(1)},
\end{aligned} \tag{1.6}$$

其中$[x]_d$为变元$x_1,\ldots,x_k$的所有次数小于等于d的单项式构成的列向量。Klep与Schweighofer的平方和对偶也可以给出半正定规划的一个Farkas引理，他们文章 [37]的证明中揭示了如下规律：当线性矩阵不等式可行域不满维时，可行域包含在一组实系数线性多项式定义的超平面的交集中，这组实系数线性多项式可由原矩阵A通过一些变换和计算得到，我们后面第三章和第五章的算法就充分运用了这一规律。

1.4 本文主要贡献和结构

给定线性矩阵不等式$\mathsf{A} = \mathsf{A}_0 + X_1\mathsf{A}_1 + \cdots + X_k\mathsf{A}_k \succeq 0$，$\mathsf{A}_0, \ldots, \mathsf{A}_k$为有理系数$(D \times D)$ 对称矩阵，相应元素二进制表示的位长不超过τ，$X_1, \ldots, X_k$为变元，$\mathsf{A} \succeq 0$的可行域记为$\mathfrak{S}(\mathsf{A})$，它包含了使得$\mathsf{A}(\mathbf{x}) = \mathsf{A}_0 + x_1\mathsf{A}_1 + \cdots + x_k\mathsf{A}_k$ 的所有特征值非负的全部实数解$\mathbf{x} \in \mathbb{R}^k$，这是一个闭的凸半代数集。

半正定规划的可行性判定是优化领域的一个基本问题，与半正定规划的准确对偶等问题有密切联系，相关研究工作可参见文献 [37, 45, 54]，这些研究工作主要针对线性矩阵不等式可行域上实数解的判定，且并未给出实数解的具体构造。我们主要关心如下问题：如何判定线性矩阵不等式可行域$\mathfrak{S}(\mathsf{A})$ 是否存在有理数解？在有理数解存在时给出有理数解。进一步，在有理数解不存在而实数解存在时给出实数解精确的实代数数表达形式。

前面我们提到了Safey El Din与支丽红给出的一般凸半代数集上有理点的存在性判定和计算方法，该算法可以给出线性矩阵不等式的可行域上有理数解的存在性判定和计算。相比较 [73]中的算法，我们的算法仅考虑由线性矩阵不等式定义的特殊凸半代数集。

本文目标主要包含以下几个方面：

- 通过探索线性矩阵不等式可行域的特殊几何结构来改进 [73]中的算法，降低算法复杂度。
- 验证Scheiderer反例不存在有理系数多项式平方和分解，从而给出该反例的计算机证明。
- 给出线性矩阵不等式的精确实数解的构造方法，作为应用，给出Scheiderer反例实系数平方和的构造。

我们前面提到了Klep和Schweighofer的平方和对偶 [37]，他们给出了$\mathfrak{S}(\mathsf{A})$不满维时几何结构的代数刻画。第三章中，我们的算法RationalLMI 可以看作文章 [37] 中相关结果的高效版本，我们的算法构造了一组有理系数线性多项式L和$(D-1, D-1)$ 阶线性矩阵不等式$\widehat{\mathsf{A}} \succeq 0$，多项式组$L$和线性矩阵不等式$\widehat{\mathsf{A}} \succeq 0$的公共有理数解与线性矩阵不等式$\mathsf{A} \succeq 0$的有理数解等价。

我们的算法RationalLMI具有迭代特性，如果$\mathfrak{S}(\mathsf{A}) \cap \mathbb{Q}^k \neq \emptyset$，它会输出$\mathfrak{S}(\mathsf{A})$上至少一个有理数解，否则输出空集。算法运行控制在$(k\tau)^{O(1)}2^{O(\min(k,D)D^2)}$

$D^{O(D^2)}$ 位操作以内，输出解的位长控制在$\tau^{O(1)}2^{O(\min(k,D)D^2)}$以内。(参见下面的定理1.3)。作为一般凸半代数集的特殊形式，它显著改进了Safey El Din与支丽红在2010年SIAMOPT [73]上给出的算法复杂度。

定理 1.3. *给定线性矩阵不等式:*

$$\mathsf{A} = \mathsf{A}_0 + X_1\mathsf{A}_1 + \cdots + X_k\mathsf{A}_k \succeq 0$$

*其中$X_1, \ldots, X_k$为变元，$\mathsf{A}_0, \ldots, \mathsf{A}_k$为$D$ 阶有理系数对称矩阵，其中元素二进制表示的位长不超过τ。那么*RationalLMI$(\mathsf{A}, [X_1, \ldots, X_k])$ *返回$\mathfrak{S}(\mathsf{A}) \cap \mathbb{Q}^k$ 中的有理点当且仅当$\mathfrak{S}(\mathsf{A}) \cap \mathbb{Q}^k \neq \emptyset$，否则返回空集。它的运行时间控制在*

$$(k\tau)^{O(1)}2^{O(\min(k,D)D^2)}D^{O(D^2)}$$

位操作，并且在非空情形，输出解坐标的位长控制在$\tau^{O(1)}2^{O(\min(k,D)D^2)}$以内。

对于线性矩阵不等式一般有$k \simeq D^2$，运行时间和输出结果大小的复杂度比之前 [73]的结果要好(我们得到$k^{1.5}$的指数项替代了k^3)。对于n元次数为$2d$的多项式的有理系数平方和分解这个重要应用，应用之前对二项式的估计，我们得到了运行时间的新的界$\tau^{O(1)}2^{O(\mathsf{M}(d,n)^3)}\mathsf{M}(d,n)^{\mathsf{M}(d,n)^2}$，这个界位于$\tau^{O(1)}2^{O(\mathsf{M}(d,n)^3)}$并且显著改进了 [73]的结果。对于输出结果的大小我们也得到了同样的界。这些被总结到下面的定理中。这个算法也是目前多项式有理系数平方和判定和计算的复杂度最好的算法。

定理 1.4. *多项式$f \in \mathbb{Q}[X_1, \ldots, X_n]$ 次数为$2d$，系数位长不超过τ。我们的算法可判定f 是否存在有理系数多项式平方和分解，在存在时给出相应的表示形式，算法复杂度为$\tau^{O(1)}2^{O(\mathsf{M}(d,n)^3)}$，其中$\mathsf{M}(d,n) = \min(d^n, n^d)$。输出表示形式中系数位长的界为$\tau^{O(1)}2^{O(\mathsf{M}(d,n)^3)}$。*

第四章中，借助RAGLIB 软件包 [69]，我们在Maple软件中演算了一些例子。2012年，Scheiderer给出了Sturmfels问题的第一个反例，我们的算法给出了*Scheiderer*反例的第一个计算机验证。需要求有理数解的线性矩阵不等式非常小：大小为6×6，且只有6个变元。我们的算法是第一个用来处理非平凡线性矩阵不等式并且计算有理数解的符号算法。

第五章中，我们设计了新算法RealLMI，给出了$\mathfrak{S}(\mathsf{A})$上精确实数解的计算方法，并给出了Scheiderer 反例精确实系数平方和分解的计算机实现。

本文结构 我们在第二章给出一些预备知识，介绍线性矩阵不等式的一些基本性质，Gram矩阵与多项式平方和分解，以及计算实代数几何中半代数集实数解判定和计算的一些结果。

在第三章，我们先给出算法RationalLMI主要思路和流程图，之后给出了两个子程序BasicCasesLMI和WeakLMI，第一个用来处理简单情形（单变元、一阶矩阵和$\mathfrak{S}(A)$满维），第二个处理$\mathfrak{S}(A)$不满维情形。然后我们给出了主算法的描述，并给出了正确性证明和复杂度分析，最后给出了两个简单例子。

在第四章，我们先回顾了有理系数平方和表示的一些主要结果和进展，然后应用算法RationalLMI给出了有理系数平方和计算的几个简单例子。最后我们将算法应用于Scheiderer的例子，给出了该例子不存在有理系数平方和表示的第一个计算机验证。

在第五章，我们先给出算法RealLMI的主要特点和流程图，然后给出了子程序BasicRealLMI、WeakRealLMI和主算法的描述，最后给出了Scheiderer反例精确实系数平方和分解的计算机实现。

在第六章，我们对本文结果进行了总结，并给出了今后的一些研究方向。

第二章　预备知识

2.1　矩阵理论基本知识

基本定义和记号　实对称矩阵M称为正定（半正定）如果它的所有特征值为正（非负），我们分别记为$\mathsf{M} \succ 0$ 和$\mathsf{M} \succeq 0$。

下面，给定环R上的矩阵或向量M，$\mathsf{M}^\star$代表M的转置。下面的命题2.1是一些常用结论，可以参见 [31, pp. 399]。

命题 2.1. *给定矩阵$\mathsf{M} \in \mathbb{R}^{n\times n}$，下面结论等价:*

1. *矩阵M为半正定的（即$\mathsf{M} \succeq 0$）。*
2. *对所有的$\mathbf{x} \in \mathbb{R}^n$，$\mathbf{x}^\star \mathsf{M} \mathbf{x} \geq 0$。*
3. *矩阵M的所有特征值非负。*
4. *矩阵M的$2^n - 1$个主子式非负。*
5. *记矩阵M的特征多项式为$\chi(y) = y^n + m_{n-1}y^{n-1} + \cdots + m_0$，则$(-1)^{(n-i)} m_i \geq 0$，对$0 \leq i \leq n-1$。*
6. *存在矩阵分解$\mathsf{M} = VV^\star$，这里$V \in \mathbb{R}^{n\times r}$，并且$r$为矩阵$\mathsf{M}$的秩。*

记$X_1, \ldots, X_k$为变元，$\mathsf{A}_0, \ldots, \mathsf{A}_k$为$(D \times D)$实对称矩阵，$\mathsf{A}$为线性矩阵$\mathsf{A}_0 + X_1\mathsf{A}_1 + \cdots + X_k\mathsf{A}_k$。对$\mathbf{x} = (x_1, \ldots, x_k) \in \mathbb{R}^k$，我们记$\mathsf{A}(\mathbf{x})$代表$\mathsf{A}_0 + x_1\mathsf{A}_1 + \cdots + x_k\mathsf{A}_k$。我们考虑线性矩阵不等式

$$\mathsf{A} = \mathsf{A}_0 + X_1\mathsf{A}_1 + \cdots + X_k\mathsf{A}_k \succeq 0。$$

我们记$\mathfrak{S}(\mathsf{A}) = \{\mathbf{x} \in \mathbb{R}^k \mid \mathsf{A}(\mathbf{x}) \succeq 0\}$为$\mathsf{A}$的可行域。这是$\mathbb{R}^k$上的一个闭的凸半代数集。若$\mathfrak{S}(\mathsf{A}) = \emptyset$，我们称线性矩阵不等式$\mathsf{A} \succeq 0$不可行，否则称为可行的。当$\mathsf{A}$可行时，如果存在向量$\mathbf{x} \in \mathbb{R}^k$使得$\mathsf{A}(\mathbf{x}) \succ 0$，我们称$\mathsf{A}$为强可行的，否则称为弱可行的。当$\mathsf{A}$为强可行时，$\mathfrak{S}(\mathsf{A})$为满维的，当$\mathsf{A}$为弱可行或不可行时，$\mathfrak{S}(\mathsf{A})$不满维。

线性矩阵不等式的基本性质

引理 2.2. *记矩阵$\mathsf{A}=\mathsf{A}_0+X_1\mathsf{A}_1+\cdots+X_k\mathsf{A}_k$，其中$\mathsf{A}_i$为有理系数$(D\times D)$对称矩阵（$0\leq i\leq k$），$E\subset\mathbb{R}^k$为一组方程定义的仿射线性子空间。假设子空间$E$中的点满足矩阵$\mathsf{A}$的第$i$行和第$i$列元素定义的方程，$\widehat{\mathsf{A}}$为删除矩阵$\mathsf{A}$的第$i$行和第$i$列元素后的$(D-1,D-1)$矩阵。那么$\mathfrak{S}(\widehat{\mathsf{A}})\cap E=\mathfrak{S}(\mathsf{A})\cap E$。*

证明. 根据命题2.1，$\mathfrak{S}(\mathsf{A})$(相应的，$\mathfrak{S}(\widehat{\mathsf{A}})$)为使得$\mathsf{A}$ (相应的，$\widehat{\mathsf{A}}$)的所有主子式非负的点构成的集合。根据构造，矩阵$\widehat{\mathsf{A}}$的所有主子式包含在矩阵A的所有主子式中，于是有$\mathfrak{S}(\mathsf{A})\subset\mathfrak{S}(\widehat{\mathsf{A}})$，并且$\mathfrak{S}(\mathsf{A})\cap E\subset\mathfrak{S}(\widehat{\mathsf{A}})\cap E$。

取$\mathbf{x}\in\mathfrak{S}(\widehat{\mathsf{A}})\cap E$，矩阵$\mathsf{A}$的第$i$行和第$i$列元素代入子空间$E$中的点后为0，则那些属于矩阵$\mathsf{A}$而不属于矩阵$\widehat{\mathsf{A}}$的主子式在$\mathbf{x}$处为0。矩阵$\mathsf{A}$的所有主子式非负。这样证明了反包含关系$\mathfrak{S}(\widehat{\mathsf{A}})\cap E\subset\mathfrak{S}(\mathsf{A})\cap E$，引理得证。 □

引理 2.3. *记矩阵$\mathsf{A}=\mathsf{A}_0+X_1\mathsf{A}_1+\cdots+X_k\mathsf{A}_k$，其中$\mathsf{A}_i$为有理系数$(D\times D)$对称矩阵$(0\leq i\leq k)$，$\mathsf{P}$为可逆矩阵并且$\mathsf{A}'=\mathsf{P}^\star\mathsf{A}\mathsf{P}$。如果$\mathbf{x}\in\mathfrak{S}(\mathsf{A})$，那么$\mathbf{x}\in\mathfrak{S}(\mathsf{A}')$。*

证明. 如果$\mathbf{x}\in\mathfrak{S}(\mathsf{A})$，我们下面证明$\mathbf{x}\in\mathfrak{S}(\mathsf{A}')$。用矩阵$\mathsf{P}^{-1}$替代矩阵$\mathsf{P}$可以得到反向包含关系的证明。实对称矩阵是半正定的当且仅当它的所有主子式非负（命题2.1）。

由于$\mathbf{x}\in\mathfrak{S}(\mathsf{A})$，$\mathsf{A}$ 的所有主子式在$\mathbf{x}$处非负。考虑删除第i_1到第i_r行和列得到的主子式$\mathfrak{m}$，考虑矩阵P删除第i_1到第i_r行和列得到的主子式$\mathfrak{p}$。直接计算可得，矩阵A' 删除第i_1到第i_r行和列得到的主子式等于$\mathfrak{m}\mathfrak{p}^2$，因此在$\mathbf{x}$处非负。通过对所有可能的$\{i_1,\ldots,i_r\}$迭代，证明矩阵$\mathsf{A}'$ 的所有主子式在$\mathbf{x}$处非负。我们得到$\mathfrak{S}(\mathsf{A})\subset\mathfrak{S}(\mathsf{A}')$。 □

2.2 Gram矩阵与多项式平方和表示

给定多项式$f\in\mathbb{Q}[x_1,\ldots,x_n]$ 次数为$2d$，判定它是否可以表示为多项式的平方和可以借助下面的Gram矩阵表示方法。

定理 2.4. *[57] 实系数多项式$f(\mathbf{x})$能分解为$\mathbb{R}[\mathbf{x}]$上多项式平方和的充分必要条件为$f(\mathbf{x})$可以表示为*

$$f(\mathbf{x})=\mathrm{v}^\star\cdot\mathsf{M}\cdot\mathrm{v}。\tag{2.1}$$

其中 v 为$x_1,\ldots,x_n$的所有次数小于等于$d=\lceil \deg(f)/2\rceil$的单项式构成的列向量，M 为实对称半正定矩阵，也称之为 f 的 *Gram* 矩阵。

Parrilo [48, 49]给出了下面的定理：

定理 2.5. 一个n变元次数为$2d$的多项式是否存在多项式平方和分解可以通过求解一个半正定规划可行性判定问题来验证。如果多项式是稠密的（无稀疏性），线性矩阵不等式的维数为$\binom{n+d}{n}\times\binom{n+d}{n}$。

通过高斯消去，存在整数$k\le \frac{1}{2}D(D+1)-\binom{n+2d}{n}$使得

$$\mathsf{M}=\{\mathsf{M}_0+Y_1\mathsf{M}_1+\ldots+Y_k\mathsf{M}_k,\ Y_1,\ldots,Y_k\in\mathbb{R}\}。\tag{2.2}$$

多项式f可以表示为多项式平方和形式等价于矩阵M可以填充为半正定矩阵(参见 [41])。如果多项式 f 是稀疏的，那么向量 v 和矩阵 M 通常也是稀疏的。我们可以通过分析牛顿多面体 (Newton Polytope) [14, 48, 62, 80] 来减小问题的规模。满足等式条件 (2.1) 的矩阵 M 不唯一，并构成全体对称矩阵集合 $\mathbb{S}$ 的一个仿射子空间

$$\mathcal{X}=\{\mathsf{M}\mid \mathsf{M}^\star=\mathsf{M}, f(\mathbf{x})=\mathrm{v}^\star\cdot\mathsf{M}\cdot\mathrm{v}\}。\tag{2.3}$$

如果仿射子空间 $\mathcal{X}$ 与对称半正定矩阵锥 $\mathbb{S}^+$ 的交集非空，$f(\mathbf{x})$ 即可分解为平方和形式。如果矩阵 M 的元素是有理数，则 f 能够分解为 $\mathbb{Q}[\mathbf{x}]$ 中的多项式平方和。

例 2.1. 我们考虑如下多项式：

$$f=x^6+4\,x^3\,y^2\,z+y^6+2\,y^4\,z^2+y^2\,z^4+4\,z^6。$$

假设

$$f=[x^3,y^3,y^2z,yz^2,z^3]\,\mathsf{A}\,[x^3,y^3,y^2z,yz^2,z^3]^\star,$$

f的Gram矩阵A是一个5×5对称矩阵：

$$\mathsf{A}=\begin{bmatrix}1 & 0 & 2 & 0 & 0\\ 0 & 1 & 0 & X_1 & -X_2\\ 2 & 0 & -2\,X_1+2 & X_2 & X_3\\ 0 & X_1 & X_2 & 1-2\,X_3 & 0\\ 0 & -X_2 & X_3 & 0 & 4\end{bmatrix}。$$

A有三个变元X_1, X_2, X_3，对应4个对称矩阵$\mathsf{A}_0, \mathsf{A}_1, \mathsf{A}_2, \mathsf{A}_3$。

通过计算，我们得到$\mathsf{A} \succeq 0$的一个特解$X_1 = -2, X_2 = 0, X_3 = -2$。将上述特解代入$\mathsf{A}$，得到Gram矩阵

$$\mathsf{M} = \begin{bmatrix} 1 & 0 & 2 & 0 & 0 \\ 0 & 1 & 0 & -2 & 0 \\ 2 & 0 & 6 & 0 & -2 \\ 0 & -2 & 0 & 5 & 0 \\ 0 & 0 & -2 & 0 & 4 \end{bmatrix}。$$

对矩阵M作LU分解，我们可以得到f的如下平方和分解：

$$f = (x^3 + 2\,y^2\,z)^2 + (y^3 - 2\,y\,z^2)^2 + 2\,(y^2\,z - z^3)^2 + y^2\,z^4 + 2\,z^6。$$

2.3 计算实代数几何基本知识

给定半代数集合

$$\mathfrak{S} = \{\mathbf{x} \in \mathbb{R}^k \mid f_1(\mathbf{x}) \geq 0, \ldots, f_s(\mathbf{x}) \geq 0\},$$

其中 $f_1, \ldots, f_s \in \mathbb{R}[x_1, \ldots, x_k]$。

计算半代数集连通分支中的样本点或判定一个半代数集是否为空是计算实代数几何中的一个基本问题，它可以采用柱形代数分解算法 [15]，但该算法具有变元个数的双指数复杂度，在实际运算中并不高效。近年来，半代数集上的实数解的存在性判定和计算多采用关键点方法，如 [3,5,6,20,24,25,61,68,71,72]，关于这些算法，也可以参考综述性文章 [4,67]。

下面我们给出计算实代数几何的一些基本结果，这些知识在后面的算法中会多次用到。

2.3.1 有理单变元表示

我们在第三章和第五章中的算法会遇到由有理系数多项式定义的半代数集$\mathfrak{S}$上实数解求解问题，关于这一问题的求解算法可以参见 [7, 第13章]。通过算法得到的这些实数解的坐标为实代数数。和 [73]一样，对于一个实数解$(\alpha_1, \ldots, \alpha_k)$，我们用$\mathscr{Q}, \Theta$对其编码。$\mathscr{Q}$是一个零维参数化

$$\mathscr{Q} = (q(T), q_0(T), q_1(T), \ldots, q_k(T))$$

$q, q_0, \ldots, q_k$属于$\mathbb{Q}[T]$，$\gcd(q, q_0) = 1$, q **不可约**并且对于q的根ϑ，$\alpha_i = q_i(\vartheta)/q_0(\vartheta)$为其坐标，$\Theta$是$\vartheta$ 的一个Thom编码（关于Thom编码和单变元表示的更详细叙述，我们可以参考 [7, 第2,12章]）。

我们后面将用到程序MinPol和Param，它们的输入为实代数数点的编码$\mathscr{Q}, \Theta$, 分别返回多项式q和向量$(\frac{q_1}{q_0}, \ldots, \frac{q_k}{q_0})$。

现在，给定一个零维参数化$\mathscr{U} = (q, q_0, \mathscr{U}_1, \ldots, \mathscr{U}_D) \subset \mathbb{Q}[T]^{2+D\times D}$（它的次数为$\delta$）和一个Thom编码$\Theta$，它们给出了$D$个向量$(\mathbf{u}_1, \ldots, \mathbf{u}_D)$ $(\mathbf{u}_i \in \mathbb{R}^D)$的编码。我们将用程序ExtractFirstEntry$((\mathscr{U}, \Theta), D)$来返回第一个向量$\mathbf{u}_1$的编码$((q, q_0, \mathscr{U}_1), \Theta)$。

2.3.2　半代数集上实数解的存在性判定和计算

下面给出两个子程序Decision和OpenDecision，关于更详细的描述，也可以参见（ [73]， [7, 第15章] 或 [5]）。

记Φ为一个无量词的公式，$\Phi = \{f_1(\mathbf{x}) \geq 0, \ldots, f_s(\mathbf{x}) \geq 0\}$, 它涉及$s$个$k$变元次数小于等于$\delta$的多项式，并且多项式系数的位长的界为$\tau$，令$\mathfrak{S} \subset \mathbb{R}^k$为$\Phi$定义的半代数集。

子程序Decision

输入：Φ为有理系数多项式不等式定义的无量词公式

输出：

- 当$\mathfrak{S} \neq \emptyset$时，返回$\mathfrak{S}$上的实数点的编码$(\mathscr{Q}, \Theta)$；
- 其他情况返回$\emptyset$。

复杂度：

- 运行的位操作数控制在$\tau s^{k+1}\delta^{O(k)}$以内，
- $\mathscr{Q}$中多项式次数的界为$O(\delta^k)$，
- $\mathscr{Q}$中的所有多项式系数的位长控制在$\tau\delta^{O(k)}$以内。

假设Φ为一个由s个次数为δ的有理系数多项式$\mathbb{Q}[x_1, \ldots, x_k]$（元素位长的界为$\tau$）的严格不等式系统，半代数集$\mathfrak{S} \subset \mathbb{R}^k$由$\Phi$定义，我们用程序OpenDecision计算$\mathfrak{S} \cap \mathbb{Q}^k$的有理数解。

子程序OpenDecision

输入：Φ为有理系数多项式的严格不等式定义的无量词公式

输出：

- 当$\mathfrak{S} \neq \emptyset$时，返回$\mathfrak{S}$中的有理点；
- 其他情况返回空集。

复杂度：

- 运行的位操作数控制在$\tau^{O(1)}s^{k+1}\delta^{O(k)}$以内；
- 在$\mathfrak{S}$非空情形，返回有理系数的位长的界为$\tau\delta^{O(k)}$。

我们将这些复杂度结果总结到下面的命题中。

命题 2.6. *[5]* 令Φ为一个由s个k 变元且次数小于等于δ系数位长的界为τ的多项式定义的无量词公式，$\mathfrak{S} \subset \mathbb{R}^k$ 为Φ定义的半代数集。我们给出算法Decision，它的输入为Φ，当$\mathfrak{S} \neq \emptyset$时，返回$\mathfrak{S}$中点的编码$(\mathscr{Q}, \Theta)$，否则返回$\emptyset$，运行的位操作数控制在$\tau^{O(1)}s^{k+1}\delta^{O(k)}$以内。$\mathscr{Q}$中多项式次数和系数位长的界分别为$O(\delta^k)$和$\tau\delta^{O(k)}$。

当Φ只包含严格不等式，当$\mathfrak{S} \neq \emptyset$时，算法OpenDecision将返回$\mathfrak{S}$中的一个有理点，否则返回空集。运行的位操作数控制在$\tau^{O(1)}s^{k+1}\delta^{O(k)}$以内。在非空情形，输出位长的界为$\tau\delta^{O(k)}$。

2.3.3 提取有理系数线性多项式

下面，我们考虑一个实代数数$\vartheta \in \mathbb{R}$，它的极小多项式是次数为δ的多项式$q \in \mathbb{Q}[\vartheta]$。我们同时考虑线性多项式

$$\mathscr{L} = g_0(\vartheta) + g_1(\vartheta)X_1 + \cdots + g_k(\vartheta)X_k$$

其中$g_0, \ldots, g_k$为$\mathbb{Q}(\vartheta)$中的有理分式，次数小于等于$\delta - 1$的q_0是它们的共同分母，它们的分子$n_0, \ldots, n_k$ 的次数也小于等于$\delta - 1$。我们假设$\mathsf{gcd}(q_0, q) = 1$，并且存在$0 \leq i \leq k$使得$n_i \neq 0$。

考虑有理系数线性多项式$\ell_0,\ldots,\ell_{\delta-1}$，它们是多项式

$$n_0+n_1X_1+\cdots+n_kX_k$$

中$1,\vartheta,\ldots,\vartheta^{\delta-1}$的系数。根据假设，存在$i$使得$n_i\neq 0$，于是存在$j$使得$\ell_j\neq 0$。我们记程序ExtractLinForms，它的输入为$\mathscr{L},q$，并且返回所有的满足$\ell_j\neq 0$的线性多项式ℓ_j。

下面的引理是从文章 [73]的算法正确性证明中提取出来的。后面的第三章和第五章多次用到这个结论，我们把结论列在下面，然后给出证明。

引理 2.7. *[73]* 令$\mathfrak{S}\subset\mathbb{R}^k$为半代数集，$\vartheta$是一个次数为$\delta$的实代数数，$q$ 是它的极小多项式，τ是q 中系数位长的界，$\mathscr{L}$ 是$\mathbb{Q}(\vartheta)[X_1,\ldots,X_k]$上的线性多项式。假设$\mathscr{L}$在$\mathfrak{S}$的所有点上为$0$。那么所有的线性多项式$L=\mathsf{ExtractLinForms}(\mathscr{L},q)$在$\mathfrak{S}\cap\mathbb{Q}^k$的所有点上为$0$，并且$L$可以在$O(\tau k\delta^{O(1)})$位操作内获得。输出结果系数位长的界为$O(\tau)$。

证明. 取$\mathbf{x}=(x_1,\ldots,x_k)\in\mathfrak{S}\cap\mathbb{Q}^k$；由假设$\mathscr{L}$在$\mathbf{x}$处为$0$，我们得到$n_0+n_1x_1+\cdots+n_kx_k=0$。由于$\vartheta$是次数为$\delta$ 的实代数数，并且n_i次数小于等于$\delta-1$，我们得到所有的线性多项式$\ell_0,\ldots,\ell_{\delta-1}$在$\mathbf{x}$处为$0$。运行时间和输出结果系数位长的界可以直接得到。 □

第三章　线性矩阵不等式有理数解的计算方法

3.1　前言

线性矩阵不等式有理数解的判定与计算对于多项式有理系数平方和计算具有重要意义，借助于Klep与Schweighofer对线性矩阵不等式定义凸集特殊几何结构的代数描述，结合计算实代数几何中半代数集样本点的有理单变元表示，我们给出了线性矩阵不等式有理数解的存在性判定和计算方法RationalLMI。

给定线性矩阵不等式$\mathsf{A}=\mathsf{A}_0+X_1\mathsf{A}_1+\cdots+X_k\mathsf{A}_k\succeq 0$，它的可行域为$\mathfrak{S}(\mathsf{A})$。其中$X_1,\ldots,X_k$为变元，$\mathsf{A}_0,\ldots,\mathsf{A}_k$ 是有理系数的$(D\times D)$对称矩阵，其中元素二进制表示的位长不超过τ。

当矩阵阶数为$D=1$或变元个数$k=1$以及$\mathfrak{S}(\mathsf{A})$满维时，我们可利用子程序BasicCasesLMI来处理这几类情形。

若存在非零向量$\mathbf{u}\in\mathbb{R}^D-\{\mathbf{0}\}$使得$\mathsf{A}\mathbf{u}=\mathbf{0}$，可利用向量$\mathbf{u}$构造可逆矩阵$\mathsf{P}$，满足$\mathsf{P}\mathbf{e}_1=\mathbf{u}$，对原矩阵做合同变换$\mathsf{A}'=\mathsf{P}^\star\mathsf{A}\mathsf{P}$，$\mathsf{A}'$的第一行和第一列为$\mathbf{0}$。$\widehat{\mathsf{A}}$表示删除矩阵$\mathsf{A}'$的第一行和第一列后所得到的$(D-1,D-1)$矩阵，调用命令$\mathsf{RationalLMI}(\widehat{\mathsf{A}},[X_1,\ldots,X_k])$可以给出$\mathfrak{S}(\widehat{\mathsf{A}})$上有理数解的存在性判定和计算，此问题与原问题$\mathfrak{S}(\mathsf{A})$上有理数解的存在性判定和计算是等价的。

当$\mathfrak{S}(\mathsf{A})$不满维时，若不存在非零向量$\mathbf{u}\in\mathbb{R}^D-\{\mathbf{0}\}$使得$\mathsf{A}\mathbf{u}=\mathbf{0}$，那么存在非零向量$\mathbf{u}_1,\ldots,\mathbf{u}_s\in\mathbb{R}^D-\{\mathbf{0}\},1\le s\le D$，使得$\sum_{i=1}^s\mathbf{u}_i^\star\mathsf{A}\mathbf{u}_i=0$，我们可以通过子程序WeakLMI得到这样一组向量。不妨设$u_{11}\neq 0$，构造可逆矩阵$\mathsf{P}=[\mathbf{u}_1,\mathsf{e}_2,\ldots,\mathsf{e}_\mathsf{D}]$，对原矩阵做合同变换

$$\mathsf{A}'=\mathsf{P}^\star\mathsf{A}\mathsf{P}=\begin{bmatrix}\mathscr{L}_1 & \mathscr{L}_2 & \cdots & \mathscr{L}_D\\ \mathscr{L}_2 & & & \\ \vdots & & \widehat{\mathsf{A}} & \\ \mathscr{L}_D & & & \end{bmatrix}。$$

我们得到一组实系数线性多项式$\mathscr{L}_1,\ldots,\mathscr{L}_D\in\mathbb{R}[X_1,\ldots,X_k]$，这些线性多项式定义的超平面的交集包含了$\mathfrak{S}(\mathsf{A})$的所有实数解，即

$$(a_1,\ldots,a_k)\in\mathfrak{S}(\mathsf{A})\Longrightarrow\mathscr{L}_i(a_1,\ldots,a_k)=0,i=1,\ldots,D。$$

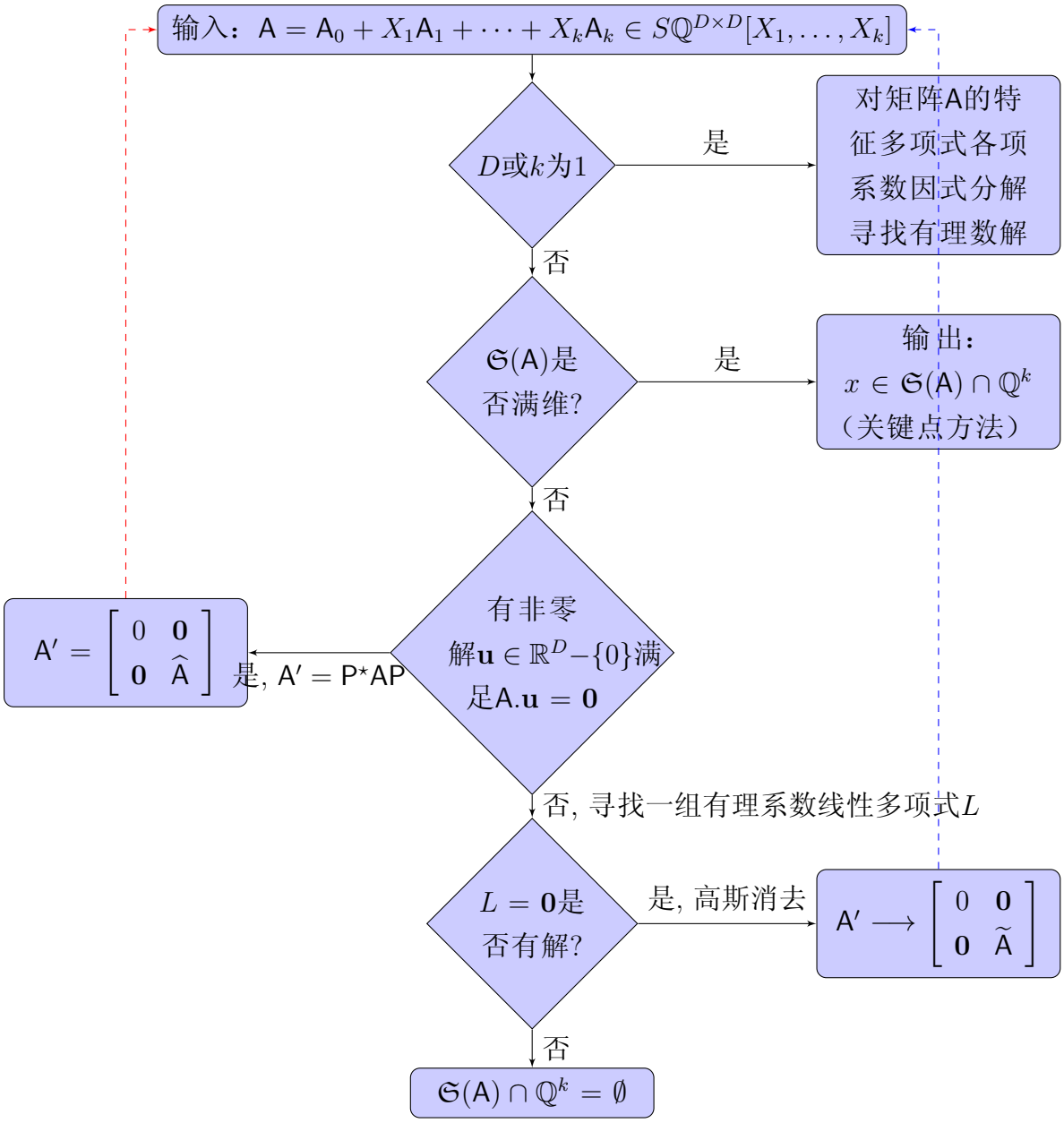

图 3.1: 线性矩阵不等式可行域有理数解判定和计算流程图

更进一步，我们可以从这组实系数线性多项式构造有理系数线性多项式，将这组实系数线性多项式表示为实代数数ϑ的多项式的形式，即

$$\mathscr{L}_i = l_{i,0}(X_1, \ldots, X_k) + \cdots + l_{i,\delta-1}(X_1, \ldots, X_k)\vartheta^{\delta-1}。$$

其中ϑ的极小多项式的次数为δ。

记集合L表示实系数线性多项式$\mathscr{L}_1, \ldots, \mathscr{L}_D$中$\vartheta^{\delta-1}, \ldots, \vartheta, 1$的所有系数，这些系数为$\mathbb{Q}[X_1, \ldots, X_k]$中的有理系数线性多项式。线性多项式$\mathscr{L}_1, \ldots, \mathscr{L}_D$定义超平面的交集上的有理数解与线性多项式$L$定义超平面的交集上的有理数解相等，因此$L = 0$的解集包含了$\mathfrak{S}(\mathsf{A})$上的全部有理数解。如果$L = 0$无解，那么$\mathfrak{S}(\mathsf{A})$没有有理数解。否则，可以利用高斯消去法给出一部分变元用另一部分变元的线性表示形式，我们同时得到了一个阶数更小的矩阵$\widetilde{\mathsf{A}}$，

$$\mathsf{A}' \longrightarrow \begin{bmatrix} 0 & \mathbf{0} \\ \mathbf{0} & \widetilde{\mathsf{A}} \end{bmatrix}。$$

$\mathfrak{S}(\widetilde{\mathsf{A}})$的有理数解是$\mathfrak{S}(\mathsf{A})$上有理数解的投影。如果$\mathfrak{S}(\widetilde{\mathsf{A}})$上不含有理数解，则$\mathfrak{S}(\mathsf{A})$上也不含有理数解，否则我们利用命令Evaluate，可以从$\mathfrak{S}(\widetilde{\mathsf{A}})$的有理数解恢复$\mathfrak{S}(\mathsf{A})$上的有理数解。

3.2　子程序BasicCasesLMI

3.2.1　算法描述

给定线性矩阵不等式:

$$\mathsf{A} = \mathsf{A}_0 + X_1\mathsf{A}_1 + \cdots + X_k\mathsf{A}_k \succeq 0,$$

它的可行域为$\mathfrak{S}(\mathsf{A})$。其中$X_1, \ldots, X_k$为变元，$\mathsf{A}_0, \ldots, \mathsf{A}_k$为$D$ 阶有理系数对称矩阵，其中元素二进制表示的位长不超过τ。我们给出子程序BasicCasesLMI的具体描述，它的输入为$\mathsf{A}, [\mathsf{X}_1, \ldots, \mathsf{X}_k]$ 并且

- 当$k = 1$，如果$\mathfrak{S}(\mathsf{A}) \cap \mathbb{Q} \neq \emptyset$，返回$\mathfrak{S}(\mathsf{A})$ 中的至少一个有理点；否则返回空集；
- 当$k > 1$，如果$\mathfrak{S}(\mathsf{A})$有非空内点，返回$\mathfrak{S}(\mathsf{A})$ 中的至少一个有理点；否则返回false。

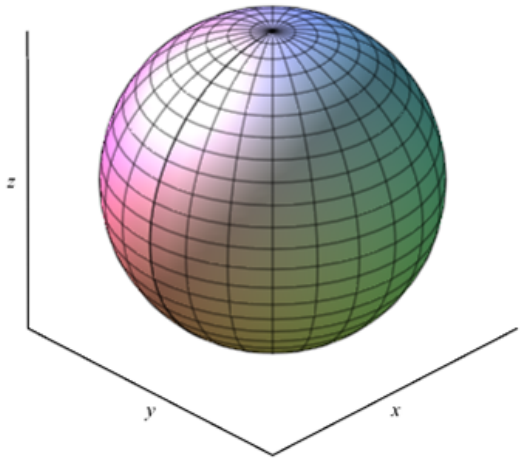

图 3.2: 线性矩阵不等式可行域满维情形

记矩阵A的特征多项式为$\chi(y) = y^D + m_{D-1}y^{D-1} + \cdots + m_0$，我们记$\Phi$为下面的公式：

$$\Phi = \{(-1)^{(i+D)}m_i \geq 0,\ 0 \leq i \leq D-1\}$$

并且Ψ为下面的公式：

$$\Psi = \{(-1)^{(i+D)}m_i > 0,\ 0 \leq i \leq D-1\}.$$

由 [57]，半代数集$\mathfrak{S}(\mathsf{A})$ 由Φ定义，$\mathfrak{S}(\mathsf{A})$的内点由Ψ定义。

BasicCasesLMI$(\mathsf{A}, [X_1, \ldots, X_k])$

1. 集合$\mathscr{U}$初始化为空集，如果$k = 1$ 并且存在一个m_i（$0 \leq i \leq D-1$）的一个线性因子$X - a$ $(a \in \mathbb{Q})$ 并且$(-1)^{(j+D)}m_j(a) \geq 0$ （$j \neq i$），把a放入集合$\mathscr{U}$中。返回$\mathscr{U}$。

2. $\mathscr{U}$ = OpenDecision(Ψ)。如果$\mathscr{U}$ 不为空集，返回$\mathscr{U}$，否则返回false。

命题 3.1. 给定线性矩阵不等式:

$$\mathsf{A} = \mathsf{A}_0 + X_1\mathsf{A}_1 + \cdots + X_k\mathsf{A}_k \succeq 0$$

其中$X_1, \ldots, X_k$为变元，$\mathsf{A}_0, \ldots, \mathsf{A}_k$为$(D \times D)$有理系数对称矩阵，其中元素二进制表示的位长不超过$\tau$。

如果$k=1$并且$\mathfrak{S}(\mathsf{A})\cap\mathbb{Q}\neq\emptyset$，BasicCasesLMI$(\mathsf{A},[X_1])$ 返回$\mathfrak{S}(\mathsf{A})$中的至少一个有理数解，否则返回空集。

如果$\mathfrak{S}(\mathsf{A})\subset\mathbb{R}^k$ 满维，BasicCasesLMI$(\mathsf{A},[X_1,\ldots,X_k])$返回$\mathfrak{S}(\mathsf{A})\cap\mathbb{Q}^k$中的有理点，其他情况返回false。

运行位操作数控制在$\tau^{O(1)}D^{O(k)}$以内，在非空情形，输出结果位长的界为$\tau^{O(1)}D^{O(k)}$。

3.2.2　算法正确性证明与复杂度分析

如果$k=1$，此时$\mathfrak{S}(\mathsf{A})\subset\mathbb{R}$（第1步）。由于$\mathfrak{S}(\mathsf{A})$为凸集，它为空集或一个点或一个包含非空内点的区间。假设它是一个点，它是Φ的唯一解，因为$\mathfrak{S}(\mathsf{A})$是由Φ来定义的。通过假设，这个解不是Ψ 的解（否则$\mathfrak{S}(\mathsf{A})$ 将包含非空内点）。假设$\mathfrak{S}(\mathsf{A})$为一个区间，它的端点如果是有理点，必定为某个m_i的有理系数线性因子的解，并且满足公式Φ。因此可以通过寻找满足$(-1)^{j+D}m_j$'s（$j\neq i$）非负的那些m_i（$0\leq i\leq D-1$）的有理系数线性因子的解。假设$\mathfrak{S}(\mathsf{A})$不满维。我们可以推出$\mathfrak{S}(\mathsf{A})$为空集，算法结束。注意到在单变元情形，因式分解和实根隔离的运行时间为τ 和D 的多项式，并且如果输出有理数解，该解位长的界为$(D\tau)^{O(1)}$ (参见 [42])。

如果$k\geq 2$。假设$\mathfrak{S}(\mathsf{A})$满维；它包含非空内点。于是，根据命题2.6，第2 步返回$\mathfrak{S}(\mathsf{A})\cap\mathbb{Q}^k$ 中的有理点当且仅当$\mathfrak{S}(\mathsf{A})\neq\emptyset$。假设$\mathfrak{S}(\mathsf{A})$不满维。由公式$\Psi$定义的半代数集是$\mathfrak{S}(\mathsf{A})$的内点；我们推断它是空集。于是，根据命题2.6，$\mathscr{U}$为空集，我们返回false。根据命题2.6，运行时间和输出结果的界可以直接得到。
□

3.3　子程序WeakLMI

3.3.1　算法描述

给定线性矩阵不等式:

$$\mathsf{A}=\mathsf{A}_0+X_1\mathsf{A}_1+\cdots+X_k\mathsf{A}_k\succeq 0,$$

它的可行域为$\mathfrak{S}(\mathsf{A})$。其中$X_1,\ldots,X_k$为变元，$\mathsf{A}_0,\ldots,\mathsf{A}_k$为$(D\times D)$有理系数对称矩阵，其中元素二进制表示的位长不超过$\tau$。我们描述子程序WeakLMI，它的

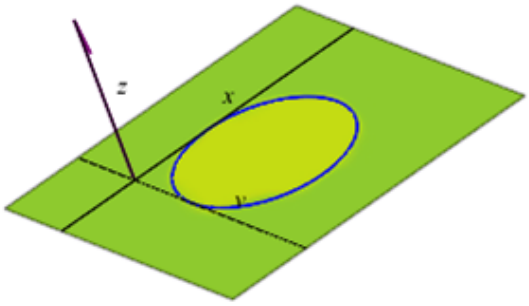

图 3.3: 线性矩阵不等式可行域不满维情形

输入为$\mathsf{A}, [X_1, \ldots, X_k]$，其中$\mathfrak{S}(\mathsf{A})$不满维，并且不存在非零向量$\mathbf{u} \in \mathbb{R}^D - \{\mathbf{0}\}$使得$\mathsf{A}\mathbf{u} = \mathbf{0}$。子程序返回$\widehat{\mathsf{A}}, L$使得

- $\widehat{\mathsf{A}}$是$(D-1) \times (D-1)$对称矩阵，它的元素在$\mathbb{Q}[X_1, \ldots, X_k]$中；
- L是$\mathbb{Q}[X_1, \ldots, X_k]$中的一组有理系数线性多项式，它们在$\mathfrak{S}(\mathsf{A}) \cap \mathbb{Q}^k$的所有点处取值为0；我们令$\mathsf{Sols}(L) \subset \mathbb{R}^k$ 表示L的公共解构成的线性子空间；
- $\widehat{\mathsf{A}}, L$满足$\mathfrak{S}(\widehat{\mathsf{A}}) \cap \mathsf{Sols}(L) \cap \mathbb{Q}^k = \mathfrak{S}(\mathsf{A}) \cap \mathbb{Q}^k$。

线性矩阵不等式的可行域$\mathfrak{S}(\mathsf{A})$为凸集。于是，根据 [73, 引理3.4]，我们知道存在线性多项式$\mathscr{L} \in \mathbb{R}[X_1, \ldots, X_k]$，它在$\mathfrak{S}(\mathsf{A})$的所有点处取值为0。在 [37, 命题3.3.1] 中，Klep 和Schweighofer 探索了线性矩阵不等式的特殊性质，并且证明了$\mathsf{A} \succeq 0$是弱可行的（即$\mathfrak{S}(\mathsf{A})$不含有非空内点）当且仅当存在非零线性多项式$\mathscr{L} \in \mathbb{R}[X_1, \ldots, X_k]$ 和$(D \times D)$矩阵W（元素在$\mathbb{R}[X_1, \ldots, X_k]$中）使得

$$\mathrm{Tr}(\mathsf{A}\mathsf{W}^\star\mathsf{W}) = -\mathscr{L}^2。$$

根据 [37, 命题3.3.1]证明中第一行的提示，这推出$\mathscr{L}$在$\mathfrak{S}(\mathsf{A})$的所有点处取值为0。更强的结论是在 [37, 引理4.3.5]的证明中给出的：存在$\mathbb{R}[X_1, \ldots, X_k]$上的线性多项式$\mathscr{L}_1, \ldots, \mathscr{L}_D$和$(D \times D)$矩阵$\mathsf{W}_1, \ldots, \mathsf{W}_D$，使得

$$\mathrm{Tr}(\mathsf{A}\mathsf{W}_i^\star\mathsf{W}_i) = -\mathscr{L}_i^2, \text{ for } 1 \le i \le D。$$

在 [37, 引理4.3.5]的证明中，矩阵$\mathsf{W}_1,\ldots,\mathsf{W}_D$由下面半代数集中的点来构造

$$G_1=\{\mathbf{u}\in\mathbb{R}^D-\{\mathbf{0}\}\mid \mathbf{u}^\star\mathsf{A}\mathbf{u}=0\},$$
$$G_2=\{(\mathbf{u}_1,\ldots,\mathbf{u}_D)\in\mathbb{R}^D\mid \sum_{i=1}^{D}\mathbf{u}_i^\star\mathsf{A}\mathbf{u}_i=0,\mathbf{u}_1,\mathbf{u}_2\neq\mathbf{0}\}。$$

下面的算法来构造$\mathscr{L}_1,\ldots,\mathscr{L}_D$可以看成是文章 [37, 引理4.3.5]中构造性证明的加强版本。这些可以通过上面半代数集中点的编码来获得。最后，根据引理2.7 (也可参见 [73])，我们可以从$\mathscr{L}_i$ 得到有理系数线性多项式，它们在$\mathfrak{S}(\mathsf{A})\cap\mathbb{Q}^k$所有点处取值为0。

我们记程序ConstructFormula1，ConstructFormula2 表示输入为A 并且分别返回下面的公式G_1,G_2：

$$||\mathbf{U}||^2>0,\mathbf{U}^\star\mathsf{A}_i\mathbf{U}=0,0\leq i\leq k$$
$$||\mathbf{U}_1||^2>0,||\mathbf{U}_2||^2>0,\sum_{i=1}^{D}\mathbf{U}_i^\star\mathsf{A}_j\mathbf{U}_i^\star=0,0\leq j\leq k$$

这里$\mathbf{U}=[U_1,\ldots,U_D]^\star$是一个由新变元构成的向量，$\mathbf{U_1},\ldots,\mathbf{U}_D$ 是一组由新变元构成的向量（$[U_{i,1},\ldots,U_{i,D}]^\star$，$1\leq i\leq D$）。我们现在可以描述算法WeakLMI。

WeakLMI$(\mathsf{A},[X_1,\ldots,X_k])$

1. 令$\mathscr{U}=$Decision(ConstructFormula1(A))。
2. 如果$\mathscr{U}$ 非空，那么
   (a) 令i 表示向量$\mathscr{U}$中非零元素的最小坐标。
   (b) 令P 表示矩阵[Param$(\mathscr{U})$, $(\mathbf{e}_j)_{1\leq j\neq i\leq D}$] 并且$\mathsf{A}'=\mathsf{P}^\star\mathsf{A}\mathsf{P}$。
   (c) 令$\mathscr{L}_1,\ldots,\mathscr{L}_D$表示向量$\mathsf{A}'\mathbf{e}_1$中的元素，令$\widehat{\mathsf{A}}$表示删除矩阵$\mathsf{A}'$的第一行和第一列后所得到的$(D-1,D-1)$矩阵。
   (d) 返回$\widehat{\mathsf{A}},L=$(ExtractLinForms$(\mathscr{L}_i,$MinPol$(\mathscr{U})),1\leq i\leq D)$。
3. 令$\mathscr{V}=(\mathfrak{V},\Theta)=$Decision(ConstructFormula2(A))。

4. 令$\mathscr{U} = \mathsf{ExtractFirstEntry}(\mathscr{V}, D)$。

   (a) 令i表示向量$\mathscr{U}$中非零元素的最小坐标。

   (b) 令P 表示矩阵$[\mathsf{Param}(\mathscr{U}), (\mathbf{e}_j)_{1\le j\ne i\le D}]$ 并且$\mathsf{A}' = \mathsf{P}^\star\mathsf{A}\mathsf{P}$。

   (c) 令$\mathscr{L}_1, \ldots, \mathscr{L}_D$表示向量$\mathsf{A}'\mathbf{e}_1$中的元素，令$\widehat{\mathsf{A}}$表示删除矩阵$\mathsf{A}'$的第一行和第一列后所得到的$(D-1, D-1)$矩阵。

   (d) 返回$\widehat{\mathsf{A}}, L = (\mathsf{ExtractLinForms}(\mathscr{L}_i, \mathsf{MinPol}(\mathscr{U})), 1 \le i \le D)$。

命题 3.2. 给定线性矩阵不等式

$$\mathsf{A} = \mathsf{A}_0 + X_1\mathsf{A}_1 + \cdots + X_k\mathsf{A}_k \succeq 0$$

其中$X_1, \ldots, X_k$为变元，$\mathsf{A}_0, \ldots, \mathsf{A}_k$为$(D \times D)$有理系数对称矩阵，其中元素二进制表示的位长不超过$\tau$。假设$\mathsf{A} \succeq 0$是弱可行或不可行并且不存在非零向量$\mathbf{u} \in \mathbb{R}^D - \{\mathbf{0}\}$ 使得$\mathsf{A}\mathbf{u} = \mathbf{0}$。

子程序$\mathsf{WeakLMI}(\mathsf{A}, [X_1, \ldots, X_k])$返回$\widehat{\mathsf{A}}, L$，$\widehat{\mathsf{A}}$ 是一个元素在$\mathbb{Q}[X_1, \ldots, X_k]$中的$(D-1, D-1)$对称矩阵，$L$为$\mathbb{Q}[X_1, \ldots, X_k]$ 中的一组有理系数线性多项式，它们在$\mathfrak{S}(\mathsf{A}) \cap \mathbb{Q}^k$的所有点处取值为0，并且$\mathfrak{S}(\widehat{\mathsf{A}}) \cap \mathsf{Sols}(L) \cap \mathbb{Q}^k = \mathfrak{S}(\mathsf{A}) \cap \mathbb{Q}^k$。

运行时间为$\tau^{O(1)}2^{O(D^2)}D^{O(D^2)}$ 位操作，$\widehat{\mathsf{A}}$中系数位长的界为$O(\tau)$，L中系数位长的界为$\tau 2^{O(D^2)}$。

3.3.2 算法正确性证明

我们简单描述 [37, 引理4.3.5]的构造。 [37, 引理4.3.5]证明中的构造基于下面两种情形：

情形1. 假设存在一个非零向量$\mathbf{u} = (u_1, \ldots, u_D)^\star \in \mathbb{R}^D - \{0\}$ 满足$\mathbf{u}^\star\mathsf{A}\mathbf{u} = 0$。第1步计算了这样一个向量。在 [37, 引理4.3.5]的证明中，如果$\mathbf{u} = \mathbf{e}_1$，于是$\mathsf{A}\,\mathbf{e}_1$中的所有非零元素$\mathscr{L}$在$\mathfrak{S}(\mathsf{A})$的所有点处取值为0；更进一步，我们已经假设$\{\mathbf{u} \mid \mathsf{A}\mathbf{u} = \mathbf{0}\} = \{\mathbf{0}\}$，$\mathscr{L}$中必然存在非零元素。

记i为满足$u_i \ne 0$的最小指标。这里，为了得到像$\mathbf{u} = \mathbf{e}_1$这样的简单情形，第2步用$\mathsf{A}' = \mathsf{P}^\star\mathsf{A}\mathsf{P}$来替换$\mathsf{A}$，这里$\mathsf{P}$为$(D \times D)$矩阵，它的第一列为$\mathbf{u}$并且其它列为向量$\mathbf{e}_j$（$j \in \{1, \ldots, D\} - \{i\}$）（参见第2b步）。注意到$\mathsf{P}$为不可逆矩阵，考虑第2b步的矩阵$\mathsf{A}'$；引理2.3 推出$\mathfrak{S}(\mathsf{A}') = \mathfrak{S}(\mathsf{A})$。更进一步，根据 [37, 引理4.3.5]的证明，$\mathsf{A}'\mathbf{e}_1$ 的所有元素（第2c步）在$\mathfrak{S}(\mathsf{A}')$的所有点处取值为0。

令L 表示第2d步得到的线性多项式，并且$\mathsf{Sols}(L) \subset \mathbb{R}^k$为它们的公共解构成的仿射线性子空间。引理2.7 推出

$$\mathfrak{S}(\mathsf{A}') \cap \mathbb{Q}^k = \mathfrak{S}(\mathsf{A}') \cap \mathsf{Sols}(L) \cap \mathbb{Q}^k。$$

更进一步，根据L的构造，矩阵A'的第一行和第一列在$\mathsf{Sols}(L)$的所有点处取值为$\mathbf{0}$。引理2.2 推出$\mathfrak{S}(\widehat{\mathsf{A}}) \cap \mathsf{Sols}(L) = \mathfrak{S}(\mathsf{A}') \cap \mathsf{Sols}(L)$；另外，$\mathfrak{S}(\mathsf{A}') = \mathfrak{S}(\mathsf{A})$，我们推出$\mathfrak{S}(\widehat{\mathsf{A}}) \cap \mathsf{Sols}(L) \cap \mathbb{Q}^k = \mathfrak{S}(\mathsf{A}) \cap \mathbb{Q}^k$。

情形2. 我们假设不存在一个非零向量$\mathbf{u} \in \mathbb{R}^D - \{\mathbf{0}\}$满足$\mathbf{u}^\star \mathsf{A} \mathbf{u} = 0$。由 [37]，存在一组向量$\mathbf{u}_1, \ldots, \mathbf{u}_D$ in $\mathbb{R}^D$ 满足$\sum_{i=1}^D \mathbf{u}_i^\star \mathsf{A} \mathbf{u}_i = 0$，并且$\mathbf{u}_1 \neq \mathbf{0}, \mathbf{u}_2 \neq \mathbf{0}$。第3步，通过计算$\mathscr{V}$来求解向量$\mathbf{u}_1, \ldots, \mathbf{u}_D$。第4步，从$\mathscr{V}$提取向量$\mathbf{u}_1 \in \mathbb{R}^D - \{\mathbf{0}\}$的编码$\mathscr{U}$；注意到$\mathbf{u}_1^\star \mathsf{A} \mathbf{u}_1 \neq 0$。在 [37, 引理4.3.5]的证明中，当$\mathbf{u}_1 = \mathbf{e}_1$时，矩阵$\mathsf{A}$的第一行和第一列在$\mathfrak{S}(\mathsf{A})$的所有点处取值为0。

我们用矩阵A'替代矩阵A来恢复这一情形，（第4b步）：这里我们有$\mathbf{e}_1^\star \mathsf{A}' \mathbf{e}_1 \neq 0$；根据引理2.3, $\mathfrak{S}(\mathsf{A}') = \mathfrak{S}(\mathsf{A})$。对应于 [37, 引理4.3.5]（情形2）证明中的构造，第4c步也给出了线性多项式$\mathscr{L}_1, \ldots, \mathscr{L}_D$的构造，它们在$\mathfrak{S}(\mathsf{A}') = \mathfrak{S}(\mathsf{A})$的所有点处取值为0。

现在，考虑到

- $\widehat{\mathsf{A}}$为第4c步定义的矩阵；
- L为第4d步得到的线性多项式，并且$\mathsf{Sols}(L) \subset \mathbb{R}^k$表示它们的公共解构成的仿射线性子空间。

和情形1一样，根据L的构造，矩阵A'的第一行和第一列在$\mathsf{Sols}(L)$的所有点处取值为$\mathbf{0}$。于是，和情形1 一样，根据引理2.2和引理2.7，我们推出

$$\mathfrak{S}(\widehat{\mathsf{A}}) \cap \mathsf{Sols}(L) = \mathfrak{S}(\mathsf{A}') \cap \mathsf{Sols}(L)。$$

由于$\mathfrak{S}(\mathsf{A}') = \mathfrak{S}(\mathsf{A})$，我们有$\mathfrak{S}(\widehat{\mathsf{A}}) \cap \mathsf{Sols}(L) \cap \mathbb{Q}^k = \mathfrak{S}(\mathsf{A}) \cap \mathbb{Q}^k$。 □

3.3.3　算法复杂度分析

命题2.6推出第1步需要$\tau^{O(1)} k^{O(D)} 2^{O(D)}$位操作。更进一步，如果$\mathscr{U}$不是空集，它用一个系数位长小于等于$\tau 2^{O(D)}$且次数小于等于$O(2^D)$的零维参数化给出$G_1$中点的编码。

假设$\mathscr{U}$非空。在这种参数化下，第2a步只需要单变元多项式的最大公因子操作；运行时间为$\tau k^D 2^D$的多项式时间。第2b-2c步没有增加额外时间消耗。最后，第2d步的位操作可以忽略，返回线性多项式的位长小于等于$\tau 2^{O(D)}$ (引理2.7)。

假设$\mathscr{U}$为空集。于是，命题2.6推出第3步需要$\tau^{O(1)} D^{O(D^2)} 2^{O(D^2)}$位操作；在非空情形，输出的零维参数化次数小于等于$O(2^{D^2})$且系数位长的界为$\tau 2^{O(D^2)}$。第4步运行消耗可忽略并且如前段所述，第4a-4d步不增加额外消耗，根据引理2.7，第4d步输出线性多项式系数位长的界为$\tau 2^{O(D^2)}$。

矩阵$\widehat{\mathsf{A}}$（第2c和4c步）的元素系数位长的估计可以直接得到。 □

3.4 算法RationalLMI

3.4.1 算法描述

给定线性矩阵不等式:

$$\mathsf{A} = \mathsf{A}_0 + X_1\mathsf{A}_1 + \cdots + X_k\mathsf{A}_k \succeq 0,$$

它的可行域为$\mathfrak{S}(\mathsf{A})$。其中$X_1, \ldots, X_k$为变元，$\mathsf{A}_0, \ldots, \mathsf{A}_k$为$(D \times D)$有理系数对称矩阵，其中元素二进制表示的位长不超过$\tau$。我们现在描述本章中的主算法RationalLMI。它的输入为$\mathsf{A}, [X_1, \ldots, X_k]$，如果$\mathsf{A} \succeq 0$存在有理数解，返回$(X_1 - \mathbf{x}_1, \ldots, X_k - \mathbf{x}_k)$来代表$\mathbf{x} = (\mathbf{x}_1, \ldots, \mathbf{x}_k) \in \mathfrak{S}(\mathsf{A}) \cap \mathbb{Q}^k$；其他情况返回$\emptyset$。

在算法的开始，我们考虑下面的半代数集：

$$G = \{\mathbf{u} \in \mathbb{R}^D - \{\mathbf{0}\} \mid \mathsf{A}\mathbf{u} = \mathbf{0}\}.$$

我们记程序ConstructFormula输入为A，并且返回定义G的公式。

我们同时也要用到其他一些子程序：

- LinearSolve: 它的输入为一组有理系数线性多项式，如果这些多项式公共解集非空，输出为一个有理点，否则输出空集。
- GaussianElimination: 输入为$\mathbb{Q}[X_1, \ldots, X_k]$中的一组有理系数线性多项式，对这些多项式进行高斯消去，返回$\mathcal{X}, \mathcal{H}, \mathcal{V}$，其中$\mathcal{X}$是一系列变元$X_{i_1}, \ldots, X_{i_\ell}$，$\mathcal{V}$ 是另外一组变元$\{X_1, \ldots, X_k\} - \{X_{i_1}, \ldots, X_{i_\ell}\}$并且$\mathcal{H}$是$\mathbb{Q}[\mathcal{V}]$ 中的一组线性多项式$h_{i_1}, \ldots, h_{i_\ell}$，并且满足关系$X_{i_r} = h_{i_r}(\mathcal{V})$。

- Substitute: 输入为一组变元$[X_1,\ldots,X_r]$，一组线性多项式$[h_1,\ldots,h_r]$和一个线性矩阵A（元素为变元$X_1,\ldots,X_k$的线性组合），在矩阵A中用h_i来替换X_i （$1\le i\le r$）。
- Evaluate: 输入为一组变元$\mathcal{X}=[X_1,\ldots,X_r]$，一组$\mathbb{Q}[Y_1,\ldots,Y_p]$中的线性多项式$\mathcal{H}=[h_1,\ldots,h_r]$ 和一组有理数$q=(q_1,\ldots,q_p)$；返回序列$(X_i-h_i(q),\ 1\le i\le r)$。

RationalLMI$(\mathsf{A},[X_1,\ldots,X_k])$

1. $\mathscr{U}=$ BasicCasesLMI$(\mathsf{A},[X_1,\ldots,X_k])$。
2. 如果$\mathscr{U}\neq$ false非空，记$(x_1,\ldots,x_k)$为$\mathscr{U}$中的点，返回$X_1-x_1,\ldots,X_k-x_k$。
3. 令$\mathscr{U}=$ LinearSolve(ConstructFormula(A))。
4. 如果$\mathscr{U}$非空，那么
   (a) 计算有理系数可逆矩阵P 满足$\mathsf{P}\mathbf{e_1}=\mathbf{u}$，令$\mathsf{A}'=\mathsf{P}^\star\mathsf{A}\mathsf{P}$，$\widehat{\mathsf{A}}$表示删除矩阵$\mathsf{A}'$的第一行和第一列后所得到的$(D-1,D-1)$ 矩阵。
   (b) 返回RationalLMI$(\widehat{\mathsf{A}},[X_1,\ldots,X_k])$。
5. $\widehat{\mathsf{A}},L=$ WeakLMI$(\mathsf{A},[X_1,\ldots,X_k])$。
6. 如果LinearSolve(L)为空，返回$\emptyset$。
7. $\mathcal{X},\mathcal{H},\mathcal{V}=$ GaussianElimination(L)。
8. $\widetilde{\mathsf{A}}=$ Substitute$(\mathcal{X},\mathcal{H},\widehat{\mathsf{A}})$，并且$R=$ RationalLMI$(\widetilde{\mathsf{A}},\mathcal{V})$。
9. 如果R非空，于是返回$R,$Evaluate$(\mathcal{X},\mathcal{H},R)$ ，否则返回$\emptyset$。

定理 3.3. *给定线性矩阵不等式:*

$$\mathsf{A}=\mathsf{A}_0+X_1\mathsf{A}_1+\cdots+X_k\mathsf{A}_k\succeq 0,$$

*其中$X_1,\ldots,X_k$为变元，$\mathsf{A}_0,\ldots,\mathsf{A}_k$为$(D\times D)$有理系数对称矩阵，其中元素二进制表示的位长不超过$\tau$。算法*RationalLMI$(\mathsf{A},[X_1,\ldots,X_k])$*返回$\mathfrak{S}(\mathsf{A})\cap\mathbb{Q}^k$中的点当且仅当$\mathfrak{S}(\mathsf{A})\cap\mathbb{Q}^k\neq\emptyset$，否则返回空集。运行时间为*

$$(k\tau)^{O(1)}2^{O(\min(k,D)D^2)}D^{O(D^2)}$$

位操作，并且在非空情形，输出结果位长的界为$\tau^{O(1)}2^{O(\min(k,D)D^2)}$。

3.4.2 算法正确性证明

假设$k=1$或$\mathfrak{S}(\mathsf{A})$满维（若$D=1$并且$k\geq 1$，$\mathfrak{S}(\mathsf{A})$满维）。于是，正确性从命题3.1得证。下面通过对D归纳来进行证明：我们的归纳假设是对于$D-1$阶$\mathbb{Q}[X_1,\ldots,X_p]$上的有理系数线性对称矩阵$\mathsf{B}$，RationalLMI($\mathsf{B},[X_1,\ldots,X_p]$)输出$\mathfrak{S}(\mathsf{B})\cap\mathbb{Q}^p$上的有理点当且仅当$\mathfrak{S}(\mathsf{B})\cap\mathbb{Q}^p$非空。

假设存在向量$\mathbf{u}\in\mathbb{R}^D-\{0\}$满足$\mathsf{A}.\mathbf{u}=\mathbf{0}$，于是第3步计算这样一个向量。引理2.3 确保$\mathfrak{S}(\mathsf{A}')$（对称矩阵$\mathsf{A}'$由第4a步得到）和$\mathfrak{S}(\mathsf{A})$相等。更进一步，通过构造，我们有$\mathsf{A}'\mathbf{e}_1=\mathbf{0}$；于是矩阵$\mathsf{A}'$的第一行和第一列为$\mathbf{0}$。于是，通过引理2.2和2.3，我们推断$\mathfrak{S}(\widehat{\mathsf{A}})=\mathfrak{S}(\mathsf{A}')=\mathfrak{S}(\mathsf{A})$。通过对矩阵$\widehat{\mathsf{A}}$的归纳假设，我们推断，如果$\mathfrak{S}(\mathsf{A})\cap\mathbb{Q}^k\neq\emptyset$，第4b步的RationalLMI命令将输出$\mathfrak{S}(\mathsf{A})$上的有理点，否则返回$\emptyset$。

现在假设没有非零向量$\mathbf{u}\in\mathbb{R}^D-\{0\}$满足$\mathsf{A}.\mathbf{u}=\mathbf{0}$；我们进入第5步。由命题3.2推出：

- $\widehat{\mathsf{A}}$是元素在$\mathbb{Q}[X_1,\ldots,X_k]$上的$(D-1,D-1)$对称矩阵；
- 所有的线性多项式L在$\mathfrak{S}(\mathsf{A})\cap\mathbb{Q}^k$的所有点处取值为0，它们中至少有一个非零；我们记$\mathsf{Sols}(L)\subset\mathbb{R}^k$表示$L$的公共解集；
- $\widehat{\mathsf{A}},L$满足$\mathfrak{S}(\widehat{\mathsf{A}})\cap\mathsf{Sols}(L)\cap\mathbb{Q}^k=\mathfrak{S}(\mathsf{A})\cap\mathbb{Q}^k$。

如果$L=0$无解，于是$\mathfrak{S}(\mathsf{A})\cap\mathbb{Q}^k$为空集（第6步）。在第（7-8）步，线性多项式$L$被用来消去$\widehat{\mathsf{A}}$中的若干变元；这将得到$(D-1,D-1)$线性对称矩阵$\widetilde{\mathsf{A}}$（第8步）。将归纳假设应用到矩阵$\widetilde{\mathsf{A}}$，我们推断，通过在第8步调用RationalLMI命令，若$\mathfrak{S}(\widehat{\mathsf{A}})\cap\mathsf{Sols}(L)\cap\mathbb{Q}^k$非空，将返回该集合中的一个点的若干分量，否则返回$\emptyset$。我们之前已经证明$\mathfrak{S}(\widehat{\mathsf{A}})\cap\mathsf{Sols}(L)\cap\mathbb{Q}^k=\mathfrak{S}(\mathsf{A})\cap\mathbb{Q}^k$。如果$R$非空，第9步Evaluate$(\mathcal{X},\mathcal{H},R)$命令将返回$\mathfrak{S}(\mathsf{A})\cap\mathbb{Q}^k$中的一个有理点，否则返回$\emptyset$，定理得证。□

3.4.3 算法复杂度分析

令$\mathcal{A}$表示阶数为D元素在$\mathbb{Q}[X_1,\ldots,X_k]$中，系数位长界为$\tau$的对称矩阵$\mathsf{A}$的集合。我们记$\mathsf{C}(\tau,D,k)$表示算法RationalLMI对所有可能的输入$\mathsf{A}\in\mathcal{A}$和$[X_1,\ldots,$

X_k]运行时间的上界；我们同时记$\mathsf{T}(\tau, D, k)$表示算法RationalLMI对所有可能的输入$\mathsf{A} \in \mathcal{A}$输出坐标位长的上界。

由命题3.1 和3.2，存在足够大的常数A和B，与τ, D, k独立，满足

(A) 第1步运行时间在$A\tau^B D^{Bk}$位操作以内，并且如果$\mathscr{U}$非空，输出点（第2步）坐标位长的界为$\tau^B D^{Bk}$；

(B) 第3步（包括求解$k+1$个$D \times D$ 规模系数位长小于等于τ)的系统，运行时间在$A\tau^B D^B$位操作以内，并且$\mathscr{U}$系数位长的界为τD^B；

(C) 第（4a-4b）步，也包括线性代数操作，构造矩阵P 时间为$A\tau^B D^B$位操作，矩阵P中元素位长的界为τD^B;

(D) 第5步需要至多$\tau^B 2^{BD^2} D^{BD^2}$ 位操作并且L中系数位长的界为$\tau 2^{BD^2}$，应用线性代数中的基本复杂度结果，$\widetilde{\mathsf{A}}$ （在第8步）中元素系数位长的界为$\tau 2^{BD^2}$。

我们令$m_{k,D} = \min(k, D)$并且下面通过对D和k归纳证明

$$\begin{aligned} \mathsf{C}(\tau, D, k) &\leq Ak\tau^B 2^{B^2 m_{k,D} D^2} D^{B^2 D^2} \\ \mathsf{T}(\tau, D, k) &\leq A\tau^B 2^{B^2 m_{k,D} D^2}. \end{aligned}$$

更精确地，我们将假设对$D' < D$并且$k' \leq k$

$$\begin{aligned} \mathsf{C}(\tau, D', k') &\leq Ak'\tau^B 2^{B^2 m_{k',D'} D'^2} D^{B^2 D'^2} \\ \mathsf{T}(\tau, D', k') &\leq A\tau^B 2^{B^2 m_{k',D'} D'^2} \end{aligned}$$

对$D' \leq D$并且$k' < k$

$$\begin{aligned} \mathsf{C}(\tau, D', k') &\leq Ak'\tau^B 2^{B^2 m_{k',D'} D'^2} D^{B^2 D'^2} \\ \mathsf{T}(\tau, D', k') &\leq A\tau^B 2^{B^2 m_{k',D'} D'^2} \end{aligned}$$

在第1-2步应用命题3.1，对$k = 1$和$D = 1$，这个归纳可以很容易初始化。

我们下面考虑一般的情形。通过观察**(A)**, **(B)**, **(C)** 和**(D)**，最坏情形的复杂度为如果$\mathscr{U}$（在第1步计算）为false并且算法执行到第5步。第3步的复杂度和第1步相比可以忽略。在$\mathscr{U}$非空时，第4b步需要

$$\begin{aligned}
\mathsf{C}(\tau,D,k) &\leq A\tau^B D^B + \mathsf{C}(\tau D^B, D-1, k)\\
&\leq A\tau^B D^B +\\
&\quad Ak\tau^B D^{B^2} 2^{B^2 m_{k,D-1}(D-1)^2} D^{B^2(D-1)^2}\\
&\leq Ak\tau^B 2^{B^2 m_{k,D} D^2} D^{B^2 D^2} \text{ 由归纳}\\
\mathsf{T}(\tau,D,k) &\leq \mathsf{T}(\tau D^B, D-1, k)\\
&\leq A\tau^B (D-1)^{B^2} 2^{B^2 m_{k,D-1}(D-1)^2} \text{ （由归纳）}\\
&\leq A\tau^B 2^{B^2 m_{k,D} D^2}
\end{aligned}$$

现在，我们要验证最坏的情形，算法RationalLMI执行到第5步。通过对**(D)**的观察，我们得到

$$\begin{aligned}
\mathsf{C}(\tau,D,k) &\leq A\tau^B D^{BD^2} + \mathsf{C}(\tau 2^{BD^2}, D-1, k-1)\\
&\leq A\tau^B D^{BD^2} +\\
&\quad A(k-1)\tau^B 2^{B^2(D^2+m_{k-1,D-1}(D-1)^2)} D^{B^2(D-1)^2}\\
&\leq Ak\tau^B 2^{B^2 m_{k,D} D^2} D^{B^2 D^2} \text{ 由归纳}\\
\mathsf{T}(\tau,D,k) &\leq \mathsf{T}(\tau 2^{BD^2}, D-1, k-1)\\
&\leq A\tau^B 2^{B^2 D^2} 2^{B^2 m_{k-1,D-1}(D-1)^2} \text{ 由归纳}\\
&\leq A\tau^B 2^{B^2 m_{k,D} D^2}
\end{aligned}$$

最后$\mathsf{C}(\tau,D,k)$ 在$(k\tau)^{O(1)} 2^{O(m_{k,D}D^2)} D^{O(D^2)}$中；$\mathsf{T}(\tau,D,k)$ 在$\tau^{O(1)} 2^{O(m_{k,D}D^2)}$中。
□

3.5　例子

例 3.1. [41] 假设$\mathsf{A} = \mathsf{A}_0 + X_1\mathsf{A}_1$，其中

$$\mathsf{A}_0 = \begin{bmatrix} 0 & 2 & 0 & 0 \\ 2 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \mathsf{A}_1 = \begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}。$$

矩阵A的特征多项式为

$$\begin{aligned} \chi(y) = {} & y^4 + (-3 - 3\,X_1)\,y^3 + ({X_1}^2 - 2 + 9\,X_1)\,y^2 \\ & + (-6\,{X_1}^2 + 3\,{X_1}^3 - 6\,X_1 + 12)\,y \\ & + 8\,{X_1}^2 - 2\,{X_1}^4 - 8。 \end{aligned}$$

令$m_3, \ldots, m_0$为$\chi(y)$中$y^3, y^2, y, 1$的系数，它们定义了半代数集Φ和Ψ。

在RationalLMI的第一步，运行BasicCasesLMI$(\mathsf{A}, [X_1])$。

- 通过因式分解，我们发现m_3的有理系数线性因子$X_1 + 1$，和m_1 的有理系数线性因子$X_1 - 2$，但是$X_1 = -1$和$X_1 = 2$都不满足Φ，这是因为$m_2(-1) = -10 < 0$和$m_0(2) = -8 < 0$。由于$k = 1$，集合$\mathscr{U}$为空集，返回空集。

$\mathfrak{S}(\mathsf{A})$没有有理数解。

例 3.2. 假设$\mathsf{A} = \mathsf{A}_0 + X_1\mathsf{A}_1$，其中

$$\mathsf{A}_0 = \begin{bmatrix} 0 & 2 & 0 & 0 \\ 2 & 0 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \mathsf{A}_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}。$$

矩阵A的特征多项式为

$$\begin{aligned} \chi(y) = {} & y^4 + (-5 - 2\,X_1)\,y^3 + 10\,X_1\,y^2 \\ & + (-5\,{X_1}^2 + 2\,{X_1}^3 - 8\,X_1 + 20)\,y \\ & + 8\,{X_1}^2 - {X_1}^4 - 16。 \end{aligned}$$

令$m_3,\ldots,m_0$为$\chi(y)$中$y^3,y^2,y,1$的系数，它们定义了半代数集Φ和Ψ。

和第一个例子一样，我们有

1. 在RationalLMI的第一步，运行BasicCasesLMI$(\mathsf{A},[X_1])$。

   - 通过因式分解，我们发现有理数线性因子$X_1+\frac{5}{2}$, X_1, $X_1+\frac{5}{2}$, X_1-2, X_1+2，但是只有解$X_1=2$满足Φ，因为$m_3(2)=-9<0, m_2(2)=20>0$, $m_1(2)=m_0(2)=0$, 返回$\{2\}$。

2. 在RationalLMI的第二步，$\mathscr{U}=\{2\}$，返回X_1-2。

我们找到了一个有理数解$X_1=2$。实际上，这是$\mathfrak{S}(\mathsf{A})$的唯一解。

第四章　多项式有理系数平方和计算

4.1　前言

我们在前面提到Sturmfels曾提出过一个问题：如果一个有理系数多项式存在实系数多项式平方和表示形式，其是否存在有理系数多项式平方和表示？在引言中我们介绍了该问题的一些后续研究工作。给定一个$2d$次有理系数多项式$f \in \mathbb{Q}[Y_1, \ldots, Y_n]$，判定多项式$f$是否存在有理系数平方和分解等价于判定$f$的Gram矩阵$\mathsf{M}$定义的线性矩阵不等式$\mathsf{M} \succeq 0$的可行域$\mathfrak{S}(\mathsf{M})$是否包含有理数解。

2010年，Safey El Din与支丽红 [73]给出了一般凸半代数集上有理点的存在性判定和计算方法，该算法可以用来判定一个有理系数多项式是否存在有理系数多项式平方和分解，给定一个$2d$次有理系数多项式$f \in \mathbb{Q}[Y_1, \ldots, Y_n]$，其系数位长不超过$\tau$，用$\mathsf{M}(d, n)$来表示$\min(n^d, d^n)$，该算法判定一个有理系数多项式是否存在有理系数多项式平方和分解的算法复杂度为$\tau^{O(1)}\mathsf{M}(d, n)^{\mathsf{M}(d,n)^6}$。

将上一章中定理3.3 应用到多项式f的Gram矩阵定义的线性矩阵不等式可得到如下结论。

定理 4.1. *多项式$f \in \mathbb{Q}[X_1, \ldots, X_n]$ 次数为$2d$，系数位长不超过τ。我们的算法可判定f 是否存在有理系数多项式平方和分解，并在分解存在时给出相应表示形式，算法复杂度为$\tau^{O(1)}2^{O(\mathsf{M}(d,n)^3)}$，其中$\mathsf{M}(d, n) = \min(d^n, n^d)$。输出表示形式中系数位长的界为$\tau^{O(1)}2^{O(\mathsf{M}(d,n)^3)}$。*

我们的算法显著改进了Safey El Din与支丽红算法的复杂度，这也是目前多项式有理系数平方和判定和计算的复杂度最好算法。

在本章中，我们利用算法RationalLMI对一些多项式的Gram矩阵定义的线性矩阵不等式的可行域是否包含有理数解进行判定，在有理数解存在时，给出有理数解并将相应的Gram矩阵进行LU分解，从而得到该多项式的有理系数平方和表示。

2012年，Scheiderer给出了Sturmfels问题的第一个反例 [74]

$$f = x^4 + x\,y^3 + y^4 - 3\,x^2\,y\,z - 4\,x\,y^2\,z + 2\,x^2\,z^2 + x\,z^3 + y\,z^3 + z^4。$$

我们的算法判定Scheiderer反例的Gram矩阵定义的线性矩阵不等式的可行域没有有理数解，从而给出了该反例不存在有理系数平方和分解的第一个计算机验证。该反例的Gram矩阵定义的线性矩阵不等式非常小：只有6 个变元，矩阵大小为6×6。我们的实现应用了RAGLIB 软件包 [69]，该软件包依赖于 [17,70]等文献中的算法。

4.2 一些简单例子的计算机实现

例 4.1. 考虑文章 [51, 例3]中的多项式

$$f(x,y,z,w)=2\,x^4+x^2\,y^2+y^4-4\,x^2\,z-$$
$$4\,x\,y\,z-2\,y^2\,w+y^2-2\,y\,z+8\,z^2-2\,z\,w+2\,w^2。$$

通过我们的算法RationalLMI，我们证实该多项式的Gram矩阵存在有理数解并给出了该多项式的有理系数平方和表示。

假设$f=[x^2,xy,y^2,y,z,w]\,\mathsf{A}\,[x^2,xy,y^2,y,z,w]^\star$，多项式$f$的Gram矩阵$\mathsf{A}$是一个$6\times 6$对称矩阵

$$\mathsf{A}=\begin{bmatrix} 2 & 0 & X_1 & 0 & -2 & 0\\ 0 & 1-2\,X_1 & 0 & 0 & -2 & 0\\ X_1 & 0 & 1 & 0 & 0 & -1\\ 0 & 0 & 0 & 1 & -1 & 0\\ -2 & -2 & 0 & -1 & 8 & -1\\ 0 & 0 & -1 & 0 & -1 & 2 \end{bmatrix}$$

这里有一个变元X_1，对应两个对称矩阵$\mathsf{A}_0,\mathsf{A}_1$。

矩阵A的特征多项式为

$$\begin{aligned}\chi(y)=\;& y^6+(-15+2\,X_1)\,y^5+(64-28\,X_1-{X_1}^2)\,y^4\\ &+(-110+108\,X_1+12\,{X_1}^2-2\,{X_1}^3)\,y^3\\ &+(78-156\,X_1-31\,{X_1}^2+22\,{X_1}^3)\,y^2\\ &+(84\,X_1+33\,{X_1}^2-18-48\,{X_1}^3)\,y\\ &-12\,X_1-13\,{X_1}^2+26\,{X_1}^3。\end{aligned}$$

令$m_5,\ldots,m_0$表示$\chi(y)$中$y^5,\ldots,1$的系数，它们定义了半代数集Φ 和Ψ。

- 在算法RationalLMI中的第一步，运行BasicCasesLMI(A, $[X_1]$)。
  - 通过因式分解，我们发现m_5的有理系数线性因子$X_1 - \frac{15}{2}$和m_0的有理系数线性因子X_1，但是只有解$X_1 = 0$满足Φ，因为：

$$m_5(0) = -15 < 0, m_4(0) = 64 > 0,$$
$$m_3(0) = -110 < 0, m_2(0) = 78 > 0, m_1(0) = -18$$

    返回$\{0\}$。

- 在算法RationalLMI的第二步，$\mathscr{U} = \{0\}$，返回X_1。

将$X_1 = 0$代入，我们可以得到f的有理系数Gram矩阵M_1。

$$\mathsf{M}_1 = \begin{bmatrix} 2 & 0 & 0 & 0 & -2 & 0 \\ 0 & 1 & 0 & 0 & -2 & 0 \\ 0 & 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 & -1 & 0 \\ -2 & -2 & 0 & -1 & 8 & -1 \\ 0 & 0 & -1 & 0 & -1 & 2 \end{bmatrix}。$$

对M_1 应用LU分解，我们得到f的如下有理系数平方和分解，

$$f = 2\,(x^2 - z)^2 + (x\,y - 2\,z)^2 + (y^2 - w)^2 + (y - z)^2 + (z - w)^2。$$

例 4.2. 我们考虑下面的多项式 [23]

$$f = x^6 - 12\,x^5 + 74\,x^4 - 272\,x^3 + 611\,x^2 - 780\,x + 442。$$

假设$f = [x^3, x^2, x, 1]\,\mathsf{A}\,[x^3, x^2, x, 1]^\star$，多项式$f$的Gram矩阵A是一个$4 \times 4$对称矩阵

$$\mathsf{A} = \begin{bmatrix} 1 & -6 & X_1 & -136 - X_2 \\ -6 & -2\,X_1 + 74 & X_2 & X_3 \\ X_1 & X_2 & -2\,X_3 + 611 & -390 \\ -136 - X_2 & X_3 & -390 & 442 \end{bmatrix}。$$

在算法RationalLMI的第一步，运行BasicCasesLMI(A, $[X_1, X_2, X_3]$)。我们发现了A $\succeq 0$的一些特解，

$$[X_1 = 4, X_2 = -144, X_3 = 52], [X_1 = 11, X_2 = -133, X_3 = 80],$$
$$[X_1 = 14, X_2 = -127, X_3 = 95], [X_1 = 17, X_2 = -119, X_3 = 114]。$$

将第一个特解代入A，我们得到f的有理系数Gram矩阵M_1。

$$\mathsf{M}_1 = \begin{bmatrix} 1 & -6 & 4 & 8 \\ -6 & 66 & -144 & 52 \\ 4 & -144 & 507 & -390 \\ 8 & 52 & -390 & 442 \end{bmatrix}。$$

对M_1应用LU分解，我们得到f的如下有理系数平方和分解，

$$f = (x^3 - 6\,x^2 + 4\,x + 8)^2 + 30\,(\frac{10}{3} + x^2 - 4\,x)^2 + 11\,(-2 + x)^2 + \frac{2}{3}。$$

将其他几个特解代入A，我们可以得到f的有理系数Gram矩阵$\mathsf{M}_2, \mathsf{M}_3, \mathsf{M}_4$。对$\mathsf{M}_2, \mathsf{M}_3, \mathsf{M}_4$应用LU分解，我们得到$f$的如下有理系数平方和分解形式，

$$f = (x^3 - 6\,x^2 + 11\,x - 3)^2 + 16\,(\frac{31}{8} + x^2 - \frac{67}{16}\,x)^2 + \frac{791\,(-\frac{1558}{791} + x)^2}{16} + \frac{755}{791}。$$

$$f = (x^3 - 6\,x^2 + 14\,x - 9)^2 + 10\,(\frac{41}{10} + x^2 - \frac{43}{10}\,x)^2 + \frac{401\,(-\frac{877}{401} + x)^2}{10} + \frac{440}{401}。$$

$$f = (x^3 - 6\,x^2 + 17\,x - 17)^2 + 4\,(3 + x^2 - \frac{17}{4}\,x)^2 + \frac{87\,(-\frac{200}{87} + x)^2}{4} + \frac{179}{87}。$$

例 4.3. 我们考虑下面的多项式 [16]

$$\begin{aligned} f =& 412\,x^4 - 18\,x^3\,y + 556\,x^2\,y^2 + 40\,x\,y^3 + 533\,y^4 - 24\,x^3 - 344\,x^2\,y + 184\,x\,y^2 \\ & -200\,y^3 + 540\,x^2 + 134\,x\,y + 678\,y^2 - 182\,x - 92\,y + 444。 \end{aligned}$$

假设$f = [x^2, xy, y^2, x, y, 1]\,\mathsf{A}\,[x^2, xy, y^2, x, y, 1]^\star$，多项式$f$的Gram矩阵A是一个$6 \times 6$对称矩阵

$$\mathsf{A}=\begin{bmatrix} 412 & -9 & X_1 & -12 & -X_2-172 & X_3 \\ -9 & 556-2\,X_1 & 20 & X_2 & 92-X_4 & 67-X_5 \\ X_1 & 20 & 533 & X_4 & -100 & X_6 \\ -12 & X_2 & X_4 & 540-2\,X_3 & X_5 & -91 \\ -X_2-172 & 92-X_4 & -100 & X_5 & -2\,X_6+678 & -46 \\ X_3 & 67-X_5 & X_6 & -91 & -46 & 444 \end{bmatrix}。$$

在算法RationalLMI的第一步，运行BasicCasesLMI(A, $[X_1,\cdots,X_6]$)。我们发现了$\mathsf{A}\succeq 0$的一个特解，

$$X_1=0,\,X_2=0,\,X_3=0,\,X_4=0,\,X_5=0,\,X_6=-462。$$

将它代入A，我们得到f的有理系数Gram矩阵M。

$$\mathsf{M}=\begin{bmatrix} 412 & -9 & 0 & -12 & -172 & 0 \\ -9 & 556 & 20 & 0 & 92 & 67 \\ 0 & 20 & 533 & 0 & -100 & -462 \\ -12 & 0 & 0 & 540 & 0 & -91 \\ -172 & 92 & -100 & 0 & 1602 & -46 \\ 0 & 67 & -462 & -91 & -46 & 444 \end{bmatrix}。$$

并对M应用LU分解，我们得到f的如下有理系数平方和分解，

$$\begin{aligned} f =& 412\,(x^2-\frac{9}{412}\,x\,y-\frac{3}{103}\,x-\frac{43}{103}\,y)^2 \\ &+\frac{228991\,(\frac{27604}{228991}+x\,y+\frac{8240}{228991}\,y^2-\frac{108}{228991}\,x+\frac{36356}{228991}\,y)^2}{412} \\ &+\frac{121887403\,(-\frac{106345922}{121887403}+y^2+\frac{2160}{121887403}\,x-\frac{23626220}{121887403}\,y)^2}{228991} \\ &+\frac{65776581108\,(-\frac{11086898965}{65776581108}+x-\frac{50443732\,y}{5481381759})^2}{121887403} \\ &+\frac{2733637045754\,(-\frac{404235922121}{4100455568631}+y)^2}{1827127253}+\frac{14038759963895}{16401822274524}。\end{aligned}$$

4.3 Scheiderer反例的计算机验证

根据 [74, 定理2.2]，多项式

$$f = x^4 + x\,y^3 + y^4 - 3\,x^2\,y\,z - 4\,x\,y^2\,z + 2\,x^2\,z^2 + x\,z^3 + y\,z^3 + z^4$$

可以表示为实系数多项式的平方和，但不能表示为有理系数多项式的平方和。

假设$f = [x^2, xy, y^2, xz, yz, z^2]\,\mathsf{A}\,[x^2, xy, y^2, xz, yz, z^2]^\star$，多项式$f$的Gram矩阵A是一个$6 \times 6$对称矩阵

$$\begin{bmatrix} 1 & 0 & X_1 & 0 & -\frac{3}{2} - X_2 & X_3 \\ 0 & -2\,X_1 & \frac{1}{2} & X_2 & -2 - X_4 & -X_5 \\ X_1 & \frac{1}{2} & 1 & X_4 & 0 & X_6 \\ 0 & X_2 & X_4 & -2\,X_3 + 2 & X_5 & \frac{1}{2} \\ -\frac{3}{2} - X_2 & -2 - X_4 & 0 & X_5 & -2\,X_6 & \frac{1}{2} \\ X_3 & -X_5 & X_6 & \frac{1}{2} & \frac{1}{2} & 1 \end{bmatrix}。$$

这里有6个变元：$X_1, X_2, X_3, X_4, X_5, X_6$ 对应7个对称矩阵$\mathsf{A}_0, \mathsf{A}_1, \mathsf{A}_2, \mathsf{A}_3, \mathsf{A}_4, \mathsf{A}_5, \mathsf{A}_6$。

- 应用软件包RAGLib [69]中的命令HasRealSolutions，计算

$$\mathscr{U} = \mathsf{OpenDecision}(\Psi)。$$

集合$\mathscr{U}$为空集，于是A不是强可行的。

- 在算法RationalLMI的第5步，由WeakLMI$(\mathsf{A}, [X_1, \cdots, X_6])$，

1. 通过命令RationalUnivariateRepresentation [66], 我们得到一个实代数

数解

$$\mathbf{u}=\begin{bmatrix} -1+\frac{1}{2}\,\vartheta+\frac{1}{2}\,\vartheta^4 \\ \frac{\vartheta^3}{2}+\frac{1}{2} \\ \vartheta^2 \\ -2\,\vartheta+\frac{1}{2}\,\vartheta^2+\frac{1}{2}\,\vartheta^5 \\ \vartheta \\ 1 \end{bmatrix},$$

这里ϑ 是一个实代数数且满足

$$\vartheta^6-4\,\vartheta^2-1=0。$$

2. $\mathscr{U}$ 非空，于是

   (a) $i=1$。

   (b) $P=[\mathsf{Param}(\mathscr{U}),e_2,\ldots,e_6]$ 并且$\mathsf{A}'=\mathsf{P}^\star\mathsf{A}\mathsf{P}$。

   (c) $\mathscr{L}_1,\ldots,\mathscr{L}_6$ 为矩阵A'的第一列中的元素

$$\begin{bmatrix} 0 \\ \frac{1}{2}\,X_2\,\vartheta^5-\,X_1\vartheta^3+\cdots-X_1-X_5 \\ \frac{1}{2}\,X_4\,\vartheta^5+\frac{1}{2}\,X_1\,\vartheta^4+\cdots-X_1+X_6+\frac{1}{4} \\ (1-X_3)\,\vartheta^5+\frac{1}{2}\,X_2\,\vartheta^3+\cdots+\frac{1}{2}+\frac{1}{2}\,X_2 \\ \frac{1}{2}\,X_5\,\vartheta^5+\cdots+1+X_2-\frac{1}{2}\,X_4 \\ \frac{1}{4}\vartheta^5+\frac{1}{2}\,X_3\,\vartheta^4+\cdots-X_3+1-\frac{1}{2}\,X_5 \end{bmatrix}。$$

   由于$i=1$，$\widehat{\mathsf{A}}$为矩阵A删除第一行和第一列后得到的5×5矩阵。

   (d) $\mathscr{L}_1,\ldots,\mathscr{L}_6$中$\vartheta^5,\ldots,\vartheta^1,1$的系数记为$L$，返回$\widehat{\mathsf{A}},L$。

- 在算法RationalLMI的第6步，$\mathscr{L}_1,\ldots,\mathscr{L}_6$中$\vartheta^5$的系数向量为

$$L_5=\left[0,\frac{1}{2}\,X_2,\frac{1}{2}\,X_4,1-X_3,\frac{1}{2}\,X_5,\frac{1}{4}\right]^\star。$$

L_5的最后一个元素为$\frac{1}{4}$，线性系统$L_5 = 0$ 无解。因此，LinearSolve(L) 返回空集。

$\mathfrak{S}(\mathsf{A})$没有有理数解。相关Maple程序可以从下面网址下载：http://www.mmrc.iss.ac.cn/~lzhi/Research/hybrid/RaLMI

第五章　线性矩阵不等式精确实数解的计算方法

5.1　前言

有些线性矩阵不等式不存在有理数解，但存在实数解，例如：

$$\mathsf{A}=\begin{bmatrix} 2\,x & 2 & 0 & 0\\ 2 & x & 0 & 0\\ 0 & 0 & 2 & x\\ 0 & 0 & x & 1 \end{bmatrix}$$

线性矩阵不等式$\mathsf{A}\succeq 0$只有一个实数解$x=\sqrt{2}$。Khachiyan和Porkolab给出了半正定规划实数解判定的算法复杂度[54]，但未能给出有效的构造方法。在上一章，我们看到Scheiderer反例的Gram矩阵定义的线性矩阵不等式的可行域没有有理数解，在文章[74]中，Scheiderer给出了该例子的实系数平方和分解，能否将我们的算法RationalLMI扩充一下，来构造线性矩阵不等式可行域上精确的实数解？

本章我们给出了线性矩阵不等式精确实数解的计算方法RealLMI，作为该算法的一个应用，我们给出了Scheiderer反例实系数平方和分解的计算机实现。

考虑线性矩阵不等式

$$\mathsf{A}=\mathsf{A}_0+X_1\mathsf{A}_1+\cdots+X_k\mathsf{A}_k\succeq 0,$$

其中$\mathsf{A}_0,\ldots,\mathsf{A}_k$是有理系数或实代数数系数（$\mathbb{Q}(\vartheta)$）的$(D\times D)$对称矩阵，其中元素二进制表示的位长不超过$\tau$，它的可行域为$\mathfrak{S}(\mathsf{A})$。我们给出了一个算法RealLMI，该算法是第三章中算法RationalLMI的扩充，在线性矩阵有理数解不存在时可以给出实数解的存在性判定和计算。如果给定的线性矩阵不等式是有理系数的，在算法RealLMI中可令多项式$g=0$，则算法RealLMI与算法RationalLMI基本一致；在线性矩阵A中包含实代数数系数时，可令多项式g为实代数数ϑ的极小多项式。算法RealLMI的特别之处在于，在变元个数$k=1$时，子程序BasicRealLMI 考虑的是给定线性矩阵A 的特征多项式$\chi(y)$ 的各项

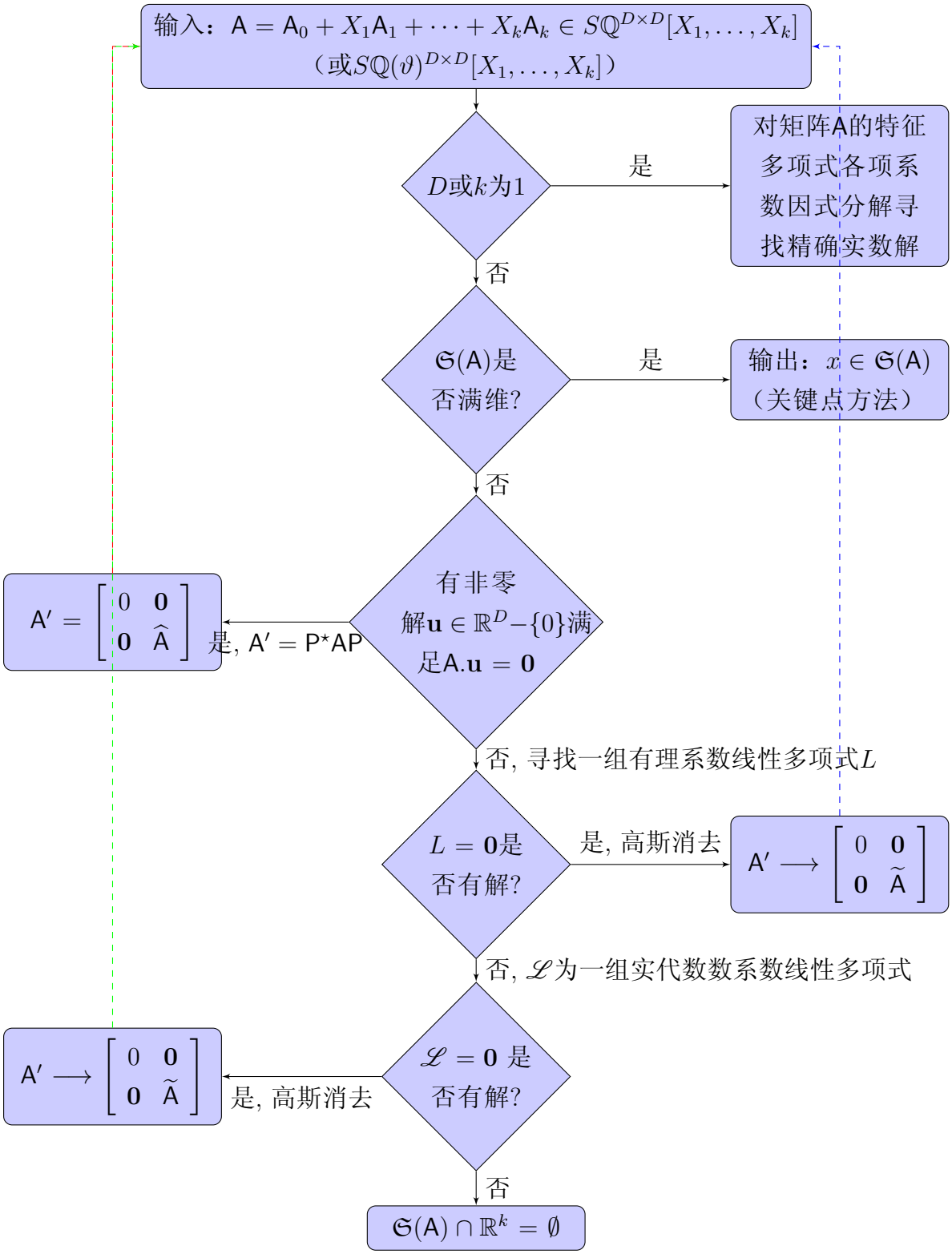

图 5.1: 线性矩阵不等式可行域精确实数解判定和计算流程图

系数的满足公式Φ 的实线性因子的解，且公式Φ和Ψ定义中的多项式增加了。当$\mathfrak{S}(\mathsf{A})$不满维时，子程序WeakRealLMI 返回中增加了$q, \mathscr{L}$，q为计算过程中实代数数ν 的极小多项式，$\mathscr{L}$ 是$\mathbb{Q}[X_1, \ldots, X_k]$ 或$\mathbb{Q}(\nu)[X_1, \ldots, X_k]$ 中的线性多项式，它们在$\mathfrak{S}(\mathsf{A})$的所有点处取值为0。在主算法RealLMI 中，如果有理系数线性多项式$L = 0$无解，则$\mathfrak{S}(\mathsf{A})$无有理数解，此时，我们考虑实系数线性多项式$\mathscr{L} = 0$ 是否有解。若$\mathscr{L} = 0$无解，则$\mathfrak{S}(\mathsf{A})$无实数解。在$L = 0$ 或$\mathscr{L} = 0$有解时利用高斯消去法给出一部分变元$\mathcal{X}$ 用另一部分变元$\mathcal{V}$ 的线性表示形式$\mathcal{H}$，同时得到一个阶数更小的矩阵$\widetilde{\mathsf{A}}$，$\mathfrak{S}(\widetilde{\mathsf{A}})$的实数解（有理数解）是$\mathfrak{S}(\mathsf{A})$ 上实数解（有理数解）的投影。如果$\mathfrak{S}(\widetilde{\mathsf{A}})$上不含实数解（有理数解），则$\mathfrak{S}(\mathsf{A})$上也不含实数解（有理数解），否则我们利用命令Evaluate，可以从$\mathfrak{S}(\widetilde{\mathsf{A}})$的实数解（有理数解）恢复$\mathfrak{S}(\mathsf{A})$上的实数解（有理数解）。

5.2　算法RealLMI

5.2.1　子程序BasicRealLMI

给定线性矩阵不等式$\mathsf{A} = \mathsf{A}_0 + X_1\mathsf{A}_1 + \cdots + X_k\mathsf{A}_k \succeq 0$，它的可行域为$\mathfrak{S}(\mathsf{A})$。其中$\mathsf{A}_0, \ldots, \mathsf{A}_k$ 是有理系数或实代数数系数（$\mathbb{Q}(\vartheta)$）的$(D \times D)$ 对称矩阵，g为实代数数ϑ的极小多项式，当$\mathsf{A}_0, \ldots, \mathsf{A}_k$中元素均为有理系数时，可令$g = 0$。本节我们给出子程序BasicRealLMI，该子程序输入为$\mathsf{A}, [\mathsf{X}_1, \ldots, \mathsf{X}_k], \mathsf{g}$，并且

- 当$k = 1$时，如果$\mathfrak{S}(\mathsf{A}) \neq \emptyset$，返回$\mathfrak{S}(\mathsf{A})$上的至少一个点；否则返回空集。
- 当$k > 1$时，如果$\mathfrak{S}(\mathsf{A})$包含非空内点，返回$\mathfrak{S}(\mathsf{A})$中的至少一个点；否则返回false。

令$\chi(y) = y^D + m_{D-1}y^{D-1} + \cdots + m_0$为矩阵A的特征多项式，我们记$\Phi$为下面的公式：

$$\Phi = \{\, g(\vartheta) = 0,\ (-1)^{(i+D)}m_i \geq 0,\ 0 \leq i \leq D-1\}$$

Ψ为下面的公式：

$$\Psi = \{\, g(\vartheta) = 0,\ (-1)^{(i+D)}m_i > 0,\ 0 \leq i \leq D-1\}.$$

由 [57]，半代数集$\mathfrak{S}(\mathsf{A})$ 由Φ定义；$\mathfrak{S}(\mathsf{A})$ 的内点由Ψ定义。

BasicRealLMI$(\mathsf{A}, [X_1, \ldots, X_k], g)$

1. 集合$\mathscr{U}$初始化为空集，如果$k=1$，存在m_i（$0\le i\le D-1$）的一个线性因子$X-a$，使得$(-1)^{(j+D)}m_j(a)\ge 0$ （$j\ne i$），把a放入集合$\mathscr{U}$中，返回$\mathscr{U}$。

2. $\mathscr{U}=\mathsf{OpenDecision}(\Psi)$。如果$\mathscr{U}$不为空集，返回$\mathscr{U}$，否则返回false。

命题 5.1. *给定线性矩阵不等式:*

$$\mathsf{A}=\mathsf{A}_0+X_1\mathsf{A}_1+\cdots+X_k\mathsf{A}_k\succeq 0$$

其中$X_1,\ldots,X_k$为变元，$\mathsf{A}_0,\ldots,\mathsf{A}_k$为$(D\times D)$有理系数或实代数数系数（$\mathbb{Q}(\vartheta)$）对称矩阵，$g$为实代数数$\vartheta$的极小多项式，当$\mathsf{A}_0,\ldots,\mathsf{A}_k$中元素均为有理系数时，可令$g=0$。

如果$k=1$，并且$\mathfrak{S}(\mathsf{A})\ne\emptyset$，$\mathsf{BasicRealLMI}(\mathsf{A},[X_1],g)$返回$\mathfrak{S}(\mathsf{A})$中的至少一个点，否则返回空集。

如果$\mathfrak{S}(\mathsf{A})\subset\mathbb{R}^k$满维，$\mathsf{BasicRealLMI}(\mathsf{A},[X_1,\ldots,X_k],g)$返回$\mathfrak{S}(\mathsf{A})$中的至少一个点，其他情形返回false。

算法正确性证明 如果$k=1$，此时$\mathfrak{S}(\mathsf{A})\subset\mathbb{R}$（第1步）。由于$\mathfrak{S}(\mathsf{A})$为凸集，它为空集或一个点或一个包含非空内点的区间。假设它是一个点，它是Φ的唯一解，因为$\mathfrak{S}(\mathsf{A})$是由Φ来定义的。通过假设，这个解不是Ψ 的解（否则$\mathfrak{S}(\mathsf{A})$将包含非空内点）。假设$\mathfrak{S}(\mathsf{A})$为一个区间，它的端点必定为某个m_i的解，并且满足公式Φ。因此可以通过寻找满足$(-1)^{j+D}m_j$'s （$j\ne i$）非负的那些m_i（$0\le i\le D-1$）的线性因子的解，来寻找$\mathfrak{S}(\mathsf{A})$的实数解。假设$\mathfrak{S}(\mathsf{A})$不满维。我们可以推出$\mathfrak{S}(\mathsf{A})$为空集，算法结束。

如果$k\ge 2$。假设$\mathfrak{S}(\mathsf{A})$满维；它包含非空内点。于是，根据命题2.6，第2步返回$\mathfrak{S}(\mathsf{A})$中的至少一个点当且仅当$\mathfrak{S}(\mathsf{A})\ne\emptyset$。假设$\mathfrak{S}(\mathsf{A})$不满维。由公式$\Psi$定义的半代数集是$\mathfrak{S}(\mathsf{A})$的内点；我们推断它是空集。于是，根据命题2.6，$\mathscr{U}$为空集，我们返回false。 □

5.2.2 子程序WeakRealLMI

给定线性矩阵不等式$\mathsf{A}=\mathsf{A}_0+X_1\mathsf{A}_1+\cdots+X_k\mathsf{A}_k\succeq 0$，它的可行域为$\mathfrak{S}(\mathsf{A})$。其中$\mathsf{A}_0,\ldots,\mathsf{A}_k$ 是有理系数或实代数数系数（$\mathbb{Q}(\vartheta)$）的$(D\times D)$ 对称矩阵，g为

实代数数ϑ的极小多项式，当$\mathsf{A}_0,\ldots,\mathsf{A}_k$中元素均为有理系数时，可令$g=0$。我们给出子程序WeakRealLMI的描述，它的输入为$\mathsf{A},[X_1,\ldots,X_k],g$，其中$\mathfrak{S}(\mathsf{A})$不满维，并且不存在非零向量$\mathbf{u}\in\mathbb{R}^D-\{\mathbf{0}\}$ 使得$\mathsf{A}\mathbf{u}=\mathbf{0}$。它返回$q,\widehat{\mathsf{A}},\mathscr{L},L$ 使得

- q为实代数数ν的极小多项式；
- $\widehat{\mathsf{A}}$ 是元素在$\mathbb{Q}[X_1,\ldots,X_k]$ 或$\mathbb{Q}(\vartheta)[X_1,\ldots,X_k]$ 中的$(D-1)\times(D-1)$对称线性矩阵；
- $\mathscr{L}$是$\mathbb{Q}[X_1,\ldots,X_k]$ 或$\mathbb{Q}(\nu)[X_1,\ldots,X_k]$ 中的线性多项式，它们在$\mathfrak{S}(\mathsf{A})$ 的所有点处取值为0；令$\mathsf{Sols}(\mathscr{L})\subset\mathbb{R}^k$ 是$\mathscr{L}$ 的公共解构成的线性子空间，

$$\mathfrak{S}(\widehat{\mathsf{A}})\cap\mathsf{Sols}(\mathscr{L})=\mathfrak{S}(\mathsf{A})；$$

- 如果矩阵A的元素中含有$\mathbb{Q}(\vartheta)[X_1,\ldots,X_k]$ 中的线性多项式（此时输入中$g\neq 0$），$L=\emptyset$；否则，L 是$\mathbb{Q}[X_1,\ldots,X_k]$中的有理系数线性多项式，它们在$\mathfrak{S}(\mathsf{A})\cap\mathbb{Q}^k$ 的所有点处取值为0 ；我们令$\mathsf{Sols}(L)\subset\mathbb{R}^k$ 表示L 的公共解构成的线性子空间，

$$\mathfrak{S}(\widehat{\mathsf{A}})\cap\mathsf{Sols}(L)\cap\mathbb{Q}^k=\mathfrak{S}(\mathsf{A})\cap\mathbb{Q}^k。$$

我们记程序ConstructFormula1，ConstructFormula2 表示输入为A 并且分别返回下面的公式G_1,G_2：

$$||\mathbf{U}||^2>0,\mathbf{U}^\star\mathsf{A}_i\mathbf{U}=0,0\leq i\leq k,g(\vartheta)=0$$

$$||\mathbf{U}_1||^2>0,||\mathbf{U}_2||^2>0,\sum_{i=1}^{D}\mathbf{U}_i^\star\mathsf{A}_j\mathbf{U}_i^\star=0,0\leq j\leq k,g(\vartheta)=0$$

这里$\mathbf{U}=[U_1,\ldots,U_D]^\star$是一个由新变元构成的向量，$\mathbf{U_1},\ldots,\mathbf{U}_D$ 是一组由新变元构成的向量（$[U_{i,1},\ldots,U_{i,D}]^\star$，$1\leq i\leq D$）。下面我们给出算法WeakRealLMI的具体描述。

WeakRealLMI$(\mathsf{A},[X_1,\ldots,X_k],g)$

1. 令$\mathscr{U}=\mathsf{Decision}(\mathsf{ConstructFormula1}(\mathsf{A}))$
2. 如果$\mathscr{U}$非空，于是

(a) 令i表示向量$\mathscr{U}$中非零元素的最小坐标，q为向量$\mathscr{U}$中实代数数ν的极小多项式。

(b) 令P 表示矩阵$[\mathsf{Param}(\mathscr{U}), (\mathbf{e}_j)_{1\le j\neq i\le D}]$ 并且$\mathsf{A}' = \mathsf{P}^\star\mathsf{A}\mathsf{P}$

(c) 令$\mathscr{L} = \mathscr{L}_1, \ldots, \mathscr{L}_D$表示向量$\mathsf{A}'\mathbf{e}_1$中的元素，令$\widehat{\mathsf{A}}$表示删除矩阵$\mathsf{A}'$的第一行和第一列后所得到的$(D-1, D-1)$ 矩阵。

(d) 若$g \neq 0$，令$L = \emptyset$。否则，令$L = (\mathsf{ExtractLinForms}(\mathscr{L}_i, \mathsf{MinPol}(\mathscr{U})), 1 \le i \le D)$，返回$q, \widehat{\mathsf{A}}, \mathscr{L}, L$。

3. 令$\mathscr{V} = (\mathfrak{V}, \Theta) = \mathsf{Decision}(\mathsf{ConstructFormula2}(\mathsf{A}))$

4. 令$\mathscr{U} = \mathsf{ExtractFirstEntry}(\mathscr{V}, D)$

(a) 令i表示向量$\mathscr{U}$中非零元素的最小坐标，q为向量$\mathscr{U}$中实代数数ν的极小多项式。

(b) 令P 表示矩阵$[\mathsf{Param}(\mathscr{U}), (\mathbf{e}_j)_{1\le j\neq i\le D}]$ 并且$\mathsf{A}' = \mathsf{P}^\star\mathsf{A}\mathsf{P}$

(c) 令$\mathscr{L} = \mathscr{L}_1, \ldots, \mathscr{L}_D$表示向量$\mathsf{A}'\mathbf{e}_1$中的元素，令$\widehat{\mathsf{A}}$表示删除矩阵$\mathsf{A}'$的第一行和第一列后所得到的$(D-1, D-1)$ 矩阵。

(d) 若$g \neq 0$，令$L = \emptyset$。否则，令$L = (\mathsf{ExtractLinForms}(\mathscr{L}_i, \mathsf{MinPol}(\mathscr{U})), 1 \le i \le D)$，返回$q, \widehat{\mathsf{A}}, \mathscr{L}, L$。

命题 5.2. 给定线性矩阵不等式$\mathsf{A} = \mathsf{A}_0 + X_1\mathsf{A}_1 + \cdots + X_k\mathsf{A}_k$，其中$\mathsf{A}_0, \ldots, \mathsf{A}_k$ 是有理系数或实代数数系数（$\mathbb{Q}(\vartheta)$）的$(D \times D)$ 对称矩阵，g为实代数数ϑ的极小多项式，当$\mathsf{A}_0, \ldots, \mathsf{A}_k$中元素均为有理系数时，可令$g = 0$。假设$\mathsf{A} \succeq 0$ 是弱可行或不可行并且不存在非零向量$\mathbf{u} \in \mathbb{R}^D - \{\mathbf{0}\}$使得$\mathsf{A}\mathbf{u} = \mathbf{0}$。

子程序$\mathsf{WeakRealLMI}(\mathsf{A}, [X_1, \ldots, X_k], g)$ 返回$q, \widehat{\mathsf{A}}, \mathscr{L}, L$，其中$q$为实代数数$\nu$的极小多项式，$\widehat{\mathsf{A}}$ 是元素在$\mathbb{Q}[X_1, \ldots, X_k]$ 或$\mathbb{Q}(\vartheta)[X_1, \ldots, X_k]$ 中的$(D-1, D-1)$对称矩阵。$\mathscr{L}$ 是$\mathbb{Q}[X_1, \ldots, X_k]$ 或$\mathbb{Q}(\nu)[X_1, \ldots, X_k]$ 中的一组线性多项式，它们在$\mathfrak{S}(\mathsf{A})$ 的所有点处取值为0。$\mathfrak{S}(\widehat{\mathsf{A}}) \cap \mathsf{Sols}(\mathscr{L}) = \mathfrak{S}(\mathsf{A})$。若输入中$g \neq 0$，$L = \emptyset$; 否则，$L$ 是$\mathbb{Q}[X_1, \ldots, X_k]$中的一组线性多项式，它们在$\mathfrak{S}(\mathsf{A}) \cap \mathbb{Q}^k$的所有点处取值为0，$\mathfrak{S}(\widehat{\mathsf{A}}) \cap \mathsf{Sols}(L) \cap \mathbb{Q}^k = \mathfrak{S}(\mathsf{A}) \cap \mathbb{Q}^k$。

算法正确性证明　与命题3.2命题类似，证明分两种情形。

情形1. 假设存在一个非零向量$\mathbf{u}=(u_1,\ldots,u_D)^\star\in\mathbb{R}^D-\{0\}$满足$\mathbf{u}^\star\mathsf{A}\mathbf{u}=0$。第1步计算了这样一个向量。在 [37, 引理4.3.5] 的证明中，如果$\mathbf{u}=\mathbf{e}_1$，那么$\mathsf{A}\,\mathbf{e}_1$中的所有非零元素$\mathscr{L}$ 在$\mathfrak{S}(\mathsf{A})$的所有点处取值为0；更进一步，我们已经假设$\{\mathbf{u}\mid\mathsf{A}\mathbf{u}=\mathbf{0}\}=\{\mathbf{0}\}$，$\mathscr{L}$中必然存在非零元素。

记i为满足$u_i\neq 0$的最小指标，如果这个向量包含实代数数ν，q为向量$\mathscr{U}$中实代数数ν的极小多项式。这里，为了得到像$\mathbf{u}=\mathbf{e}_1$这样的简单情形，第2步用$\mathsf{A}'=\mathsf{P}^\star\mathsf{A}\mathsf{P}$来替换$\mathsf{A}$，这里$\mathsf{P}$为$(D\times D)$矩阵，它的第一列为$\mathbf{u}$并且其它列为向量$\mathbf{e}_j$（$j\in\{1,\ldots,D\}-\{i\}$）（参见第2b步）。注意到$\mathsf{P}$为不可逆矩阵，考虑第2b步的矩阵$\mathsf{A}'$；引理2.3 推出$\mathfrak{S}(\mathsf{A}')=\mathfrak{S}(\mathsf{A})$。更进一步，根据 [37, 引理4.3.5]的证明，$\mathsf{A}'\mathbf{e}_1$ 的所有元素（第2c步）在$\mathfrak{S}(\mathsf{A}')$的所有点处取值为0。$\widehat{\mathsf{A}}$的元素均在$\mathsf{A}$中，所以它是元素在$\mathbb{Q}[X_1,\ldots,X_k]$ 或$\mathbb{Q}(\vartheta)[X_1,\ldots,X_k]$ 中的$(D-1,D-1)$对称矩阵，引理2.2 推出$\mathfrak{S}(\widehat{\mathsf{A}})\cap\mathsf{Sols}(\mathscr{L})=\mathfrak{S}(\mathsf{A}')\cap\mathsf{Sols}(\mathscr{L})$；另外，$\mathfrak{S}(\mathsf{A}')=\mathfrak{S}(\mathsf{A})$，于是$\mathfrak{S}(\widehat{\mathsf{A}})\cap\mathsf{Sols}(\mathscr{L})=\mathfrak{S}(\mathsf{A})$。

若$g\neq 0$，$L=\emptyset$；否则，L 表示第2d步得到的线性多项式，并且$\mathsf{Sols}(L)\subset\mathbb{R}^k$为它们的公共解构成的仿射线性子空间。更进一步，根据L的构造，矩阵A'的第一行和第一列在$\mathsf{Sols}(L)$的所有点处取值为$\mathbf{0}$。引理2.7 推出

$$\mathfrak{S}(\mathsf{A}')\cap\mathbb{Q}^k=\mathfrak{S}(\mathsf{A}')\cap\mathsf{Sols}(L)\cap\mathbb{Q}^k。$$

引理2.2 推出$\mathfrak{S}(\widehat{\mathsf{A}})\cap\mathsf{Sols}(L)=\mathfrak{S}(\mathsf{A}')\cap\mathsf{Sols}(L)$；另外，$\mathfrak{S}(\mathsf{A}')=\mathfrak{S}(\mathsf{A})$，我们推出$\mathfrak{S}(\widehat{\mathsf{A}})\cap\mathsf{Sols}(L)\cap\mathbb{Q}^k=\mathfrak{S}(\mathsf{A})\cap\mathbb{Q}^k$。

情形2. 我们假设不存在一个非零向量$\mathbf{u}\in\mathbb{R}^D-\{\mathbf{0}\}$满足$\mathbf{u}^\star\mathsf{A}\mathbf{u}=0$。由 [37]，存在一组向量$\mathbf{u}_1,\ldots,\mathbf{u}_D$ in $\mathbb{R}^D$ 满足$\sum_{i=1}^D\mathbf{u}_i^\star\mathsf{A}\mathbf{u}_i=0$，并且$\mathbf{u}_1\neq\mathbf{0},\mathbf{u}_2\neq\mathbf{0}$。第3步，通过计算$\mathscr{V}$来求解向量$\mathbf{u}_1,\ldots,\mathbf{u}_D$。第4步，从$\mathscr{V}$提取向量$\mathbf{u}_1\in\mathbb{R}^D-\{\mathbf{0}\}$的编码$\mathscr{U}$；注意到$\mathbf{u}_1^\star\mathsf{A}\mathbf{u}_1\neq 0$。在 [37, 引理4.3.5]的证明中，当$\mathbf{u}_1=\mathbf{e}_1$时，矩阵$\mathsf{A}$的第一行和第一列在$\mathfrak{S}(\mathsf{A})$的所有点处取值为0。

我们用矩阵A'替代矩阵A来恢复这一情形，（第4b步）：这里我们有$\mathbf{e}_1^\star\mathsf{A}'\mathbf{e}_1\neq 0$；根据引理2.3, $\mathfrak{S}(\mathsf{A}')=\mathfrak{S}(\mathsf{A})$。对应于 [37, 引理4.3.5]（情形2）证明中的构造，第4c步也给出了线性多项式$\mathscr{L}_1,\ldots,\mathscr{L}_D$的构造，它们在$\mathfrak{S}(\mathsf{A}')=\mathfrak{S}(\mathsf{A})$的所有点处取值为0。$\widehat{\mathsf{A}}$的元素均在$\mathsf{A}$中，所以它是元素在$\mathbb{Q}[X_1,\ldots,X_k]$ 或$\mathbb{Q}(\vartheta)[X_1,\ldots,X_k]$中的$(D-1,D-1)$ 对称矩阵，引理2.2 推出$\mathfrak{S}(\widehat{\mathsf{A}})\cap\mathsf{Sols}(\mathscr{L})=\mathfrak{S}(\mathsf{A}')\cap\mathsf{Sols}(\mathscr{L})$；另外，$\mathfrak{S}(\mathsf{A}')=\mathfrak{S}(\mathsf{A})$，于是$\mathfrak{S}(\widehat{\mathsf{A}})\cap\mathsf{Sols}(\mathscr{L})=\mathfrak{S}(\mathsf{A})$。

若$g \neq 0$，$L = \emptyset$；否则，L表示第2d步得到的线性多项式，并且$\mathsf{Sols}(L) \subset \mathbb{R}^k$为它们的公共解构成的仿射线性子空间。和情形1一样，根据L的构造，矩阵A'的第一行和第一列在$\mathsf{Sols}(L)$的所有点处取值为$\mathbf{0}$。和情形1一样，引理2.7推出

$$\mathfrak{S}(\mathsf{A}') \cap \mathbb{Q}^k = \mathfrak{S}(\mathsf{A}') \cap \mathsf{Sols}(L) \cap \mathbb{Q}^k。$$

引理2.2 推出$\mathfrak{S}(\widehat{\mathsf{A}}) \cap \mathsf{Sols}(L) = \mathfrak{S}(\mathsf{A}') \cap \mathsf{Sols}(L)$；另外，$\mathfrak{S}(\mathsf{A}') = \mathfrak{S}(\mathsf{A})$，我们推出$\mathfrak{S}(\widehat{\mathsf{A}}) \cap \mathsf{Sols}(L) \cap \mathbb{Q}^k = \mathfrak{S}(\mathsf{A}) \cap \mathbb{Q}^k$。 □

5.2.3 主算法

给定线性矩阵不等式$\mathsf{A} = \mathsf{A}_0 + X_1\mathsf{A}_1 + \cdots + X_k\mathsf{A}_k \succeq 0$，它的可行域为$\mathfrak{S}(\mathsf{A})$。其中$\mathsf{A}_0, \ldots, \mathsf{A}_k$ 是有理系数或实代数数系数（$\mathbb{Q}(\vartheta)$）的$(D \times D)$ 对称矩阵，g为实代数数ϑ的极小多项式，当$\mathsf{A}_0, \ldots, \mathsf{A}_k$中元素均为有理系数时，可令$g = 0$。我们下面描述本章的主算法RealLMI。它的输入为$\mathsf{A}, [X_1, \ldots, X_k], g$，如果$\mathsf{A} \succeq 0$存在实数解，它返回$(X_1 - \mathbf{x}_1, \ldots, X_k - \mathbf{x}_k)$来代表$\mathbf{x} = (\mathbf{x}_1, \ldots, \mathbf{x}_k) \in \mathfrak{S}(\mathsf{A})$，其他情况下返回$\emptyset$。

在算法的开始，我们考虑下面的半代数集：

$$G = \{\mathbf{u} \in \mathbb{R}^D - \{\mathbf{0}\} \mid \mathsf{A}\mathbf{u} = \mathbf{0},\ g(\vartheta) = 0\}。$$

我们记程序ConstructFormula输入为A，并且返回定义G的公式。

RealLMI$(\mathsf{A}, [X_1, \ldots, X_k], g)$

1. $\mathscr{U}$ = BasicRealLMI$(\mathsf{A}, [X_1, \ldots, X_k], g)$。
2. 如果$\mathscr{U} \neq$ false非空，记$(x_1, \ldots, x_k)$为$\mathscr{U}$中的点，返回$X_1 - x_1, \ldots, X_k - x_k$。
3. 令$\mathscr{U}$ = LinearSolve(ConstructFormula(A))。
4. 如果$\mathscr{U}$非空，于是
   (a) 计算可逆矩阵P，它的元素在$\mathbb{Q}$或$\mathbb{Q}(\vartheta)$中，并且满足$\mathsf{P}\mathbf{e}_1 = \mathbf{u}$，记$\mathsf{A}' = \mathsf{P}^\star\mathsf{A}\mathsf{P}$，$\widehat{\mathsf{A}}$表示删除矩阵$\mathsf{A}'$的第一行和第一列后所得到的$(D-1, D-1)$矩阵。
   (b) 返回RealLMI$(\widehat{\mathsf{A}}, [X_1, \ldots, X_k], g)$。

5. $q, \widehat{\mathsf{A}}, \mathscr{L}, L = \mathsf{WeakRealLMI}(\mathsf{A}, [X_1, \ldots, X_k], g)$。

6. 若$\mathsf{LinearSolve}(L)$非空，$\mathcal{X}, \mathcal{H}, \mathcal{V} = \mathsf{GaussianElimination}(L)$；若$\mathsf{LinearSolve}(\mathscr{L})$非空，$\mathcal{X}, \mathcal{H}, \mathcal{V} = \mathsf{GaussianElimination}(\mathscr{L})$；否则，返回$\emptyset$。

7. $\widetilde{\mathsf{A}} = \mathsf{Substitute}(\mathcal{X}, \mathcal{H}, \widehat{\mathsf{A}})$，并且$R = \mathsf{RealLMI}(\widetilde{\mathsf{A}}, \mathcal{V}, q)$。

8. 如果R 非空，于是返回$R, \mathsf{Evaluate}(\mathcal{X}, \mathcal{H}, R)$，否则，返回$\emptyset$。

定理 5.3. *给定线性矩阵不等式$\mathsf{A} = \mathsf{A}_0 + X_1\mathsf{A}_1 + \cdots + X_k\mathsf{A}_k$，其中$\mathsf{A}_0, \ldots, \mathsf{A}_k$ 是有理系数或实代数数系数（$\mathbb{Q}(\vartheta)$）的$(D \times D)$ 对称矩阵，g为实代数数ϑ的极小多项式，当$\mathsf{A}_0, \ldots, \mathsf{A}_k$中元素均为有理系数时，可令$g = 0$。当$\mathfrak{S}(\mathsf{A}) \neq \emptyset$时，算法$\mathsf{RealLMI}(\mathsf{A}, [X_1, \ldots, X_k], g)$ 返回$\mathfrak{S}(\mathsf{A})$中的点，否则返回空集。*

算法正确性证明　假设$k = 1$，或$\mathfrak{S}(\mathsf{A})$ 满维（若$D = 1$并且$k \geq 1$，$\mathfrak{S}(\mathsf{A})$满维）。正确性从命题5.1得证。下面通过对D归纳证明：我们的归纳假设是对于$D-1$阶$\mathbb{Q}[X_1, \ldots, X_p]$（或$\mathbb{Q}(\vartheta)[X_1, \ldots, X_p]$）上的线性对称矩阵$\mathsf{B}$，$g$为实代数数$\vartheta$的极小多项式，$\mathsf{RealLMI}(\mathsf{B}, [X_1, \ldots, X_p], g)$输出$\mathfrak{S}(\mathsf{B})$上的实数解当且仅当$\mathfrak{S}(\mathsf{B})$非空。

假设存在向量$\mathbf{u} \in \mathbb{R}^D - \{0\}$满足$\mathsf{A}.\mathbf{u} = \mathbf{0}$，第3步计算这样一个向量。引理2.3 确保$\mathfrak{S}(\mathsf{A}')$ （对称矩阵A'由第4a步得到）和$\mathfrak{S}(\mathsf{A})$相等。更进一步，通过构造，我们有$\mathsf{A}'\mathbf{e}_1 = \mathbf{0}$；矩阵$\mathsf{A}'$的第一行和第一列为$\mathbf{0}$。通过引理2.2 和2.3，我们推断$\mathfrak{S}(\widehat{\mathsf{A}}) = \mathfrak{S}(\mathsf{A}') = \mathfrak{S}(\mathsf{A})$。通过对矩阵$\widehat{\mathsf{A}}$的归纳假设，我们推断，如果$\mathfrak{S}(\mathsf{A}) \neq \emptyset$，第4b步的$\mathsf{RealLMI}$命令将输出$\mathfrak{S}(\mathsf{A})$ 上的实数解，否则返回$\emptyset$。

现在假设没有非零向量$\mathbf{u} \in \mathbb{R}^D - \{0\}$满足$\mathsf{A}.\mathbf{u} = \mathbf{0}$；我们进入第5步。命题5.2推出：

- q为实代数数ν的极小多项式；
- $\widehat{\mathsf{A}}$ 是元素在$\mathbb{Q}[X_1, \ldots, X_k]$ 或$\mathbb{Q}(\vartheta)[X_1, \ldots, X_k]$ 中的$(D-1) \times (D-1)$对称线性矩阵；
- $\mathscr{L}$是$\mathbb{Q}[X_1, \ldots, X_k]$ 或$\mathbb{Q}(\nu)[X_1, \ldots, X_k]$ 中的线性多项式，它们在$\mathfrak{S}(\mathsf{A})$ 的所有点处取值为0；令$\mathsf{Sols}(\mathscr{L}) \subset \mathbb{R}^k$ 是$\mathscr{L}$ 的公共解构成的线性子空间，

$$\mathfrak{S}(\widehat{\mathsf{A}}) \cap \mathsf{Sols}(\mathscr{L}) = \mathfrak{S}(\mathsf{A});$$

- 如果矩阵A的元素中含有$\mathbb{Q}(\vartheta)[X_1,\ldots,X_k]$ 中的线性多项式（此时输入中$g \neq 0$），$L=\emptyset$；否则，L 是$\mathbb{Q}[X_1,\ldots,X_k]$中的有理系数线性多项式，它们在$\mathfrak{S}(\mathsf{A})\cap\mathbb{Q}^k$ 的所有点处取值为0 ；我们令$\mathsf{Sols}(L)\subset\mathbb{R}^k$ 表示L 的公共解构成的线性子空间，

$$\mathfrak{S}(\widehat{\mathsf{A}})\cap\mathsf{Sols}(L)\cap\mathbb{Q}^k=\mathfrak{S}(\mathsf{A})\cap\mathbb{Q}^k。$$

如果$L=0$无解，那么$\mathfrak{S}(\mathsf{A})\cap\mathbb{Q}^k$为空集；如果$\mathscr{L}=0$无解，那么$\mathfrak{S}(\mathsf{A})$为空集；线性多项式$L$或$\mathscr{L}$被用来消去$\widehat{\mathsf{A}}$中的若干变元；这将得到$(D-1,D-1)$线性对称矩阵$\widetilde{\mathsf{A}}$（第6步）。在第7步，将归纳假设应用到矩阵$\widetilde{\mathsf{A}}$，我们推断，通过调用RealLMI命令，若$\mathfrak{S}(\widehat{\mathsf{A}})\cap\mathsf{Sols}(L)\cap\mathbb{Q}^k$非空，将返回该集合中的一个有理点的若干分量；若$\mathfrak{S}(\widehat{\mathsf{A}})\cap\mathsf{Sols}(\mathscr{L})$非空，将返回该集合中的一个实数解的若干分量；否则返回$\emptyset$。我们之前已经证明$\mathfrak{S}(\widehat{\mathsf{A}})\cap\mathsf{Sols}(L)\cap\mathbb{Q}^k=\mathfrak{S}(\mathsf{A})\cap\mathbb{Q}^k$；$\mathfrak{S}(\widehat{\mathsf{A}})\cap\mathsf{Sols}(\mathscr{L})=\mathfrak{S}(\mathsf{A})$；如果$R$非空，第8步$\mathsf{Evaluate}(\mathcal{X},\mathcal{H},R)$命令将返回$\mathfrak{S}(\mathsf{A})$中的一个有理数解或精确的实数解，否则返回$\emptyset$，定理得证。 □

5.2.4 例子

例 5.1. [41] 我们再来看一下第三章中的例子，假设$\mathsf{A}=\mathsf{A}_0+X_1\mathsf{A}_1$，其中

$$\mathsf{A}_0=\begin{bmatrix}0&2&0&0\\2&0&0&0\\0&0&2&0\\0&0&0&1\end{bmatrix},\quad \mathsf{A}_1=\begin{bmatrix}2&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}。$$

矩阵A的特征多项式为

$$\begin{aligned}\chi(y)=&\,y^4+(-3-3\,X_1)\,y^3+({X_1}^2-2+9\,X_1)\,y^2\\&+(-6\,{X_1}^2+3\,{X_1}^3-6\,X_1+12)\,y\\&+8\,{X_1}^2-2\,{X_1}^4-8。\end{aligned}$$

令$m_3,\ldots,m_0$为$\chi(y)$中$y^3,y^2,y,1$的系数，它们定义了半代数集Φ和Ψ。

- 在RealLMI的第一步，$\mathsf{A}_0,\mathsf{A}_1$均为有理系数，令$g_0=0$，
  运行$\mathsf{BasicRealLMI}(\mathsf{A},[X_1],g_0)$。

– 通过因式分解，我们发现m_3的线性因子$X_1-\sqrt{2}$，并且$X_1=\sqrt{2}$ 满足Φ，返回$\sqrt{2}$。

- 在算法RealLMI的第二步，$\mathscr{U}=\{\sqrt{2}\}$，返回$X_1-\sqrt{2}$。

实际上，$\sqrt{2}$为$\mathfrak{S}(\mathsf{A})$的唯一解。

例 5.2. 我们再来看一下第四章中的例子：

$$\mathsf{A}=\begin{bmatrix} 2 & 0 & X_1 & 0 & -2 & 0 \\ 0 & 1-2\,X_1 & 0 & 0 & -2 & 0 \\ X_1 & 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 & -1 & 0 \\ -2 & -2 & 0 & -1 & 8 & -1 \\ 0 & 0 & -1 & 0 & -1 & 2 \end{bmatrix}。$$

矩阵A的特征多项式$\chi(y)$中$y^5,\ldots,1$的系数$m_5,\ldots,m_0$为：

$$\begin{aligned} m_5 &= -15+2\,X_1, \\ m_4 &= 64-28\,X_1-{X_1}^2, \\ m_3 &= -110+108\,X_1+12\,{X_1}^2-2\,{X_1}^3, \\ m_2 &= 78-156\,X_1-31\,{X_1}^2+22\,{X_1}^3, \\ m_1 &= 84\,X_1+33\,{X_1}^2-18-48\,{X_1}^3, \\ m_0 &= -12\,X_1-13\,{X_1}^2+26\,{X_1}^3。 \end{aligned}$$

它们定义了半代数集Φ 和Ψ。

- 在算法RealLMI中的第一步，A为有理系数，令$g_0=0$，
运行BasicRealLMI$(\mathsf{A},[X_1],g_0)$。

  – 通过因式分解，我们发现m_0的线性因子X_1和$X_1-\frac{1}{4}+\frac{\sqrt{1417}}{52}$，它们的解$X_1=0$和$X_1=\frac{1}{4}-\frac{\sqrt{1417}}{52}$满足$\Phi$，返回$\{\frac{1}{4}-\frac{\sqrt{1417}}{52},0\}$。

- 在算法RealLMI的第二步，$\mathscr{U}=\{\frac{1}{4}-\frac{\sqrt{1417}}{52},0\}$，返回$X_1-\frac{1}{4}+\frac{\sqrt{1417}}{52}$和$X_1$。

实际上，

$$\mathfrak{S}(\mathsf{A}) = \left[\frac{1}{4} - \frac{\sqrt{1417}}{52}, 0\right]$$

是满维的，A是强可行的。

5.3 Scheiderer反例实系数平方和分解的计算机实现

我们在上一章中给出了Scheiderer关于Sturmfels问题反例 [74]，多项式

$$f = x^4 + x\,y^3 + y^4 - 3\,x^2\,y\,z - 4\,x\,y^2\,z + 2\,x^2\,z^2 + x\,z^3 + y\,z^3 + z^4$$

不能表示为有理系数多项式的平方和的计算机验证。Scheiderer给出了f的如下实系数多项式平方和分解，

$$f = (x^2 + \frac{y^2\,\beta}{2} - \frac{x\,z}{2} + \frac{z^2\,(2\,\beta+1)}{2\,\beta})^2 - \beta\,(x\,y - \frac{y^2}{2\,\beta} + \frac{x\,z\,\beta}{2} + \frac{y\,z}{\beta} - \frac{z^2}{2})^2。$$

这里$\beta \approx -1.860805853(-0.2541016884)$是$\beta^3 - 4\beta - 1$的一个负数根。

下面我们借助本章中的算法RealLMI给出这一平方和分解的计算机实现。

假设$f = [x^2, xy, y^2, xz, yz, z^2]\,\mathsf{A}\,[x^2, xy, y^2, xz, yz, z^2]^\star$，多项式$f$的Gram矩阵A是一个$6 \times 6$对称矩阵

$$\begin{bmatrix}
1 & 0 & X_1 & 0 & -\frac{3}{2} - X_2 & X_3 \\
0 & -2\,X_1 & \frac{1}{2} & X_2 & -2 - X_4 & -X_5 \\
X_1 & \frac{1}{2} & 1 & X_4 & 0 & X_6 \\
0 & X_2 & X_4 & -2\,X_3 + 2 & X_5 & \frac{1}{2} \\
-\frac{3}{2} - X_2 & -2 - X_4 & 0 & X_5 & -2\,X_6 & \frac{1}{2} \\
X_3 & -X_5 & X_6 & \frac{1}{2} & \frac{1}{2} & 1
\end{bmatrix}。$$

这里有6个变元：$X_1, X_2, X_3, X_4, X_5, X_6$ 对应7个对称矩阵$\mathsf{A}_0, \mathsf{A}_1, \mathsf{A}_2, \mathsf{A}_3, \mathsf{A}_4, \mathsf{A}_5, \mathsf{A}_6$。

- 应用软件包RAGLib [69]中的命令HasRealSolutions，计算

$$\mathscr{U} = \mathsf{OpenDecision}(\Psi)。$$

集合$\mathscr{U}$为空集，于是A不是强可行的。

- 在算法RealLMI的第5步，A为有理系数，令$g_0 = 0$，
运行WeakRealLMI(A, $[X_1, \cdots, X_6], g_0$)。

1. 通过命令RationalUnivariateRepresentation [66], 我们得到一个实代数数解

$$\mathbf{u} = \begin{bmatrix} -1 + \frac{1}{2}\vartheta + \frac{1}{2}\vartheta^4 \\ \frac{\vartheta^3}{2} + \frac{1}{2} \\ \vartheta^2 \\ -2\,\vartheta + \frac{1}{2}\vartheta^2 + \frac{1}{2}\vartheta^5 \\ \vartheta \\ 1 \end{bmatrix},$$

2. $\mathscr{U}$非空，于是
   (a) $i = 1$，$g = \vartheta^6 - 4\,\vartheta^2 - 1 = 0$为实代数数$\vartheta$的极小多项式。
   (b) $P = [\mathsf{Param}(\mathscr{U}), e_2, \ldots, e_6]$ 并且A′ = P⋆AP。
   (c) $\mathscr{L}_1, \ldots, \mathscr{L}_6$为矩阵A′的第一列中的元素

$$\begin{bmatrix} 0 \\ \frac{1}{2}X_2\,\vartheta^5 - X_1\vartheta^3 + \cdots - X_1 - X_5 \\ \frac{1}{2}X_4\,\vartheta^5 + \frac{1}{2}X_1\,\vartheta^4 + \cdots - X_1 + X_6 + \frac{1}{4} \\ (1 - X_3)\,\vartheta^5 + \frac{1}{2}X_2\,\vartheta^3 + \cdots + \frac{1}{2} + \frac{1}{2}X_2 \\ \frac{1}{2}X_5\,\vartheta^5 + \cdots + 1 + X_2 - \frac{1}{2}X_4 \\ \frac{1}{4}\vartheta^5 + \frac{1}{2}X_3\,\vartheta^4 + \cdots - X_3 + 1 - \frac{1}{2}X_5 \end{bmatrix}。$$

   由于$i = 1$，$\widehat{\mathsf{A}}$为矩阵A删除第一行和第一列后得到的5×5矩阵。

(d) $\mathscr{L}_1,\ldots,\mathscr{L}_6$中$\vartheta^5,\ldots,\vartheta^1,1$的系数记为$L$, 返回$g,\widehat{\mathsf{A}},\mathscr{L},L$。

- 在算法RealLMI的第6步，$\mathscr{L}_1,\ldots,\mathscr{L}_6$中$\vartheta^5$的系数向量为

$$L_5=\left[0,\frac{1}{2}X_2,\frac{1}{2}X_4,1-X_3,\frac{1}{2}X_5,\frac{1}{4}\right]^\star。$$

L_5的最后一个元素为$\frac{1}{4}$，线性系统$L_5=0$ 无解。因此，LinearSolve(L) 返回空集。求解$\mathscr{L}=0$，我们用X_4,X_5,X_6来表示X_1,X_2,X_3，

$$\left\{\begin{array}{rcl} X_1 &=& \frac{1}{2}X_4\,\vartheta^5-\frac{1}{2}\vartheta^4\,X_6+\cdots-\frac{1}{4}+X_6,\\ X_2 &=& (-\frac{1}{2}X_5-X_6)\,\vartheta^5+\frac{\vartheta^4}{4}+\cdots+\frac{1}{2}X_4-1,\\ X_3 &=& -\frac{\vartheta^4}{2}+(\frac{1}{2}X_5+\frac{1}{2}X_6)\,\vartheta^3+\cdots-\frac{1}{2}X_5-\frac{1}{2}X_6+1。\end{array}\right.$$

- 在算法RealLMI的第7步，矩阵$\widehat{\mathsf{A}}$转变为5×5含3个变元X_4,X_5,X_6的对称矩阵B，

$$\left[\begin{array}{ccccc} -X_4\,\vartheta^5+\cdots+\frac{1}{2}-2\,X_6\,, & \frac{1}{2}\,, & (-\frac{1}{2}X_5-X_6)\,\vartheta^5+\cdots+\frac{1}{2}X_4-1, & -X_4-2\,, & -X_5\\ \frac{1}{2}\,, & 1\,, & X_4\,, & 0\,, & X_6\\ (-\frac{1}{2}X_5-X_6)\,\vartheta^5+\cdots+\frac{1}{2}X_4-1, & X_4\,, & \vartheta^4+\cdots+X_5+X_6\,, & X_5\,, & \frac{1}{2}\\ -X_4-2\,, & 0\,, & X_5\,, & -2\,X_6\,, & \frac{1}{2}\\ -X_5\,, & X_6\,, & \frac{1}{2}\,, & \frac{1}{2}\,, & 1 \end{array}\right]。$$

运行RealLMI$(\mathsf{B},[X_4,X_5,X_6],g)$。

– 应用软件包RAGLib [69]中的命令HasRealSolutions，计算

$$\mathscr{U}=\mathsf{OpenDecision}(\Psi)。$$

集合$\mathscr{U}$为空集，于是B不是强可行的。

– 运行WeakRealLMI$(\mathsf{B},[X_4,X_5,X_6],g)$，我们得到

1.

$$\mathbf{u}=\left[\begin{array}{c} 1\\ -1\\ 4\,\nu^4-\nu^2-16\\ \nu^2+8-2\,\nu^4\\ -\nu^4+4 \end{array}\right]。$$

2. $\mathscr{U}$非空，于是

(a) $i=1$，$q=\nu^6-4\,\nu^2-1=0$为实代数数ν的极小多项式。经过化简，我们可以得到$\vartheta=\nu$。

(b) $P_1=[\mathsf{Param}(\mathscr{U}),e_2,\ldots,e_5]$ 并且$B'=\mathsf{P_1}^{\star}B\mathsf{P_1}$。

(c) 矩阵B′的第一列$\mathscr{L}'$为

$$\begin{bmatrix} 0 \\ -\frac{1}{2}+(4\,\nu^4-\nu^2-16)\,X_4+(-\nu^4+4)\,X_6 \\ \frac{1}{2}\,\nu^5\,X_5+\cdots-8\,X_5-\frac{1}{2}\,X_4-8\,X_6+1 \\ -X_4+(4\,\nu^4-\nu^2-16)\,X_5-2\,(\nu^2+8-2\,\nu^4)\,X_6-\frac{\nu^4}{2} \\ -X_5-X_6 \end{bmatrix}。$$

– 求解$\mathscr{L}'=0$，我们得到

$$X_5=-X_6,\ X_4=-\nu^2\,X_6-\frac{\nu^4}{2}。\tag{5.1}$$

更进一步，我们有

$$X_1=X_6,\ X_2=-1,\ X_3=X_4+1。\tag{5.2}$$

– 我们将矩阵B转化为一个4×4只含一个变元X_6的对称矩阵C，

$$\mathsf{C}=\begin{bmatrix} 1 & -\nu^2\,X_6-\frac{\nu^4}{2} & 0 & X_6 \\ -\nu^2\,X_6-\frac{\nu^4}{2} & \nu^4+2\,\nu^2\,X_6 & -X_6 & \frac{1}{2} \\ 0 & -X_6 & -2\,X_6 & \frac{1}{2} \\ X_6 & \frac{1}{2} & \frac{1}{2} & 1 \end{bmatrix}。$$

- 运行RealLMI$(\mathsf{C},[X_6],q)$，我们发现X_6 满足

$$-1-8X_6+8X_6^3=0,\tag{5.3}$$

其他所有变元可由变元X_6表示:

$$X_1=X_6,\ X_2=-1,X_4=\frac{1}{4X_6},X_5=-X_6,\ X_3=\frac{1}{4X_6}+1。\tag{5.4}$$

- 将（5.4）中的解替换到矩阵A中，我们得到

$$\mathsf{M}=\begin{bmatrix} 1 & 0 & X_6 & 0 & \frac{-1}{2} & 1+\frac{1}{4X_6} \\ 0 & -2\,X_6 & \frac{1}{2} & -1 & -2-\frac{1}{4X_6} & X_6 \\ X_6 & \frac{1}{2} & 1 & \frac{1}{4X_6} & 0 & X_6 \\ 0 & -1 & \frac{1}{4X_6} & -\frac{1}{2X_6} & -X_6 & \frac{1}{2} \\ \frac{-1}{2} & -2-\frac{1}{4X_6} & 0 & -X_6 & -2\,X_6 & \frac{1}{2} \\ 1+\frac{1}{4X_6} & X_6 & X_6 & \frac{1}{2} & \frac{1}{2} & 1 \end{bmatrix}。$$

对矩阵M进行LU分解并且在（5.3）定义的代数扩域上进行计算，我们发现矩阵M半正定且秩为2。因此，我们有f的如下平方和分解，

$$\begin{aligned} f &= \left(x^2+y^2\,X_6-\frac{y\,z}{2}+\frac{1}{4}\,\frac{z^2\,(1+4\,X_6)}{X_6}\right)^2 \\ &\quad -2\,X_6\left(x\,y-\frac{1}{4}\,\frac{y^2}{X_6}+\frac{1}{2}\,\frac{x\,z}{X_6}+y\,z\,X_6-\frac{z^2}{2}\right)^2。 \end{aligned}$$

两个负数根$X_6\approx -0.930402926555852$和$X_6\approx -0.127050844182526$将给出多项式$f$的实系数平方和分解。这个表示形式和文章 [74]中的表示是一致的。

第六章　结论与展望

给定线性矩阵不等式$\mathsf{A} = \mathsf{A}_0 + X_1\mathsf{A}_1 + \cdots + X_k\mathsf{A}_k \succeq 0$，其中$\mathsf{A}_0, \ldots, \mathsf{A}_k$是有理系数的$(D \times D)$ 对称矩阵，其中元素二进制表示的位长不超过τ，它的可行域为$\mathfrak{S}(\mathsf{A})$。

在第三章，我们给出了一个算法RationalLMI来判定$\mathfrak{S}(\mathsf{A})$是否包含有理数解，在有理数解存在时给出有理数解。当矩阵阶数为$D = 1$或变元个数$k = 1$以及$\mathfrak{S}(\mathsf{A})$满维时，这几类简单情形可利用子程序BasicCasesLMI来处理。若存在非零向量$\mathbf{u} \in \mathbb{R}^D - \{\mathbf{0}\}$使得$\mathsf{A}\mathbf{u} = \mathbf{0}$，我们得到了一个阶数更小的线性矩阵不等式$\widehat{\mathsf{A}} \succeq 0$，通过对矩阵$\widehat{\mathsf{A}}$迭代可以给出$\mathfrak{S}(\mathsf{A})$上有理数解的存在性判定和计算。当$\mathfrak{S}(\mathsf{A})$不满维时，若不存在非零向量$\mathbf{u} \in \mathbb{R}^D - \{\mathbf{0}\}$使得$\mathsf{A}\mathbf{u} = \mathbf{0}$，在子程序WeakLMI我们得到一组实系数线性多项式$\mathscr{L}_1, \ldots, \mathscr{L}_D \in \mathbb{R}[X_1, \ldots, X_k]$，这些线性多项式定义的超平面的交集包含了$\mathfrak{S}(\mathsf{A})$的所有实数解。更进一步，我们可以从这组实系数线性多项式构造有理系数线性多项式L，$L = 0$的解集包含了$\mathfrak{S}(\mathsf{A})$上的全部有理数解。如果$L = 0$无解，那么$\mathfrak{S}(\mathsf{A})$没有有理数解。否则，可以利用高斯消去法给出一部分变元用另一部分变元的线性表示形式，我们同时得到了一个阶数更小的矩阵$\widetilde{\mathsf{A}}$，$\mathfrak{S}(\widetilde{\mathsf{A}})$的有理数解是$\mathfrak{S}(\mathsf{A})$上有理数解的投影。通过对矩阵$\widetilde{\mathsf{A}}$迭代可以给出$\mathfrak{S}(\mathsf{A})$上有理数解的存在性判定和计算。算法RationalLMI的运行时间控制在$(k\tau)^{O(1)}2^{O(\min(k,D)D^2)}D^{O(D^2)}$位操作，并且在$\mathfrak{S}(\mathsf{A})$非空情形，输出解坐标的位长控制在$\tau^{O(1)}2^{O(\min(k,D)D^2)}$以内。作为一般凸半代数集的特殊形式，我们的算法显著改进了Safey El Din与支丽红算法的复杂度。

在第四章，我们利用算法RationalLMI对一些多项式f的Gram矩阵M定义的线性矩阵不等式$\mathsf{M} \succeq 0$的可行域$\mathfrak{S}(\mathsf{M})$是否包含有理数解进行判定，在有理数解存在时，给出有理数解并将相应的Gram矩阵进行LU分解，从而得到该多项式的有理系数平方和表示。给定多项式$f \in \mathbb{Q}[X_1, \ldots, X_n]$ 次数为$2d$，系数位长不超过τ。我们的算法可判定f 是否存在有理系数多项式平方和分解，并在分解存在时给出相应表示形式，算法复杂度为$\tau^{O(1)}2^{O(\mathsf{M}(d,n)^3)}$，其中$\mathsf{M}(d,n) = \min(d^n, n^d)$。输出表示形式中系数位长的界为$\tau^{O(1)}2^{O(\mathsf{M}(d,n)^3)}$。这是目前多项式有理系数平方和判定和计算的复杂度最好的算法。最后，我们判

定Scheiderer反例的Gram矩阵定义的线性矩阵不等式的可行域没有有理数解，从而给出了该反例不存在有理系数平方和分解的第一个计算机验证。

在第五章，考虑线性矩阵不等式$\mathsf{A} = \mathsf{A}_0 + X_1\mathsf{A}_1 + \cdots + X_k\mathsf{A}_k \succeq 0$，其中$\mathsf{A}_0, \ldots, \mathsf{A}_k$是有理系数或实代数数系数（$\mathbb{Q}(\vartheta)$）的$(D \times D)$对称矩阵，其中元素二进制表示的位长不超过$\tau$，它的可行域为$\mathfrak{S}(\mathsf{A})$。我们设计了新算法RealLMI，在线性矩阵有理数解不存在时可以给出实数解的存在性判定和计算。如果给定的线性矩阵不等式是有理系数的，在算法RealLMI中可令多项式$g = 0$，则算法RealLMI与算法RationalLMI 基本一致；在线性矩阵A中包含实代数数系数时，可令多项式g为实代数数ϑ的极小多项式。算法RealLMI在$\mathfrak{S}(\mathsf{A})$不满维时，我们可以得到一组实系数线性多项式$\mathscr{L}$和一组有理系数线性多项式L，$\mathscr{L}$在$\mathfrak{S}(\mathsf{A})$ 的所有点处取值为0，L在$\mathfrak{S}(\mathsf{A})$ 的所有有理点处取值为0。如果有理系数线性多项式$L = 0$无解，则$\mathfrak{S}(\mathsf{A})$无有理数解。若实系数线性多项式$\mathscr{L} = 0$无解，则$\mathfrak{S}(\mathsf{A})$无实数解。在$L = 0$或$\mathscr{L} = 0$有解时利用高斯消去法给出一部分变元用另一部分变元的线性表示形式，同时得到一个阶数更小的矩阵$\widetilde{\mathsf{A}}$，$\mathfrak{S}(\widetilde{\mathsf{A}})$的实数解（有理数解）是$\mathfrak{S}(\mathsf{A})$ 上实数解（有理数解）的投影。通过对矩阵$\widetilde{\mathsf{A}}$迭代可以给出$\mathfrak{S}(\mathsf{A})$上实数解（有理数解）的存在性判定和计算。最后，作为算法RealLMI的应用，我们给出了Scheiderer反例实系数平方和分解的计算机实现。

今后的工作主要包含以下几个方面：

1. 给出线性矩阵不等式整数解的存在性判定和计算方法，改进 [35,36] 中的算法，降低算法复杂度。

2. 设计针对二次多项式定义半代数集上实数解的判定和计算的高效算法，进一步降低本文中的算法复杂度。

参考文献

[1] F. Alizadeh. Interior point methods in semidefinite programming with applications to combinatorial optimization. *SIAM Journal on Optimization*, 5(1):13–51, 1995.

[2] E. Artin. Über die Zerlegung definiter Funktionen in Quadrate[J]. *Hamb. Abh.*, 5:100–115, 1927.

[3] P. Aubry, F. Rouillier, and M. Safey El Din. Real solving for positive dimensional systems. *Journal of Symbolic Computation*, 34(6):543–560, 2002.

[4] S. Basu. Algorithms in real algebraic geometry: A survey. In K. Bekka, G. Fichou, J.-P. Monnier, and R. Quarez, editors, *Conference Real Algebraic Geometry*. Universitéde Rennes 1 / IRMAR, 6 2011.

[5] S. Basu, R. Pollack, and M.-F. Roy. On the combinatorial and algebraic complexity of quantifier elimination. *Journal of the ACM*, 43(6):1002–1045, Nov. 1996.

[6] S. Basu, R. Pollack, and M.-F. Roy. A new algorithm to find a point in every cell defined by a family of polynomials. In B. Caviness and J. Johnson, editors, *Quantifier Elimination and Cylindrical Algebraic Decomposition*, Texts and Monographs in Symbolic Computation, pages 341–350. Springer Vienna, 1998.

[7] S. Basu, R. Pollack, and M.-F. Roy. *Algorithms in real algebraic geometry*, volume 10 of *Algorithms and Computation in Mathematics*. Springer-Verlag, second edition, 2006.

[8] S. J. Benson and Y. Ye. DSDP5: Software for semidefinite programming. Technical Report ANL/MCS-P1289-0905, Mathematics and Computer Science Division, Argonne National Laboratory, Argonne, IL, Sept. 2005.

[9] G. Blekherman. There are significantly more nonegative polynomials than sums of squares. *Israel Journal of Mathematics*, 153(1):355–380, December 2006.

[10] G. Blekherman, P. Parrilo, and R. Thomas. *Semidefinite Optimization and Convex Algebraic Geometry*. MOS-SIAM Series on Optimization. Society for Industrial and Applied Mathematics (SIAM, 3600 Market Street, Floor 6, Philadelphia, PA 19104), 2013.

[11] S. Boyd, L. El Ghaoui, E. Feron, and V. Balakrishnan. *Linear Matrix Inequalities in System and Control Theory*. SIAM studies in applied mathematics: 15, 1994.

[12] G. Cassier. Problème des moments sur un compact de $\mathbf{R}^n$ et décomposition de polynômes à plusieurs variables. *Journal of Functional Analysis*, 58:254–266, 1984.

[13] G. Chesi. Lmi techniques for optimization over polynomials in control: A survey. *Automatic Control, IEEE Transactions on*, 55(11):2500–2510, Nov 2010.

[14] M. Choi, T. Lam, and B. Reznick. Sums of squares of real polynomials. *Proceedings of Symposia in Pure Mathematics*, 58(2):103–126, 1995.

[15] G. Collins. Quantifier elimination for real closed fields by cylindrical algebraic decompostion. In H. Brakhage, editor, *Automata Theory and Formal Languages 2nd GI Conference Kaiserslautern, May, 1975*, volume 33 of *Lecture Notes in Computer Science*, pages 134–183. Springer Berlin Heidelberg, 1975.

[16] J. A. de Loera, F. Santos, and F. D. Ciencias. An effective version of pólya's theorem on positive definite forms, 1995.

[17] J. Faugère, G. Moroz, F. Rouillier, and M. Safey El Din. Classification of the perspective-three-point problem, discriminant variety and real solving polynomial systems of inequalities. In D. Jeffrey, editor, *Proceedings of the*

twenty-first international symposium on Symbolic and algebraic computation, ISSAC '08, pages 79–86, New York, NY, USA, 2008. ACM.

[18] M. X. Goemans and F. Rendl. Semidefinite programming in combinatorial optimization. *Mathematical Programming*, 79:143–161, 1999.

[19] M. X. Goemans and D. P. Williamson. Improved approximation algorithms for maximum cut and satisfiability problems using semidefinite programming. *Journal of the ACM*, 42(6):1115–1145, Nov. 1995.

[20] D. Grigoriev and N. Vorobjov. Solving systems of polynomial inequalities in subexponential time. *Journal of Symbolic Computation*, 5(1/2):37–64, 1988.

[21] F. Guo, E. L. Kaltofen, and L. Zhi. Certificates of impossibility of hilbert-artin representations of a given degree for definite polynomials and functions. In *Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation*, ISSAC '12, pages 195–202, New York, NY, USA, 2012. ACM.

[22] W. Habicht. Über die Zerlegung strikte definite Formen in Qauadrate[J]. *Comment. Math. Helv.*, 12:317–322, 1940.

[23] J. Harrison. Verifying nonlinear real formulas via sums of squares. In K. Schneider and J. Brandt, editors, *Proceedings of the 20th International Conference on Theorem Proving in Higher Order Logics, TPHOLs 2007*, volume 4732 of *Lecture Notes in Computer Science*, pages 102–118, Kaiserslautern, Germany, 2007. Springer-Verlag.

[24] J. Heintz, M.-F. Roy, and P. Solernó. On the theoretical and practical complexity of the existential theory of reals. *The Computer Journal*, 36(5):427–431, 1993.

[25] J. Heintz, M.-F. Roy, and P. Solernó. On the complexity of semi-algebraic sets. In *Information processing 89 : proceedings of the IFIP 11th World Computer Congress, San Francisco,U.S.A.*, pages 293–298, 1989.

[26] D. Henrion and A. Garulli, editors. *Positive polynomials in control*, volume 312 of *Lecture Notes in Control and Information Sciences*. Springer-Verlag, Berlin, 2005.

[27] D. Hilbert. Ueber die darstellung definiter formen als summen von formenquadraten. *Mathematische Annalen*, 32:342–350, 1888.

[28] D. Hilbert. Über ternäre definite Formen[J]. *Acta Math*, 17:169–197, 1893.

[29] D. Hilbert. Mathematsche Probleme[J]. *Göttinger Nachrichten*, pages 253–297, 1900.

[30] C. Hillar. Sums of polynomial squares over totally real fields are rational sums of squares. *Proceedings of the American Mathematical Society*, 137:921–930, 2009.

[31] R. Horn and C. Johnson. *Matrix analysis*. Cambridge University Press, 1985.

[32] E. Kaltofen, B. Li, Z. Yang, and L. Zhi. Exact certification of global optimality of approximate factorizations via rationalizing sums-of-squares with floating point scalars. In D. Jeffrey, editor, *Proceedings of the twenty-first international symposium on Symbolic and algebraic computation*, ISSAC '08, pages 155–164, New York, NY, USA, 2008. ACM.

[33] E. Kaltofen, B. Li, Z. Yang, and L. Zhi. Exact certification in global polynomial optimization via sums-of-squares of rational functions with rational coefficients. *Journal of Symbolic Computation*, 47(1):1–15, Jan. 2012.

[34] E. L. Kaltofen, 2009. Private communication, February 24, 2009.

[35] L. Khachiyan and L. Porkolab. Computing integral points in convex semialgebraic sets. In *Proceedings of the 38th Annual Symposium on Foundations of Computer Science*, FOCS '97, pages 162–171, Washington, DC, USA, 1997. IEEE Computer Society.

[36] L. Khachiyan and L. Porkolab. Integer optimization on convex semialgebraic sets. *Discrete and Computational Geometry*, 23(2):207–224, 2000.

[37] I. Klep and M. Schweighofer. An exact duality theory for semidefinite programming based on sums of squares. *Mathematics of Operations Research*, 38(3):569–590, Aug. 2013.

[38] J. Krivine. Anneaux preordonnes[J]. *J. Anal. Math.*, 12:307–326, 1964.

[39] E. Landau. Über die darstellung definiter funktionen als summe von quadraten. *Math. Ann.*, 62:290–329, 1906.

[40] J. B. Lasserre. Global optimization with polynomials and the problem of moments. *SIAM Journal on Optimization*, 11(3):796–817, 2001.

[41] M. Laurent. Polynomial instances of the positive semidefinite and euclidean distance matrix completion problems. *SIAM Journal on Matrix Analysis and Applications*, 22(3):874–894, June 2000.

[42] A. Lenstra, H. Lenstra, and L. Lovàsz. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261:515–534, 1982.

[43] M. Marshall. *Positive polynomials and sums of squares*, volume 146 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2008.

[44] T. Motzkin. *The arithmetic-geometric inequality*, pages 205–224. Inequalities. Academic Press, 1967.

[45] M.Ramana. An exact duality theory for semidefinite programming and its complexity implications. *Mathematical Programming*, 77(1):129–162, 1997.

[46] Y. Nesterov and A. Nemirovskii. *Interior-Point polynomial algorithms in convex programming*, volume 13 of *Studies in Applied Mathematics*. SIAM, Philidelphia, PA, 1994.

[47] A. Papachristodoulou, J. Anderson, G. Valmorbida, S. Prajna, P. Seiler, and P. A. Parrilo. *SOSTOOLS: Sum of squares optimization toolbox for MATLAB*. `http://arxiv.org/abs/1310.4716`, 2013. Available

from http://www.eng.ox.ac.uk/control/sostools, http://www.cds.caltech.edu/sostools and http://www.mit.edu/~{}parrilo/sostools.

[48] P. A. Parrilo. *Structured Semidefinite Programs and Semialgebraic Geometry Methods in Robustness and Optimization[D].* PhD thesis, California Institute of Technology, Pasadena, CA, 2000. URL: http://www.mit.edu/~parrilo/.

[49] P. A. Parrilo. Semidefinite programming relaxations for semialgebraic problems. *Mathematical Programming*, 96(2):293–320, 2003.

[50] H. Peyrl and P. A. Parrilo. A macaulay 2 package for computing sum of squares decompositions of polynomials with rational coefficients. In *Proceedings of the 2007 international workshop on Symbolic-numeric computation*, SNC '07, pages 207–208, New York, NY, USA, 2007. ACM.

[51] H. Peyrl and P. A. Parrilo. Computing sum of squares decompositions with rational coefficients. *Theoretical Computer Science*, 409(2):269–281, Dec. 2008.

[52] A. Pfister. Zur Darstellung definiter Funktionen als Summe von Quadraten. *Inventiones Math.*, 4(4):229–236, 1967.

[53] G. Polya. Über positive Darstellung von Polynomen Viereljschr. *Ges. Zürich*, 73:141–145, 1928.

[54] L. Porkolab and L. Khachiyan. On the complexity of semidefinite programs. *Journal of Global Optimization*, 10(4):351–365, June 1997.

[55] Y. Pourchet. Sur la répresentation en somme de carrés des polynômes a une indeterminée sur un corps de nombres algébraiques[J]. *Acta Arithmetica*, 19:89–109, 1971.

[56] V. Powers. Positivity and sums of squares: Theory and practice. In K. Bekka, G. Fichou, J.-P. Monnier, and R. Quarez, editors, *Conference Real Algebraic Geometry*. Universitéde Rennes 1 / IRMAR, 6 2011.

[57] V. Powers and T. Wörmann. An algorithm for sums of squares of real polynomials. *Journal of Pure and Applied Algebra*, 127:99–104, 1998.

[58] A. Prestel and C. N. Delzell. *Positive polynomials*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2001. From Hilbert's 17th problem to real algebra.

[59] A. R. Rajwade. *Squares*, volume 171 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1993.

[60] M. Ramana and P. Pardalos. Semidefinite programming. In T. Terlaky, editor, *Interior Point Methods of Mathematical Programming*, volume 5 of *Applied Optimization*, pages 369–398. Springer US, 1996.

[61] J. Renegar. On the computational complexity and geometry of the first-order theory of the reals. *Journal of Symbolic Computation*, 13:255–352, 1992.

[62] B. Reznick. Extremal PSD forms with few terms[J]. *Duke Mathematical Journal*, 45(2):363–374, 1978.

[63] B. Reznick. Uniform denominators in Hilbert's 17th problem[J]. *Mathematische Zeitschrift*, 220:75–97, 1995.

[64] B. Reznick. Some concrete aspects of Hilbert's 17th problem[J]. In C. N. Delzell and J. J. Madden, editors, *Real Algebraic Geometry and Ordered Structures*, volume 253 of *Contemporary Mathematics*, pages 251–272. AMS, Providence, RI, USA, 2000.

[65] R. Robinson. Some definite polynomials which are not sums of squares of real polynomials. In *Selected questions of algebra and logic*, pages 264–282, 1969.

[66] F. Rouillier. Solving zero-dimensional systems through the rational univariate representation. *Applicable Algebra in Engineering, Communication and Computing*, 9:433–461, 1999.

[67] F. Rouillier. Efficient algorithms based on critical points method. In *Algorithmic and Quantitative Aspects of Real Algebraic Geometry in Mathematics and Computer Science*, pages 123–138, 2001.

[68] F. Rouillier, M. Roy, and M. Safey. Finding at least one point in each connected component of a real algebraic set defined by a single equation. *Journal of Complexity*, 16(4):716–750, 2000.

[69] M. Safey El Din. *RAGLib (Real Algebraic Geometry Library), Maple Package*. http://www-polsys.lip6.fr/~safey/RAGLib/.

[70] M. Safey El Din. Testing sign conditions on a multivariate polynomial and applications. *Mathematics in Computer Science*, 1(1):177–207, 2007.

[71] M. Safey El Din and E. Schost. Polar varieties and computation of one point in each connected component of a smooth real algebraic set. In J. Sendra, editor, *International Symposium on Symbolic and Algebraic Computation 2003 - ISSAC'2003, Philadelphie, USA*, pages 224–231. ACM Press, aug 2003.

[72] M. Safey El Din and E. Schost. Properness defects of projections and computation of at least one point in each connected component of a real algebraic set. *Discrete and Computational Geometry*, 32(3):417–430, 2004.

[73] M. Safey El Din and L. Zhi. Computing rational points in convex semialgebraic sets and sum of squares decompositions. *SIAM Journal on Optimization*, 20(6):2876–2889, Sept. 2010.

[74] C. Scheiderer. Descending the ground field in sums of squares representations. *eprint arXiv:1209.2976v2*, 09/2012.

[75] C. Scheiderer. Positivity and sums of squares: A guide to recent results. In M. Putinar and S. Sullivant, editors, *Emerging Applications of Algebraic Geometry*, volume 149 of *The IMA Volumes in Mathematics and its Applications*, pages 271–324. Springer New York, 2009.

[76] J. F. Sturm. Using SeDuMi 1.02, a MATLAB toolbox for optimization over symmetric cones. *Optimization Methods and Software*, 11/12:625–653, 1999. URL: http://sedumi.mcmaster.ca.

[77] M. Todd. Semidefinite optimization. *Acta Numerica*, 10:515–560, 2001.

[78] K.-C. Toh, M. Todd, and R. Tütüncü. SDPT3 - a matlab software package for semidefinite programming. *Optimization Methods and Software*, 11:545–581, 1998.

[79] L. Vandenberghe and S. Boyd. Semidefinite programming. *SIAM Review*, 38(1):49–95, 1996.

[80] H. Waki, S. Kim, M. Kojima, and M. Muramatsu. Sums of squares and semidefinite program relaxations for polynomial optimization problems with structured sparsity[J]. *SIAM Journal on Optimization*, 17(1):218–242, 2006.

[81] H. Wolkowicz, R. Saigal, and L. E. Vandenberghe. *Handbook of Semidefinite Programming: Theory, Algorithms, and Applications*. Kluwer Academic, Boston, 2000.

[82] X.-Y. Zhao, D. Sun, and K.-C. Toh. A Newton-CG augmented Lagrangian method for semidefinite programming. *SIAM Journal on Optimization*, 20(4):1737–1765, 2010.

发表文章目录

[1] Qingdong Guo, Mohab Safey El Din, Lihong Zhi. Computing rational solutions of linear matrix inequalities. Proceedings of the 38th international symposium on Symbolic and algebraic computation, ISSAC '13, 197-204, ACM, 2013

ISSAC 2013 Distinguished Student Author Award

[2] Qingdong Guo, Mohab Safey El Din, Lihong Zhi. Computing exact solutions of linear matrix inequalities. Preprint.

简　　历

基本情况

郭庆东，男，1988 年 4 月出生于山东省成武县。

E-mail:qdguo@mmrc.iss.ac.cn

教育状况

2009 年 9 月至 2014 年 7 月，中国科学院数学与系统科学研究院，硕博连读研究生，专业：应用数学，导师：支丽红研究员。

2005 年 9 月至 2009 年 7 月，山东大学（威海）数学与统计学院，本科，专业：信息与计算科学。

会议活动

2013年6月26-29日，第38届国际符号和代数计算会议，做学术报告，波士顿

2013年4月19日，基于符号数值计算的可信计算研讨会，做学术报告，北京

2012年10月26-28日，第十届亚洲计算机数学会议，北京

2012年7月2-3日，基于符号数值计算的可信计算研讨会，做学术报告，北京

2011年11月26-28日，第四届全国计算机数学会议，广州大学

2011年7月17-20日，可信计算国际会议，广西南宁

2011年4-5月，中法代数与重写研讨会，清华大学

研究生阶段获得荣誉

2013年9月，　第十届数学与系统科学研究院院长奖学金优秀奖

2013年6月，　第38届国际符号和代数计算会议最佳学生论文奖

2013年5月，　2012-2013学年中国科学院大学三好学生

2011年5月，　2010-2011学年中国科学院研究生院三好学生

2011年5月，　中国科学院研究生院纪念中国共产党建党90周年党史知识竞赛三等奖

致　　谢

五年的硕博连读生活转瞬即逝，回首走过的岁月，心中倍感充实。论文即将完成之日，感慨良多。首先诚挚地感谢我的导师支丽红研究员，从论文选题，中期修改到最终定稿的过程中，自始至终都倾注着导师的心血。导师以严谨的治学之道，宽厚仁慈的胸怀，积极乐观的生活态度，为我树立了一辈子学习的典范，她的教诲与鞭策，将激励我在科学研究的道路上励精图治，开拓创新。

衷心感谢法国巴黎第六大学 Mohab Safey El Din 教授，在共同完成ISSAC 2013 文章期间，我得到了很多有用的帮助和建议。衷心感谢美国北卡罗来纳州立大学 Erich Kaltofen 教授，在第十届亚洲计算机数学会议期间，通过与他的交流和探讨，我获得了很多启发。

非常感谢数学机械化中心的各位老师，特别是吴文俊院士、高小山研究员、李洪波研究员、李子明研究员、王定康研究员、刘卓军研究员、程进三副研究员、袁春明副研究员、黄雷助理研究员、陈绍示助理研究员、李伟助理研究员，从他们那里我学习到了很多的知识。同时感谢周代珍老师、丁健敏老师、李佳老师的热心帮助。

感谢现在或曾经在数学机械化中心学习的杨争峰师兄、吴晓丽师姐、王怀富师兄、付国锋师兄、郭峰师兄、马玥师姐、梁野师兄、李喆师姐、李楠师兄、李子佳师兄、马晓栋师兄、吴宝峰师兄、戴照鹏师兄、黄冲师兄、刘琦师妹、刘越师弟、王础师弟、郝志伟师弟以及其他师弟师妹，感谢同在实验室学习的郭建新、孙志强、金凯、张凤、闵程、张晓明、李阁、岳志强、王继斌、康劲等同学的关心和帮助。同时感谢同在中科院数学院学习的本科校友陈兴师兄、杨家青师兄、宋洪婷、韩华伟、田雪、杨晓龙师弟、王腾师弟、刘源师弟及其他师弟师妹的关心和帮助。

最后, 谨以此文献给我挚爱的父母，他们在背后的默默支持是我前进的动力。在此祝愿他们身体健康，心情愉快!