中国科学: 数学 2021 年 第 51 卷 第 1 期: 67～86
SCIENTIA SINICA Mathematica
综 述

多项式组的特征分解

献给张景中、杨路教授 85 华诞

王东明[1,2,3*], 牟晨琪[1,2], 董日娜[1]

1. 北京航空航天大学数学科学学院, 数学、信息与行为教育部重点实验室, 北京 100191;
2. 北京航空航天大学大数据科学与脑机智能高精尖创新中心, 北京 100191;
3. Centre National de la Recherche Scientifique, Paris 75794, France
E-mail: dongming.wang@lip6.fr, chenqi.mou@buaa.edu.cn, rina.dong@buaa.edu.cn

收稿日期: 2020-02-01; 接受日期: 2020-03-30; 网络出版日期: 2020-12-31; * 通信作者
国家自然科学基金 (批准号: 11771034 和 11971050) 资助项目

摘要 任一多项式理想的特征对是指由该理想的约化字典序 Gröbner 基 $\mathcal{G}$ 和含于其中的极小三角列 $\mathcal{C}$ 构成的有序对 $(\mathcal{G},\mathcal{C})$. 当 $\mathcal{C}$ 为正则列或正规列时, 分别称特征对 $(\mathcal{G},\mathcal{C})$ 为正则的或正规的. 当 $\mathcal{G}$ 生成的理想与 $\mathcal{C}$ 的饱和理想相同时, 称特征对 $(\mathcal{G},\mathcal{C})$ 为强的. 一组多项式的 (强) 正则或 (强) 正规特征分解是指将该多项式组分解为有限多个 (强) 正则或 (强) 正规特征对, 使其满足特定的零点与理想关系. 本文简要回顾各种三角分解及相应零点与理想分解的理论和方法, 然后重点介绍 (强) 正则与 (强) 正规特征对和特征分解的性质, 说明三角列、Ritt 特征列和字典序 Gröbner 基之间的内在关联, 建立特征对的正则化定理以及正则、正规特征对的强化方法, 进而给出两种基于字典序 Gröbner 基计算、按伪整除关系分裂和构建、商除可除理想等策略的 (强) 正规与 (强) 正则特征分解算法. 这两种算法计算所得的强正规与强正则特征对和特征分解都具有良好的性质, 且能为输入多元多项式组的零点提供两种不同的表示. 本文还给出示例和部分实验结果, 用以说明特征分解方法及其实用性和有效性.

关键词 特征对 特征分解 三角分解 Gröbner 基 多项式组

MSC (2010) 主题分类 13P10, 13P15, 68W30

1 引言

以德国数学家 C. F. Gauß 命名的高斯消去法是线性方程组三角化的经典方法. 该方法的早期版本见诸于公元前 50 年前后成书的《九章算术》, 并出现在高斯 1809–1826 年间发表的与最小二乘法和地形测算有关的著作中 (参见文献 [1]). 高斯消去法应用广泛、中外流传, 是线性代数不可或缺的基本工具. 如何将这个方法推广到非线性方程组, 特别是多项式方程组, 这是众多数学家千百年来力图解决的

英文引用格式: Wang D M, Mou C Q, Dong R N. Characteristic decomposition of polynomial sets (in Chinese). Sci Sin Math, 2021, 51: 67–86, doi: 10.1360/SSM-2020-0025

© 2020《中国科学》杂志社

代数学难题. 从 14 世纪的朱世杰[2], 到法国的 Bézout[3] 等代数学家, 再到英国的 Sylvester-Macaulay 学派[4,5], 有关这个问题的研究源源不断, 但其结果都离问题的满意解决差之甚远. 直到 20 世纪 70 年代末, 我国数学家吴文俊[6] 提出了将多项式方程组化为特征列的整序原理, 进而给出了将任意多项式方程组分解为有限多个三角形方程组的机械化方法, 多项式方程组的三角化问题才获得完全解决. 吴文俊对中国数学史作过系统深入的研究, 熟知我国古代数学的发展脉络和贯穿其中的构造性、算法化和机械化思想. 他多次强调, 他的三角化方法, 也就是众所周知的吴方法, 其发现主要是受到了我国古代算法数学思想的启发, 虽然方法的描述和论证中使用的代数几何工具借鉴了美国数学家 Ritt[7] 在其有关微分代数的著作中所引进的特征列等概念 (因此吴方法也被称为吴 -Ritt 特征列方法). 该方法因最初在几何定理机器证明方面特别成功的应用 (参见文献 [8]), 后经吴文俊本人及其追随者的改进发展, 又被广泛用于解决形形色色的科学与工程问题, 激发了大量后续工作 (参见文献 [9–14]), 备受学术界关注.

吴方法的创建拉开了之后 40 年有关多项式系统三角化研究的序幕. 受其影响, 法国计算机代数学家 Lazard[15] 引进了多种三角列的概念, 并于 1991 年提出了首个不依赖特征列的三角分解方法. 稍后, Kalkbrener[16] 和王东明[17] 分别提出了多项式组的正则分解方法和多项式系统的良好与不可约三角分解方法, 其中正则链的概念与杨路和张景中[12] 独立引进的良性升链的概念等价. 这些方法与吴方法一起成为 20 世纪 90 年代三角列与三角分解研究高度活跃时期的 4 种代表性方法. 法国学者 Aubry 和 Moreno Maza[18] 实施了所有 4 种方法并对其进行了系统的实验与比较研究. 他们还与 Lazard 一起对这些方法计算所得的各种三角列和三角分解的性质以及它们之间的关系进行了深入的理论研究 (参见文献 [19]). 与此同时, 王东明[20,21] 又提出了将多项式系统分解为简单系统和正则系统的有效方法. 1999 年前后, 多篇后来有广泛影响的原创论文包括文献 [18–21] 和长篇辅导综述文献 [22] 相继发表, 从而将三角列理论和方法相关研究推向高潮.

在 2001 年至 2015 年的 15 年间, 三角列和三角分解的理论与方法持续发展, 算法和软件系统不断改进, 研究成果层出不穷. Moreno Maza、陈长波等进一步发展了正则链的算法与软件, 并提出了综合三角分解的概念与算法[23–25]. Dellière[26] 建立了王简单系统与动态可构造闭集之间的联系, Gerdt 等研究了与简单系统有关的 Thomas 分解, 给出了算法及程序实现, 并将其用于微分方程的符号分析[27,28]. 王东明、牟晨琪、李晓亮等提出了有限域上的简单分解算法[29,30], 高小山、黄震宇等研究了有限域上的三角分解方法并将其用于密码体系的安全性分析[31–33]. 高小山、袁春明等将特征列方法推广到了微分与差分情形[34,35].

求解多项式方程组的另一典型的代数方法是由 Buchberger[36] 于 1965 年提出的 Gröbner 基方法. Gröbner 基是多项式组生成理想的性质良好的有限生成元, 便于解决诸多与多项式理想有关的计算问题, 而字典序 Gröbner 基的结构和性质与三角列最为相似 (参见文献 [37,38]). Lazard 最早研究了二元多项式理想的字典序 Gröbner 基的结构, 之后其结果被推广至零维多元根理想的字典序 Gröbner 基 (参见文献 [39–41]). 而在 Gröbner 基与三角列的交叉研究方面, Lazard[42] 和 Dahan[43] 研究了零维情形二者之间的关系, 并提出了由字典序 Gröbner 基计算三角分解的算法. 2016 年, 王东明在文献 [44] 中揭示了 Ritt 特征列与字典序 Gröbner 基之间的内在关联, 由此建立了非正则情形字典序 Gröbner 基的结构定理, 并发现了文献 [19] 中构造 Ritt 特征列方法的致命错误. 这项工作不仅将非正则情形 Ritt 特征列的构造问题重置为公开问题, 而且导致了特征对概念的引入, 催生了本文作者有关多项式组特征分解的一系列研究工作 (参见文献 [45–48]).

任意理想的特征对是指由该理想的约化字典序 Gröbner 基 $\mathcal{G}$ 和含于其中的极小三角列 $\mathcal{C}$ (称为理想 $\langle\mathcal{G}\rangle$ 的 W 特征列) 构成的有序对 $(\mathcal{G},\mathcal{C})$. 当 W 特征列 $\mathcal{C}$ 为正则列或正规列时, 分别称特征对

$(\mathcal{G}, \mathcal{C})$ 为正则的或正规的. 当 Gröbner 基 $\mathcal{G}$ 生成的理想和 W 特征列 $\mathcal{C}$ 的饱和理想 $\mathrm{sat}(\mathcal{C})$ 相同时, 即 $\langle\mathcal{G}\rangle = \mathrm{sat}(\mathcal{C})$ 时, 称特征对 $(\mathcal{G}, \mathcal{C})$ 为强的. 一组多项式的 (强) 正则或 (强) 正规特征分解是指将该多项式组分解为有限多个 (强) 正则或 (强) 正规特征对, 使其满足特定的零点与理想关系. 本文是作者在特征分解方面研究工作的一个小结, 主要介绍特征对和特征分解的概念、性质、算法和实施. 在回顾三角列、三角系统和三角分解的基本概念和性质之后, 我们重新阐释特征列与特征对的概念, 揭示理想的特征对在正规情形与 Ritt 特征列的内在联系 (第 3.1 和 3.2 小节), 建立特征对的正则化定理和由正规或正则特征对到强正规或强正则特征对的强化方法 (第 3.3 和 3.4 小节), 介绍基于约化字典序 Gröbner 基内在结构关系的正规特征分解算法和基于可除分支构建与理想商除的强正则特征分解算法 (第 4 节) 以及两种算法在计算机代数软件 Maple 中的实施和部分实验结果, 用以说明特征分解方法的有效性和实用价值 (第 5 节).

多项式组的特征分解为符号计算领域 Gröbner 基和三角列两大核心方法的融合架起了优势互补的桥梁, 为揭示二者之间的内在关联开辟了新的途径: (强) 特征对提供了同一理想基于 Gröbner 基和三角列的两种不同表示方式, 约化字典序 Gröbner 基中多项式之间的伪整除关系 (属于三角列方法的研究范畴) 是正规特征分解算法设计的理论基础, 特征对的强化是通过计算 W 特征列饱和理想的 Gröbner 基再提取 W 特征列的方式实现的, 等等. 特征分解也为研究理想的几何性质提供了良好的工具: 强正规和强正则特征分解对应的都是代数簇的非混合等维分解, 即每个特征对中的理想对应的代数簇都具有相同参数且是等维的, 而其维数由 W 特征列中多项式的个数直接确定. 实验结果表明, 基于可除分支构建与理想商除的正则特征分解算法可以有效地控制特征对的数目, 它比常规正则分解算法计算所得的正则分解的分支数要少. 特征分解因其具有这些良好性质而有别于传统的 Gröbner 基计算和三角分解, 它直接提供了多项式组的更多代数与几何信息以及表示与研究这些信息的途径, 是符号计算与计算代数几何领域中的新兴研究方向.

2 多项式系统的三角分解

2.1 基本概念与记号

设 $\mathbb{K}$ 是特征为 0 的数域, $\mathbb{K}[\boldsymbol{x}]$ 为 $\mathbb{K}$ 上关于变元 $x_1, x_2, \ldots, x_n$ 的多元多项式环, 取定变元序为 $x_1 < x_2 < \cdots < x_n$. 对于任意多项式 $F \in \mathbb{K}[\boldsymbol{x}]$, 称 F 中出现的最大变元为 F 的导元, 记作 $\mathrm{lv}(F)$. 令 $\mathrm{lv}(F) = x_i$, 则多项式 F 可以写作

$$F = Ix_i^k + R,$$

其中

$$I \in \mathbb{K}[\boldsymbol{x}_{i-1}] := \mathbb{K}[x_1, \ldots, x_{i-1}], \quad R \in \mathbb{K}[\boldsymbol{x}_i], \quad \deg(R, x_i) < k = \deg(F, x_i).$$

我们将 F 关于 $\mathrm{lv}(F)$ 的最高次数项的系数 I 称作 F 的初式, 记为 $\mathrm{ini}(F)$.

定义 2.1 由 $\mathbb{K}[\boldsymbol{x}]$ 中的多项式构成的有序集 $[T_1, T_2, \ldots, T_r]$ 称为三角列, 如果 $T_1, T_2, \ldots, T_r \notin \mathbb{K}$ 且 $\mathrm{lv}(T_1) < \mathrm{lv}(T_2) < \cdots < \mathrm{lv}(T_r)$.

对任意三角列 $\mathcal{T} = [T_1, T_2, \ldots, T_r] \subset \mathbb{K}[\boldsymbol{x}]$, 记 $\mathrm{lv}(\mathcal{T}) := \{\mathrm{lv}(T) \mid T \in \mathcal{T}\}$, $\mathrm{ini}(\mathcal{T}) := \{\mathrm{ini}(T) \mid T \in \mathcal{T}\}$, $\mathcal{T}_i := [T_1, T_2, \ldots, T_i]$ $(i = 1, \ldots, r)$. 称变元 $\{x_1, x_2, \ldots, x_n\} \setminus \mathrm{lv}(\mathcal{T})$ 为 $\mathcal{T}$ 的参数. 由 $\mathbb{K}[\boldsymbol{x}]$ 中的三角列 $\mathcal{T} = [T_1, T_2, \ldots, T_r]$ 定义的饱和理想为 $\mathrm{sat}(\mathcal{T}) := \langle\mathcal{T}\rangle : J^\infty$, 其中 $J = \mathrm{ini}(T_1)\,\mathrm{ini}(T_2)\cdots\mathrm{ini}(T_r)$.

设 $P, Q \in \mathbb{K}[\boldsymbol{x}]$ 为非零多项式, 且 $Q \notin \mathbb{K}$. 称 P 对 Q 为约化的, 如果 $\deg(P, \mathrm{lv}(Q)) < \deg(Q, \mathrm{lv}(Q))$. 称三角列 $\mathcal{T} \subset \mathbb{K}[\boldsymbol{x}]$ 为约化的, 如果对任意 $T, T' \in \mathcal{T}$ 都有 $\deg(T, \mathrm{lv}(T')) < \deg(T', \mathrm{lv}(T'))$. 若 $\mathcal{T}$ 只包

含一个非零常数, 或 $\mathcal{T}$ 为约化的三角列, 则称 $\mathcal{T}$ 为升列. 特别地, 如果 $\mathcal{T}$ 中不包含非零常数, 那么 $\mathcal{T}$ 又被称为非平凡升列.

对 $\mathbb{K}[\boldsymbol{x}]$ 中的任意多项式 P、Q 和三角列 $\mathcal{T}=[T_1,\ldots,T_r]$, 将 P 和 Q 关于变元 x_i 的伪余式和结式分别记为 $\mathrm{prem}(P,Q,x_i)$ 和 $\mathrm{res}(P,Q,x_i)$, 而将 F 关于 $\mathcal{T}$ 的伪余式和结式分别记为

$$\begin{aligned}&\mathrm{prem}(P,\mathcal{T}):=\mathrm{prem}(\mathrm{prem}(\ldots,\mathrm{prem}(F,T_r,\mathrm{lv}(T_r)),\ldots),T_1,\mathrm{lv}(T_1)),\\&\mathrm{res}(P,\mathcal{T}):=\mathrm{res}(\mathrm{res}(\ldots,\mathrm{res}(F,T_r,\mathrm{lv}(T_r)),\ldots),T_1,\mathrm{lv}(T_1)).\end{aligned}$$

显然, $\mathrm{prem}(P,Q,\mathrm{lv}(Q))$ 对 Q 是约化的, 而 $\mathrm{prem}(P,\mathcal{T})$ 对 $\mathcal{T}$ 的每个多项式均为约化的.

不同类型的三角列包括特征列、正则列、正规列、简单列和不可约三角列等. 首先介绍其中的正则列和正规列, 而 Ritt 特征列、简单列和不可约三角列等概念在后面各节中再进行介绍.

定义 2.2 设 $\mathcal{T}=[T_1,\ldots,T_r]$ 为 $\mathbb{K}[\boldsymbol{x}]$ 中的三角列. 若对任意 $1<i\leqslant r$ 均有 $\mathrm{res}(\mathrm{ini}(T_i),\mathcal{T}_{i-1})\neq 0$, 则称 $\mathcal{T}$ 为正则的或为正则列; 若 $\mathrm{ini}(T_1),\ldots,\mathrm{ini}(T_r)$ 仅含有 $\mathcal{T}$ 的参数, 则称三角列 $\mathcal{T}$ 为正规的或为正规列.

正则列的上述定义源自文献 [12]. 不难证明, 任意正规列都是正则的, 然而正则列却不一定是正规的.

称 $\mathbb{K}[\boldsymbol{x}]$ 中的多项式组 $\mathcal{P}$ 和 $\mathcal{Q}$ 构成的有序对 $[\mathcal{P},\mathcal{Q}]$ 为 $\mathbb{K}[\boldsymbol{x}]$ 中的多项式系统. 定义 $\mathbb{K}[\boldsymbol{x}]$ 中多项式系统 $[\mathcal{P},\mathcal{Q}]$ 的零点集 $\mathsf{Z}(\mathcal{P}/\mathcal{Q})$ 如下:

$$\mathsf{Z}(\mathcal{P}/\mathcal{Q}):=\{\bar{\boldsymbol{x}}\in\bar{\mathbb{K}}^n\mid P(\bar{\boldsymbol{x}})=0,Q(\bar{\boldsymbol{x}})\neq 0,\forall\,P\in\mathcal{P},Q\in\mathcal{Q}\},$$

其中 $\bar{\mathbb{K}}$ 为 $\mathbb{K}$ 的代数闭包. 对于 $\mathcal{Q}=\emptyset$ 的特殊情形, 将 $\mathsf{Z}(\mathcal{P}/\emptyset)$ 简记为 $\mathsf{Z}(\mathcal{P})$. 设 $[\mathcal{T},\mathcal{U}]$ 为 $\mathbb{K}[\boldsymbol{x}]$ 中的多项式系统. 如果 $\mathcal{T}$ 是三角列, 且对任意 $I\in\mathrm{ini}(\mathcal{T})$ 和 $\bar{\boldsymbol{x}}\in\mathsf{Z}(\mathcal{T}/\mathcal{U})$ 都有 $I(\bar{\boldsymbol{x}})\neq 0$, 则称 $[\mathcal{T},\mathcal{U}]$ 为三角系统.

定义 2.3 称 $\mathbb{K}[\boldsymbol{x}]$ 中的三角系统 $[\mathcal{T},\mathcal{U}]$ 为正则系统, 如果 $\mathrm{lv}(\mathcal{T})\cap\mathrm{lv}(\mathcal{U})=\emptyset$, 且对任意以 x_i 为主变元的 $I\in\mathrm{ini}(\mathcal{U})$ 和 $\bar{\boldsymbol{x}}\in\mathsf{Z}(\mathcal{T}_{<x_i}/\mathcal{U}_{<x_i})$ 都有 $I(\bar{\boldsymbol{x}})\neq 0$, 其中 $\mathcal{T}_{<x_i}:=\{T\in\mathcal{T}\mid\mathrm{lv}(T)<x_i\}$ (而 $\mathcal{U}_{<x_i}$ 类似定义).

可以证明, $\mathbb{K}[\boldsymbol{x}]$ 中的三角列 $\mathcal{T}$ 为正则列当且仅当存在多项式组 $\mathcal{U}\subset\mathbb{K}[\boldsymbol{x}]$ 使得 $[\mathcal{T},\mathcal{U}]$ 构成正则系统 (参见文献 [49, 第 5.1 小节]). 设 $[\mathcal{T},\mathcal{U}]$ 为 $\mathbb{K}[\boldsymbol{x}]$ 中的三角系统, 其中 $\mathcal{T}=[T_1,\ldots,T_r]$. 称 $\boldsymbol{\xi}=(\xi_1,\ldots,\xi_n)$ 为 $[\mathcal{T},\mathcal{U}]$ 的正则零点, 如果对于任意 $T\in\mathcal{T}$ 和 $U\in\mathcal{U}$ 有 $T(\boldsymbol{\xi})=0$, $U(\boldsymbol{\xi})\neq 0$, 且 $\boldsymbol{\xi}$ 满足形式

$$\boldsymbol{\xi}=(x_1,\ldots,x_{p_1-1},\xi_{p_1},x_{p_1+1},\ldots,x_{p_r-1},\xi_{p_r},x_{p_r+1},\ldots,x_n)\in\tilde{\mathbb{K}}^n,$$

其中 $x_{p_i}=\mathrm{lv}(T_i)$, $i=1,\ldots,r$, 而 $\tilde{\mathbb{K}}$ 是将参数 x_k 视为超越元、将 ξ_{p_i} $(1\leqslant i\leqslant r)$ 视为代数元依次添加到 $\mathbb{K}$ 中得到的扩域. 将 $[\mathcal{T},\mathcal{U}]$ 的所有正则零点构成的集合记为 $\mathrm{RZ}(\mathcal{T}/\mathcal{U})$. 可以证明, 对于 $\mathbb{K}[\boldsymbol{x}]$ 中的任意两个正则系统 $[\mathcal{T},\mathcal{U}_1]$ 和 $[\mathcal{T},\mathcal{U}_2]$, 都有 $\mathrm{RZ}(\mathcal{T}/\mathcal{U}_1)=\mathrm{RZ}(\mathcal{T}/\mathcal{U}_2)$, 因此, 正则系统 $[\mathcal{T},\mathcal{U}]$ 的正则零点集也称为 $\mathcal{T}$ 的正则零点集, 记为 $\mathrm{RZ}(\mathcal{T})$ (参见文献 [49, 命题 5.1.1]).

2.2 多项式组的特征列与零点分解

Ritt [7] 首先引进了特征列的概念, 特征列是一种特殊的三角列. 为了研究非空多项式组的零点集, 吴文俊在理论、算法、效率和应用等方面极大地发展了特征列方法 [8,9].

定义 2.4 设 $\mathcal{P}$ 为 $\mathbb{K}[\boldsymbol{x}]$ 中任意给定的有限多项式集合. 称升列 $\mathcal{C} \subseteq \mathbb{K}[\boldsymbol{x}]$ 为理想 $\langle \mathcal{P} \rangle$ 的 Ritt 特征列, 如果 $\mathcal{C} \subseteq \langle \mathcal{P} \rangle$, 并且对所有多项式 $P \in \langle \mathcal{P} \rangle$ 都有 $\operatorname{prem}(P, \mathcal{C}) = 0$. 若升列 $\tilde{\mathcal{C}} \subseteq \mathbb{K}[\boldsymbol{x}]$ 满足 $\tilde{\mathcal{C}} \subseteq \langle \mathcal{P} \rangle$ 且对所有多项式 $P \in \mathcal{P}$ 都有 $\operatorname{prem}(P, \tilde{\mathcal{C}}) = 0$, 则称 $\tilde{\mathcal{C}}$ 为多项式集合 $\mathcal{P}$ 的特征列.

理想 $\langle \mathcal{P} \rangle$ 的 Ritt 特征列一般定义为所有包含于 $\langle \mathcal{P} \rangle$ 的升列中秩最小者. 依据文献 [50, 定理 5.5.3], Ritt 原始的特征列定义与上述 Ritt 特征列定义等价. 多项式组 $\mathcal{P}$ 的特征列这一概念则是由吴文俊引进的, 因而多项式组的特征列也被称为吴特征列. 显然, 吴特征列的要求比 Ritt 特征列的要求弱, 这使得其计算更为便捷. 同时, 吴特征列的零点与多项式组的零点之间有如下关系, 它们是利用特征列进行几何定理机器证明的理论基础.

命题 2.1 (吴特征列的零点关系 [49, 命题 2.2.2]) 设非平凡升列 $\mathcal{C} = [C_1, \ldots, C_r]$ 为 $\mathcal{P} \subseteq \mathbb{K}[\boldsymbol{x}]$ 的吴特征列, 令 $\mathcal{P}_i = \mathcal{P} \cup \{\operatorname{ini}(C_i)\}$ $(i = 1, \ldots, r)$, 而 $\mathcal{I} = \operatorname{ini}(\mathcal{C})$, 则下列关系成立:

$$\mathsf{Z}(\mathcal{C}/\mathcal{I}) \subseteq \mathsf{Z}(\mathcal{P}) \subseteq \mathsf{Z}(\mathcal{C}), \tag{2.1}$$

$$\mathsf{Z}(\mathcal{C}/\mathcal{I}) = \mathsf{Z}(\mathcal{P}/\mathcal{I}), \tag{2.2}$$

$$\mathsf{Z}(\mathcal{P}) = \mathsf{Z}(\mathcal{C}/\mathcal{I}) \cup \bigcup_{i=1}^{r} \mathsf{Z}(\mathcal{P}_i). \tag{2.3}$$

吴文俊 [9] 不仅提出了特征列的概念, 还给出了由任意有限多项式集合计算其特征列的算法. 在计算得到多项式集合 $\mathcal{P}$ 的特征列 $\mathcal{C}$ 后, 零点关系 $\mathsf{Z}(\mathcal{P}_i \cup \mathcal{C}) = \mathsf{Z}(\mathcal{P}_i)$ 成立. 考虑到命题 2.1 中的零点关系 (2.3), 为了计算 $\mathsf{Z}(\mathcal{P})$, 我们可以将 $\mathcal{P}_i \cup \mathcal{C}$ 作为新的 $\mathcal{P}$ 计算其特征列, 并重复此步骤. 这一过程必然终止, 而我们将得到有限多个特征列 $\mathcal{C}_1, \ldots, \mathcal{C}_s$ 使得零点关系

$$\mathsf{Z}(\mathcal{P}) = \bigcup_{i=1}^{s} \mathsf{Z}(\mathcal{C}_i / \operatorname{ini}(\mathcal{C}_i))$$

成立. 上述过程提供了多项式组 $\mathcal{P}$ 基于特征列的零点分解方法, 它是下面将要介绍的三角分解方法中最典型的一种. 有关特征列方法的其他细节, 可参见文献 [8,10,11,38,51–53].

2.3 多项式系统的三角分解与不可约三角分解

对 $\mathbb{K}[\boldsymbol{x}]$ 中任意多项式系统 $[\mathcal{F}, \mathcal{G}]$ 进行三角分解, 是指计算有限多个三角系统 $[\mathcal{T}_1, \mathcal{U}_1], [\mathcal{T}_2, \mathcal{U}_2], \ldots, [\mathcal{T}_s, \mathcal{U}_s]$, 使得如下零点关系成立:

$$\mathsf{Z}(\mathcal{F}/\mathcal{G}) = \bigcup_{i=1}^{s} \mathsf{Z}(\mathcal{T}_i/\mathcal{U}_i).$$

多项式组的三角分解是多项式系统三角分解的特殊情形, 即对任意多项式组 $\mathcal{F} \subseteq \mathbb{K}[\boldsymbol{x}]$ 计算有限多个三角列 $\mathcal{T}_1, \mathcal{T}_2, \ldots, \mathcal{T}_s \subset \mathbb{K}[\boldsymbol{x}]$, 使得

$$\mathsf{Z}(\mathcal{F}) = \bigcup_{i=1}^{s} \mathsf{Z}(\mathcal{T}_i / \operatorname{ini}(\mathcal{T}_i)).$$

由于三角列结构特殊、便于迭代求解, 因此, 通过三角分解可以将多项式方程组 $\mathcal{F} = 0$ 的求解问题转化为有限多个由三角列定义的多项式方程组 $\mathcal{T}_1 = 0, \ldots, \mathcal{T}_s = 0$ 的求解问题, 从而使计算简化. 三角系统有正规、正则、简单和不可约等不同类型, 有关它们的基本性质与计算方法, 可参见文献 [49,52]. 其中, 不可约三角系统是正则系统的特殊情形, 其性质和计算方法主要由吴文俊和王东明 [8,17,21] 给出. 不可约三角系统是代数扩域域塔的自然表示, 其计算主要基于代数扩域上多项式的因子分解.

定义 2.5 设 $\mathcal{T}=[T_1,\ldots,T_r]$ 为 $\mathbb{K}[\boldsymbol{x}]$ 中的正则列, $\boldsymbol{u}$ 为 $\mathcal{T}$ 的全部参数, 而令 $y_i=\mathrm{lv}(T_i)$ $(i=1,\ldots,r)$. 不失一般性, 假设变元序为 $\boldsymbol{u}<y_1<\cdots<y_r$, 则 $\mathcal{T}$ 可写成 $[T_1(\boldsymbol{u},y_1),\ldots,T_r(\boldsymbol{u},y_1,\ldots,y_r)]$. 称 $\mathcal{T}$ 为不可约三角列, 如果下列条件成立:

(1) 若 $r=1$, 则 $T_1(\boldsymbol{u},y_1)$ 在域 $\mathbb{K}(\boldsymbol{u})$ 上不可约.

(2) 若 $r>1$, 则

(i) $T_1(\boldsymbol{u},y_1)$ 在域 $\mathbb{K}(\boldsymbol{u})$ 上不可约;

(ii) 假定 $\mathcal{T}_{k-1}:=[T_1,\ldots,T_{k-1}]$ 为不可约三角列 $(1<k\leqslant r)$, 那么对任意 $(\boldsymbol{u},\overline{y}_1,\ldots,\overline{y}_{k-1})\in\mathrm{RZ}(\mathcal{T}_{k-1})$, $T_k(\boldsymbol{u},\overline{y}_1,\ldots,\overline{y}_{k-1},y_k)$ 在域 $\mathbb{K}(\boldsymbol{u})(\overline{y}_1,\ldots,\overline{y}_{k-1})$ 上不可约.

设 $[\mathcal{T},\mathcal{U}]$ 为 $\mathbb{K}[\boldsymbol{x}]$ 中的正则系统. 若 $\mathcal{T}$ 为 $\mathbb{K}[\boldsymbol{x}]$ 中的不可约三角列, 则 $[\mathcal{T},\mathcal{U}]$ 称为不可约三角系统. $\mathbb{K}[\boldsymbol{x}]$ 中多项式系统 $[\mathcal{P},\mathcal{Q}]$ 的不可约三角分解是指计算有限多个不可约三角系统 $[\mathcal{T}_1,\mathcal{U}_1],\ldots,[\mathcal{T}_s,\mathcal{U}_s]$ 使得

$$\mathsf{Z}(\mathcal{P}/\mathcal{Q})=\bigcup_{i=1}^{s}\mathsf{Z}(\mathcal{T}_i/\mathcal{U}_i). \tag{2.4}$$

定理 2.1 ([49, 定理 4.3.11]) 设 $[\mathcal{T}_1,\mathcal{U}_1],\ldots,[\mathcal{T}_s,\mathcal{U}_s]$ 为 $\mathbb{K}[\boldsymbol{x}]$ 中多项式系统 $[\mathcal{P},\mathcal{Q}]$ 的不可约三角分解, 则下列结论成立:

(1) 对任意 $1\leqslant i\leqslant s$ 和任意 $P\in\mathcal{P}$, 都有 $\mathrm{prem}(P,\mathcal{T}_i)=0$;

(2) $\mathsf{Z}(\mathcal{P}/\mathcal{Q})=\bigcup_{i=1}^{s}\mathsf{Z}(\mathcal{T}_i/\mathrm{ini}(\mathcal{T}_i)\cup\mathcal{Q})$.

有关不可约三角系统的更多性质和不可约三角分解算法, 可参见文献 [49, 第 4 章].

2.4 代数簇的不可约与等维分解及三角列表示

代数几何中的 Hilbert 强零点定理建立了根理想与代数簇之间的一一对应关系. 从代数角度来看, 对于 Noether 环 $\mathcal{R}$ 中任一个给定的理想 $\mathfrak{a}$, 均存在有限多个素理想 $\mathfrak{p}_1,\ldots,\mathfrak{p}_r\subseteq\mathcal{R}$ 使得 $\sqrt{\mathfrak{a}}=\mathfrak{p}_1\cap\cdots\cap\mathfrak{p}_r$, 且对任意 $i\neq j$ 都有 $\mathfrak{p}_i\not\subseteq\mathfrak{p}_j$. 根据根理想与代数簇以及素理想与不可约代数簇之间的对应关系, 从几何角度来看, 上述根理想的素分解可以翻译为如下结论.

命题 2.2 ([38, 定理 4.6.4]) 设 $\mathbb{K}$ 为代数闭域, $V\subseteq\mathbb{K}^n$ 为非空代数簇, 则存在有限多个不可约代数簇 $V_1,\ldots,V_s\subseteq\mathbb{K}^n$ 使得 $V=V_1\cup\cdots\cup V_r$, 且对任意 $i\neq j$ 都有

$$V_i\not\supseteq V_j.$$

上述命题中的 $V=V_1\cup\cdots\cup V_r$ 称为代数簇 V 的不可约分解, 而 $V_1,\ldots,V_r$ 称为 V 的非冗余不可约分支. 若不记次序, 代数簇的非冗余不可约分支是唯一确定的. 就代数簇的表示而言, Gröbner 基方法和三角列方法都为其提供了构造性工具. 下面主要介绍代数簇的三角列表示.

命题 2.3 ([49, 定理 6.2.14]) 设 $\mathcal{C}\subseteq\mathbb{K}[\boldsymbol{x}]$ 为不可约三角列, 则 $\mathrm{sat}(\mathcal{C})$ 为 $\mathbb{K}[\boldsymbol{x}]$ 中的素理想, 进而 $\mathsf{Z}(\mathrm{sat}(\mathcal{C}))$ 为不可约代数簇.

由此可知, 对于任意一个由多项式组 $\mathcal{P}$ 定义的代数簇 $\mathsf{Z}(\mathcal{P})\subseteq\mathbb{K}^n$, 都可以通过计算 $\mathcal{P}$ 的不可约三角分解来构造 $\mathsf{Z}(\mathcal{P})$ 的不可约分解.

除此之外, 代数簇作为一类几何对象, 维数是其重要的几何特征. 对于代数簇 $V\subseteq\mathbb{K}^n$, 如果 V 的所有非冗余不可约分支都具有相同的维数, 那么称 V 为等维代数簇. 又设代数簇 V 具有形如 $\bigcup_{i=1}^{s}V_i$ 的分解. 若所有 V_i 均为等维代数簇, 则称该分解为 V 的等维分解. 构造代数簇的等维分解同样可以通过三角分解来实现.

对任意多项式组 $\mathcal{P} \subseteq \mathbb{K}[\boldsymbol{x}]$, 都可以计算有限多个正则系统 $[\mathcal{T}_1,\mathcal{U}_1],\ldots,[\mathcal{T}_s,\mathcal{U}_s]$ 使得

$$\mathsf{Z}(\mathcal{P}) = \bigcup_{i=1}^{s} \mathsf{Z}(\mathrm{sat}(\mathcal{T}_i)) \tag{2.5}$$

构成代数簇 $\mathsf{Z}(\mathcal{P})$ 的一个等维分解. 特别在 (2.5) 中, 对任意 i, $\mathsf{Z}(\mathrm{sat}(\mathcal{T}_i))$ 都是维数为 $n-|\mathcal{T}_i|$ 的等维代数簇. 等维性是正则分解的重要几何特征之一.

2.5 多项式系统的正则分解与简单分解

正则系统的概念由王东明 [21] 提出, 他还证明了正则系统的若干良好性质. 设 $\mathcal{T} = [T_1,\ldots,T_r]$ 为 $\mathbb{K}[\boldsymbol{x}]$ 中的任意正则列, 则下述结论成立: $\mathcal{T}$ 的零点集非空; 对任意 $i=1,\ldots,r$, 初式 $\mathrm{ini}(T_i)$ 在商环

$$\mathbb{K}[\boldsymbol{x}]/\,\mathrm{sat}([T_1,\ldots,T_{i-1}])$$

中的像均可逆; $\mathcal{T}$ 具有投影性质. 顺便指出, 投影性质是一般三角系统所不具备的性质.

简单系统是一类特殊的正则系统, 其概念源自 J. M. Thomas 在微分代数领域的工作, 后来王东明 [20,49] 给出了简单系统的性质和计算方法. 由于其中的多项式具有无平方的性质, 简单系统适用于计算多项式系统 (不含重数) 的解的个数.

定义 2.6 $\mathbb{K}[\boldsymbol{x}]$ 中的正则系统 $[\mathcal{T},\mathcal{U}]$ 称为简单系统, 如果 $\mathcal{U}$ 为三角列, 且对任意主变元为 x_p 的多项式 $P \in \mathcal{T}\cup\mathcal{U}$ 和 $\bar{\boldsymbol{x}}_{p-1} \in \mathsf{Z}(\mathcal{T}_{<x_p}/\mathcal{U}_{<x_p})$, $P(\tilde{\boldsymbol{x}}_{p-1},x_p)$ 都是无平方的. 三角列 $\mathcal{T} \subseteq \mathbb{K}[\boldsymbol{x}]$ 称为简单列, 如果存在三角列 $\mathcal{U}$, 使得 $[\mathcal{T},\mathcal{U}]$ 为简单系统.

对 $\mathbb{K}[\boldsymbol{x}]$ 中的多项式系统 $[\mathcal{P},\mathcal{Q}]$, 由正则 (或简单) 系统 $[\mathcal{T}_1,\mathcal{U}_1],\ldots,[\mathcal{T}_s,\mathcal{U}_s]$ 构成的有限集合称为 $[\mathcal{P},\mathcal{Q}]$ 的一个正则 (或简单) 分解, 如果

$$\mathsf{Z}(\mathcal{P}/\mathcal{Q}) = \bigcup_{i=1}^{s} (\mathsf{Z}(\mathcal{T}_i/\mathcal{U}_i).$$

此外, 多项式系统 $[\mathcal{P},\emptyset]$ 的正则 (或简单) 分解也被称为 $\mathcal{P}$ 的正则 (或简单) 分解.

本节简单介绍了正则系统和简单系统的基本概念, 有关它们的更多性质以及对任意多项式系统进行正则和简单分解的算法, 可参见文献 [49,52].

3 多项式组的特征对和特征分解

3.1 Gröbner 基、W 特征列与特征对

Gröbner 基的概念最初由 Buchberger [36] 于 1965 年提出. 一个多项式理想的 Gröbner 基是该理想的一组具有良好性质的生成元, 且可以从理想的任意有限生成元计算得出. Gröbner 基可用于解决诸多与多项式理想有关的问题, 是解决理想的成员判定问题与多项式方程组求解问题的有效工具.

用 $\mathcal{T}(\boldsymbol{x})$ 记 $\mathbb{K}$ 上变元 $x_1,\ldots,x_n$ 构成的所有项组成的集合. 如果集合 $\mathcal{T}(\boldsymbol{x})$ 上的全序关系 $<$ 是良序, 并且对任意 $\boldsymbol{\mu}_1,\boldsymbol{\mu}_2,\boldsymbol{\mu} \in \mathcal{T}(\boldsymbol{x})$, $\boldsymbol{\mu}_1 < \boldsymbol{\mu}_2$ 都可以导出 $\boldsymbol{\mu}\boldsymbol{\mu}_1 < \boldsymbol{\mu}\boldsymbol{\mu}_2$, 那么称 $<$ 为 $\mathbb{K}[\boldsymbol{x}]$ 的一个项序. 设 $F \in \mathbb{K}[\boldsymbol{x}]$ 为非零多项式, $<$ 为 $\mathbb{K}[\boldsymbol{x}]$ 上的项序, 称多项式 F 关于 $<$ 最大的项为 F 的首项, 用 $\mathrm{lt}(F)$ 表示.

定义 3.1 集合 $\mathcal{T}(\boldsymbol{x})$ 上的项序字典序 $<_{\mathrm{lex}}$ 定义如下: 对任意 $\boldsymbol{x}^{\boldsymbol{\alpha}} := x_1^{\alpha_1}\cdots x_n^{\alpha_n}$, $\boldsymbol{x}^{\boldsymbol{\beta}} := x_1^{\beta_1}\cdots x_n^{\beta_n}$ $\in \mathcal{T}(\boldsymbol{x})$, $\boldsymbol{x}^{\alpha} <_{\mathrm{lex}} \boldsymbol{x}^{\beta}$ 当且仅当存在 i $(1 \leqslant i \leqslant n)$ 使得 $\alpha_j = \beta_j$ $(i+1 \leqslant j \leqslant n)$ 且 $\alpha_i < \beta_i$.

定义 3.2 给定 $\mathbb{K}[\boldsymbol{x}]$ 上的项序 $<$, 设 $\mathfrak{I} \subset \mathbb{K}[\boldsymbol{x}]$ 为理想. 若 $\mathfrak{I}$ 的有限子集 $\mathcal{G} = \{G_1, G_2, \ldots, G_s\}$ 满足

$$\langle \mathrm{lt}(G_1), \ldots, \mathrm{lt}(G_s) \rangle = \langle \mathrm{lt}(\mathfrak{I}) \rangle,$$

则称 $\mathcal{G}$ 为 $\mathfrak{I}$ 关于 $<$ 的 Gröbner 基.

本文主要考虑多项式理想的约化字典序 Gröbner 基, 这是因为任一理想的约化 Gröbner 基唯一且字典序 Gröbner 基的消元性质保证了变元的分离. 如无特别说明, 本文以后所使用的 Gröbner 基均指约化字典序 Gröbner 基. 从任意多项式理想的约化字典序 Gröbner 基中, 我们都可以按照如下定义提取出一种特殊的三角列.

定义 3.3 设 $\mathcal{P}$ 为 $\mathbb{K}[\boldsymbol{x}]$ 中的任意多项式组, $\mathcal{G}$ 为其生成的理想 $\langle \mathcal{P} \rangle$ 的约化 Gröbner 基. 将 $\mathcal{G}$ 中的所有多项式分成不同集合, 使得每个集合中多项式的导元相同. 再从每个集合中取出关于字典序最小的多项式, 并将这些多项式按照给定变元序从小到大排列后得到的集合称为理想 $\langle \mathcal{P} \rangle$ 的 W 特征列.

命题 3.1 ([44, 命题 3.1]) 对任意多项式理想 $\langle \mathcal{P} \rangle \subseteq \mathbb{K}[\boldsymbol{x}]$ 的 W 特征列 $\mathcal{C}$, 下列结论成立:

(1) 对任意 $P \in \mathcal{P}$, $\mathrm{prem}(P, \mathcal{C}) = 0$;

(2) $\langle \mathcal{C} \rangle \subseteq \langle \mathcal{P} \rangle \subseteq \mathrm{sat}(\mathcal{C})$;

(3) $\mathsf{Z}(\mathcal{C}/\mathrm{ini}(\mathcal{C})) \subseteq \mathsf{Z}(\mathcal{P}) \subseteq \mathsf{Z}(\mathcal{C})$.

下述结构定理揭示了任意维多项式理想的 W 特征列中特定多项式之间 (从而也是 Gröbner 基中的多项式之间) 的伪整除关系. 这些伪整除关系使得我们可以采取有效的分裂策略进行正规特征分解 (详见本文第 4.1 小节).

定理 3.1 ([44, 定理 3.9]) 设 $\mathcal{C} = [C_1, \ldots, C_r]$ 为 $\langle \mathcal{P} \rangle \subseteq \mathbb{K}[\boldsymbol{x}]$ 的 W 特征列. 若 $\mathcal{C}$ 非正规, 则存在整数 k $(1 \leqslant k \leqslant r)$ 使得 $[C_1, \ldots, C_k]$ 正规并且 $[C_1, \ldots, C_{k+1}]$ 非正则. 假设 $\mathcal{C}$ 的所有参数在给定的变元序下比其他变元都小, 并令 $I_{k+1} := \mathrm{ini}(C_{k+1})$, 而 l 为使得 $\mathrm{lv}(I_{k+1}) = \mathrm{lv}(C_l)$ 成立的最小整数, 则下列结论成立:

(1) 如果 I_{k+1} 关于 C_l 不是约化的, 那么

$$\mathrm{prem}(I_{k+1}, [C_1, \ldots, C_l]) = 0, \quad \mathrm{prem}(C_{k+1}, [C_1, \ldots, C_k]) = 0;$$

(2) 如果 I_{k+1} 关于 C_l 是约化的, 那么 $\mathrm{prem}(C_l, [C_1, \ldots, C_{l-1}, I_{k+1}]) = 0$, 且要么

$$\mathrm{res}(\mathrm{ini}(I_{k+1}), [C_1, \ldots, C_{l-1}]) = 0$$

成立, 要么

$$\mathrm{prem}(C_{k+1}, [C_1, \ldots, C_{l-1}, I_{k+1}, C_{l+1}, \ldots, C_k]) = 0$$

成立.

注意, 上述定理中有一个假设, 即 W 特征列 $\mathcal{C}$ 的所有参数均小于其他变元. 为了表述方便, 将这一假设简称为序条件. 如果这个假设成立, 我们就说序条件对于 $\mathcal{C}$ 成立.

定义 3.4 设 $\mathcal{G} \subset \mathbb{K}[\boldsymbol{x}]$ 为约化字典序 Gröbner 基, 而 $\mathcal{C} \subset \mathbb{K}[\boldsymbol{x}]$ 为 $\langle \mathcal{G} \rangle$ 的 W 特征列, 则称有序对 $(\mathcal{G}, \mathcal{C})$ 为理想 $\langle \mathcal{G} \rangle$ 的特征对. 此外, 如果 $\mathrm{sat}(\mathcal{C}) = \langle \mathcal{G} \rangle$, 那么称 $(\mathcal{G}, \mathcal{C})$ 为强特征对. 类似地, 如果 W 特征列 $\mathcal{C}$ 是正规的或者正则的, 则称 $(\mathcal{G}, \mathcal{C})$ 为正规或正则特征对. 特别地, 在本文中, $(\{1\}, [1])$ 被视为平凡的特征对, 它也是强正规特征对.

对任意多项式理想, 我们都可以通过计算 Gröbner 基并从中提取 W 特征列的方式来得到特征对. 特征对提供了多项式理想的两种不同表示方式: 一方面是从 Gröbner 基的角度, 而另一方面则是从三角列的角度. 自然地, 特征对也提供了研究多项式理想的两种不同工具, 即 Gröbner 基理论中的基本运算—范式和三角列方法中的基本运算—伪除.

3.2 多项式组的正规特征分解

多项式组 $\mathcal{F}$ 的正则或正规特征分解是指有限多个正则或正规特征对 $(\mathcal{G}_1,\mathcal{C}_1),\ldots,(\mathcal{G}_e,\mathcal{C}_e)$ 使得

$$\sqrt{\langle\mathcal{F}\rangle}=\sqrt{\langle\mathcal{G}_1\rangle}\cap\cdots\cap\sqrt{\langle\mathcal{G}_e\rangle}=\sqrt{\mathrm{sat}(\mathcal{C}_1)}\cap\cdots\cap\sqrt{\mathrm{sat}(\mathcal{C}_e)} \tag{3.1}$$

这一理想关系成立, 或等价地, 使得

$$\mathsf{Z}(\mathcal{F})=\bigcup_{i=1}^{e}\mathsf{Z}(\mathcal{G}_i)=\bigcup_{i=1}^{e}\mathsf{Z}(\mathrm{sat}(\mathcal{C}_i)) \tag{3.2}$$

这一零点关系成立.

正规特征分解和正则特征分解是两个新概念. 当序条件对于 W 特征列成立时, Gröbner 基和正规三角列之间存在的内在联系可以指导我们进行正规三角分解; 当序条件不总成立时, 我们可以采用不同的策略将多项式组分解为有限多个正规特征对. 无论是正规特征分解还是正则特征分解, 它都可以同时得到正规或正则列集合以及相应的 Gröbner 基集合, 使其满足相应的零点关系. 特别地, Gröbner 基作为多项式理想的良好表示, 从中提取出来的正规列或正则列构成的集合以更简洁的形式携带着相似的零点信息. 有关更多 (强) 正规特征分解和 (强) 正则特征分解的理论基础和良好性质, 可参见文献 [44,45]. 特别地, 文献 [45] 证明了正规特征分解的如下结论.

定理 3.2 ([45, 定理 3.11]) 对 $\mathbb{K}[\boldsymbol{x}]$ 中任意有限非空的多项式组 $\mathcal{F}$, 均可以在有限步内计算出 $\mathcal{F}$ 的一个正规特征分解.

上述定理的证明是通过构造具体的正规特征分解算法并证明其正确性及终止性来完成的, 具体证明细节可参见文献 [45, 第 4.2 小节], 而相应的正规特征分解算法将会在本文第 4 节中进行介绍.

注 3.1 从多项式组 $\mathcal{F}\subseteq\mathbb{K}[\boldsymbol{x}]$ 的任一正规特征分解中均可提取出 $\mathcal{F}$ 的一个正规三角分解 $\mathcal{C}_1,\ldots,\mathcal{C}_e$, 于是每个 $\mathcal{C}_i$ $(i=1,\ldots,e)$ 都是正规列, 且满足

$$\mathsf{Z}(\mathcal{F})=\bigcup_{i=1}^{e}\mathsf{Z}(\mathcal{C}_i/\operatorname{ini}(\mathcal{C}_i)).$$

正规列的投影性质使我们可以得到其零点集非空的参数条件, 因此, 正规分解是求解参数多项式系统的有效方法. 由于通过正规特征分解得到的参数条件不一定互不相交, 因此, 它们不一定能构成参数空间的一个划分. 然而, 由正规三角列的初式所构成的条件多项式组中只含有参数, 这使得通过正规分解来计算综合三角分解比通过正则分解的方式在理论上更为容易 (参见文献 [24]).

设 $\mathfrak{a}$ 为 $\mathbb{K}[\boldsymbol{x}]$ 中的真理想. 如果它的所有伴随素理想的高度都相同, 那么称 $\mathfrak{a}$ 为纯等维的. 由文献 [54, 命题 4.1.3] 可知, 对于任意正则列 $\mathcal{T}$ 而言, $\mathrm{sat}(\mathcal{T})$ 都是纯等维的, 进而可以得到有关多项式组的正规特征分解的如下结论.

命题 3.2 ([45, 命题 3.13]) 设 Ψ 为多项式组 $\mathcal{F}\subseteq\mathbb{K}[\boldsymbol{x}]$ 的一个正规特征分解, 且对于 Ψ 中任意正规特征对 $(\mathcal{G},\mathcal{C})$ 都有 $\mathrm{sat}(\mathcal{C})=\langle\mathcal{C}\rangle$, 则可以得到

$$\sqrt{\langle\mathcal{F}\rangle}=\bigcap_{(\mathcal{G},\mathcal{C})\in\Psi}\sqrt{\langle\mathcal{G}\rangle},$$

其中每个 $\langle\mathcal{G}\rangle$ 都是纯等维的.

事实上, 由文献 [54, 定理 4.1.4] 可知上述命题中的 $\langle\mathcal{G}\rangle$ 也是强等维的. 下面的定理则告诉我们如何从一个理想的 W 特征列 (当其正规时) 来构造这个理想的 Ritt 特征列, 其证明过程可参见文献 [45].

定理 3.3 ([45, 定理 3.14]) 设 $\mathcal{C}=[C_1,\ldots,C_r]$ 为理想 $\langle\mathcal{P}\rangle\subseteq\mathbb{K}[\boldsymbol{x}]$ 的 W 特征列, 令

$$\mathcal{C}^*=[C_1,\mathrm{prem}(C_2,[C_1]),\ldots,\mathrm{prem}(C_r,[C_1,\ldots,C_{r-1}])]. \tag{3.3}$$

如果 $\mathcal{C}$ 是正规列, 那么下列结论成立:

(1) $\mathcal{C}^*$ 也是正规列;

(2) $\mathcal{C}^*$ 是 $\langle\mathcal{P}\rangle$ 的 Ritt 特征列;

(3) $\mathsf{Z}(\mathcal{C}^*/\operatorname{ini}(\mathcal{C}^*))=\mathsf{Z}(\mathcal{C}/\operatorname{ini}(\mathcal{C}))$.

设 Ψ 为多项式组 $\mathcal{F}\subseteq\mathbb{K}[\boldsymbol{x}]$ 的一个正规特征分解. 如果对 Ψ 中每个特征对中的 W 特征列 $\mathcal{C}$ 按照 (3.3) 计算出 $\mathcal{C}^*$, 那么将得到

$$\mathsf{Z}(\mathcal{F})=\bigcup_{(\mathcal{G},\mathcal{C})\in\Psi}\mathsf{Z}(\mathcal{C}^*/\operatorname{ini}(\mathcal{C}^*))=\bigcup_{(\mathcal{G},\mathcal{C})\in\Psi}\mathsf{Z}(\operatorname{sat}(\mathcal{C}^*)),$$

其中对每个特征对 $(\mathcal{G},\mathcal{C})\in\Psi$, $\mathcal{C}^*$ 为 $\langle\mathcal{G}\rangle$ 的 Ritt 特征列.

3.3 特征对的正则化与强化

特征对是由约化字典序 Gröbner 基及其 W 特征列构成的有序对. 任意给定的多项式理想的 W 特征列是唯一的, 但不同的多项式理想可以有相同的 W 特征列, 这促使我们来考虑具有更强性质的特征对—强正规特征对. 对于强正规特征对而言, 正规 W 特征列与约化字典序 Gröbner 基相互确定. 下面的定理告诉如何将任意正规特征对强化.

定理 3.4 ([45, 定理 3.19]) 设 $(\mathcal{G},\mathcal{C})$ 为 $\mathbb{K}[\boldsymbol{x}]$ 中的正规特征对, $\bar{\mathcal{G}}$ 为 $\operatorname{sat}(\mathcal{C})$ 的约化字典序 Gröbner 基, 而 $\bar{\mathcal{C}}$ 为 $\langle\bar{\mathcal{G}}\rangle$ 的 W 特征列. 假设序条件对于 $\mathcal{C}$ 成立, 则 $\bar{\mathcal{C}}$ 是正规的且 $\operatorname{sat}(\bar{\mathcal{C}})=\operatorname{sat}(\mathcal{C})$, 即 $(\bar{\mathcal{G}},\bar{\mathcal{C}})$ 是强正规特征对.

由上述定理可知, 通过计算一次 W 特征列的饱和理想的约化字典序 Gröbner 基即可实现正规特征对的强化, 从而得到强正规特征对. 对更一般的正则特征对而言, 如果序条件对其成立, 那么其强化方式与上述定理叙述的情形完全相同. 如果序条件不满足, 那么利用上述方法不一定能将正则特征对强化, 因为此时正则列的饱和理想的 W 特征列不一定是正则的. 但对于任意多项式理想, 我们仍然可以通过多次计算 W 特征列的饱和理想的 Gröbner 基的方式来尝试构造强正则特征对, 特别是非平凡的强正则特征对.

定理 3.5 (强正则化 [48, 定理 11]) 设 $\mathcal{C}_1$ 为 $\mathbb{K}[\boldsymbol{x}]$ 中理想 $\mathfrak{I}$ 的 W 特征列, $\mathcal{G}_i$ 为 $\operatorname{sat}(\mathcal{C}_{i-1})$ 的约化字典序 Gröbner 基, 而 $\mathcal{C}_i$ 为 $\langle\mathcal{G}_i\rangle$ 的 W 特征列 $(i\geqslant 2)$, 则一定存在整数 $m\geqslant 2$ 使得 $\mathfrak{I}\subseteq\operatorname{sat}(\mathcal{C}_1)\subseteq\operatorname{sat}(\mathcal{C}_m)$, 并且要么 $\mathcal{C}_m$ 是正则列, 要么 $\operatorname{sat}(\mathcal{C}_m)=\langle 1\rangle$.

从任意多项式理想 $\mathfrak{I}$ 构造强正则特征对的过程如图 1 所示.

3.4 多项式组的强正则与强正规特征分解

文献 [45] 证明了可以将 $\mathcal{F}\subset\mathbb{K}[\boldsymbol{x}]$ 的正规特征分解 $\Psi=\{(\mathcal{G}_1,\mathcal{C}_1),\ldots,(\mathcal{G}_t,\mathcal{C}_t)\}$ 转化为强正规特征分解 $\bar{\Psi}=\{(\bar{\mathcal{G}}_1,\bar{\mathcal{C}}_1),\ldots,(\bar{\mathcal{G}}_t,\bar{\mathcal{C}}_t)\}$, 这时每个 $(\bar{\mathcal{G}}_i,\bar{\mathcal{C}}_i)$ 均为强正规特征对.

$$
\begin{array}{rcccccccl}
\mathfrak{I} = & \mathfrak{I}_1 & = & \langle \mathcal{G}_1 \rangle & \longrightarrow & \mathcal{C}_1 & \longrightarrow & \mathrm{sat}(\mathcal{C}_1) & (\neq \langle 1 \rangle) \\
 & \cap\!\shortmid & & & & & & \cap\!\shortmid & \\
= & \mathfrak{I}_2 & = & \langle \mathcal{G}_2 \rangle & \longrightarrow & \mathcal{C}_2 & \longrightarrow & \mathrm{sat}(\mathcal{C}_2) & (\neq \langle 1 \rangle) \\
 & \cap\!\shortmid & & & & & & \cap\!\shortmid & \\
 & \vdots & & & & & & \vdots & \\
 & \cap\!\shortmid & & & & & & \cap\!\shortmid & \\
= & \mathfrak{I}_{m-1} & = & \langle \mathcal{G}_{m-1} \rangle & \longrightarrow & \mathcal{C}_{m-1} & \longrightarrow & \mathrm{sat}(\mathcal{C}_{m-1}) & (\neq \langle 1 \rangle) \\
 & \cap\!\shortmid & & & & & & \shortmid\!\shortmid & \\
= & \mathfrak{I}_m & = & \langle \mathcal{G}_m \rangle & \longrightarrow & \mathcal{C}_m & \longrightarrow & \mathrm{sat}(\mathcal{C}_m) & = \mathrm{sat}(\mathcal{C}_{m+1}) = \cdots
\end{array}
$$

图 1 通过计算饱和理想对特征对进行强正则化

定理 3.6 ([45, 定理 3.22]) 设 $\Psi = \{(\mathcal{G}_1, \mathcal{C}_1), \ldots, (\mathcal{G}_t, \mathcal{C}_t)\}$ 为 $\mathcal{F} \subseteq \mathbb{K}[\boldsymbol{x}]$ 的正规特征分解. 如果对每个 $(\mathcal{G}_i, \mathcal{C}_i)$ 都按照定理 3.4 所述计算得到强正规特征对 $(\bar{\mathcal{G}}_i, \bar{\mathcal{C}}_i)$, $i = 1, \ldots, t$, 那么

$$
\mathsf{Z}(\mathcal{F}) = \bigcup_{i=1}^{t} \mathsf{Z}(\bar{\mathcal{G}}_i) = \bigcup_{i=1}^{t} \mathsf{Z}(\bar{\mathcal{C}}_i / \mathrm{ini}(\bar{\mathcal{C}}_i)) = \bigcup_{i=1}^{t} \mathsf{Z}(\mathrm{sat}(\bar{\mathcal{C}}_i))
$$

成立, 即 $\bar{\Psi} = \{(\bar{\mathcal{G}}_1, \bar{\mathcal{C}}_1), \ldots, (\bar{\mathcal{G}}_t, \bar{\mathcal{C}}_t)\}$ 是 $\mathcal{F}$ 的强正规特征分解.

当序条件总满足时, 由定理 3.1 可以看出正则特征分解也是正规特征分解. 进一步, 还可以根据上述定理得到强正规特征分解. 当序条件不总是满足时, 我们可以基于可除分支构建和理想商除构造出有限多个强正则特征对 $(\bar{\mathcal{G}}_1, \bar{\mathcal{C}}_1), \ldots, (\bar{\mathcal{G}}_t, \bar{\mathcal{C}}_t)$ 使 (3.1) 成立, 即计算出 $\mathcal{F}$ 的强正则特征分解, 具体方法在下一节中以算法的形式详细描述.

4 特征分解算法

根据 W 特征列中特定多项式之间的伪整除关系, 文献 [44,45] 基于定理 3.1 提出了正规特征分解算法. 而受代数簇除法运算的启发, 文献 [48] 提出了另一种强正则特征分解算法, 该算法主要基于 W 特征列的饱和理想以及理想商运算的分解策略, 优点在于不需要考虑序条件. 下面分别介绍这两种分解算法.

4.1 按结构关系分裂的分解算法

设 $\mathcal{F} \subseteq \mathbb{K}[\boldsymbol{x}]$ 为输入多项式组、Φ 为多项式组构成的集合, 初始化时为 $\{\mathcal{F}\}$, 而 Ψ 为计算所得的正规特征对集合. 首先假设在计算过程中序条件总是成立. 从集合 Φ 中选取多项式组 $\mathcal{P}$ 并将其从 Φ 中移除, 然后计算理想 $\langle \mathcal{P} \rangle$ 的约化字典序 Gröbner 基 $\mathcal{G}$, 并从中提取出 $\langle \mathcal{G} \rangle$ 的 W 特征列 $\mathcal{C} = [C_1, \ldots, C_r]$. 为了简单起见, 将 $\mathrm{ini}(C_i)$ 记为 I_i $(i = 1, \ldots, r)$.

(1) 如果 $\mathcal{C}$ 是正规的, 那么我们已经得到正规特征对 $(\mathcal{G}, \mathcal{C})$, 且由命题 3.1(3) 可知,

$$
\mathsf{Z}(\mathcal{C} / \mathrm{ini}(\mathcal{C})) \subseteq \mathsf{Z}(\mathcal{P}) \subseteq \mathsf{Z}(\mathcal{C}). \tag{4.1}
$$

然后将正规特征对 $(\mathcal{G}, \mathcal{C})$ 添入 Ψ, 并将多项式组 $\mathcal{G} \cup \{I_1\}, \ldots, \mathcal{G} \cup \{I_r\}$ 添加到 Φ 中等待下一步处理.

(2) 如果 $\mathcal{C}$ 不是正规的, 那么根据定理 3.1 可以得到 $\mathcal{C}$ 中多项式之间的伪整除关系, 利用这些伪整除关系可以将 $\mathcal{G}$ 进行如下分裂, 此处整数 k 和 l 与定理 3.1 中的一致.

(2.1) 如果 I_{k+1} 对 C_l 不是约化的, 那么将多项式组 $\mathcal{G}\cup\{I_1\},\ldots,\mathcal{G}\cup\{I_l\},\mathcal{G}\cup\{I_{k+1}\}$ 添入 Φ 等待下一步处理.

(2.2) 如果 I_{k+1} 对 C_l 是约化的, 那么将 C_l 关于 I_{k+1} 的伪商记作 $Q=\mathrm{pquo}(C_l,I_{k+1})$, 然后再按下列两种情形进行.

(2.2.1) 若 $\mathrm{prem}(\mathrm{ini}(Q),\mathcal{C}_{l-1})=0$, 则将多项式组 $\mathcal{G}\cup\{I_1\},\ldots,\mathcal{G}\cup\{I_{l-1}\}$, $\mathcal{G}\cup\{\mathrm{ini}(I_{k+1})\}$ 添入 Φ 等待下一步处理.

(2.2.2) 若 $\mathrm{prem}(\mathrm{ini}(Q),\mathcal{C}_{l-1})\neq 0$, 则将多项式组 $\mathcal{G}\cup\{I_1\},\ldots,\mathcal{G}\cup\{I_{l-1}\}$, $\mathcal{G}\cup\{\mathrm{prem}(Q,\mathcal{C}_{l-1})\}$, $\mathcal{G}\cup\{I_{k+1}\}$ 添入 Φ 等待下一步处理.

完成上述分裂过程后, 继续从 Φ 中选取下一个多项式组 $\mathcal{P}'$ 并将其从 Φ 中移除, 同样计算 $\langle\mathcal{P}'\rangle$ 的约化字典序 Gröbner 基 $\mathcal{G}'$, 然后将 $\mathcal{G}'$ 按照相同的策略进行分裂. 当 Φ 为空时, 这一过程终止.

现将计算任意多项式组正规特征分解的上述方法提炼为算法, 如算法 1 所示.

算法 1 正规特征分解 $\Psi:=\mathsf{CharDec}(\mathcal{F},<)$

输入: 有限非空多项式组 $\mathcal{F}\subseteq\mathbb{K}[\boldsymbol{x}]$, 变元序 $<$.

输出: 当 $\mathsf{Z}(\mathcal{F})=\emptyset$ 时返回空集, 否则返回 $\mathcal{F}$ 的一个正规特征分解 Ψ.

有关算法 CharDec 的详细描述及终止性和正确性证明等, 可参见文献 [45]. 需要特别指出的是, 该算法假设序条件总满足, 但这一假设并非总是成立. 为了处理序条件不满足的情形, 文献 [46] 提出了临时换序策略, 寻找可以让序条件满足的变元序以便可以继续进行分裂.

4.2 基于可除分支构建和理想商除的分解算法

本小节介绍基于 Gröbner 基和理想运算的强正则分解算法. 这一算法主要由两个子算法构成, 一个算法利用理想的饱和运算来计算强正则特征对, 而另一个算法则通过理想的商运算来计算强正则特征因子.

定理 3.5 表明, 从任意一个多项式理想 $\mathfrak{I}\subseteq\mathbb{K}[\boldsymbol{x}]$ 出发, 都可以通过计算 $\mathfrak{I}$ 的 W 特征列的饱和理想及其 Gröbner 基来构造一个强正则特征对. 据此提出的算法 2 的输入输出如下所示, 该算法可以从任意多项式理想出发构造强正则特征对.

算法 2 计算强正则特征对 $(\mathcal{G},\mathcal{C}):=\mathsf{srcPair}(\mathfrak{I})$

输入: 任意多项式理想 $\mathfrak{I}\subseteq\mathbb{K}[\boldsymbol{x}]$.

输出: 强正则特征对 $(\mathcal{G},\mathcal{C})$, 使得 $\mathfrak{I}\subseteq\mathrm{sat}(\mathcal{C})=\langle\mathcal{G}\rangle$ 成立.

对于 $\mathbb{K}[\boldsymbol{x}]$ 中的任意两个理想 $\mathfrak{I}$ 和 $\mathfrak{J}$, 如果 $\mathfrak{I}:\mathfrak{J}\neq\mathfrak{I}$, 那么称 $\mathfrak{J}$ 可除 $\mathfrak{I}$.

定义 4.1 设 $\mathfrak{I}$ 为 $\mathbb{K}[\boldsymbol{x}]$ 中的理想, 而 $\mathcal{C}$ 为 $\mathfrak{I}$ 的 W 特征列. 称 $\mathcal{C}$ 为强特征列, 如果 $\mathrm{sat}(\mathcal{C})=\mathfrak{I}$. 如果 $\mathrm{sat}(\mathcal{C})$ 不可除 $\mathfrak{I}$, 那么称 $\mathcal{C}$ 为病态的.

如果理想 $\mathfrak{I}\subseteq\mathbb{K}[\boldsymbol{x}]$ 的 W 特征列 $\mathcal{C}$ 为强的, 那么显然 $\mathcal{C}$ 携带了 $\mathfrak{I}$ 的全部信息. 如果 $\mathcal{C}$ 是病态的, 我们会发现对于那些结构相对复杂的理想 $\mathfrak{I}$, 几乎无法从 $\mathcal{C}$ 中得到 $\mathfrak{I}$ 的重要信息.

命题 4.1 ([48, 命题 17]) 设 $\mathfrak{I}$ 和 $\mathfrak{J}$ 为 $\mathbb{K}[\boldsymbol{x}]$ 中的理想. 如果 $\mathfrak{I}\subseteq\mathfrak{J}$, 那么

$$\sqrt{\mathfrak{I}}=\sqrt{\mathfrak{J}}\cap\sqrt{\mathfrak{I}:\mathfrak{J}}.$$

对于 $\mathbb{K}[\boldsymbol{x}]$ 中的任意两个理想 $\mathfrak{I}$ 和 $\mathfrak{J}$, 若 $\mathfrak{I} \subseteq \mathfrak{J}$, 由命题 4.1 可知, $\sqrt{\mathfrak{I}} = \sqrt{\mathfrak{J}} \cap \sqrt{\mathfrak{I} : \mathfrak{J}}$. 当 $\mathfrak{I} : \mathfrak{J} = \mathfrak{I}$ 时, 这个分解是平凡的. 对于任意给定理想 $\mathfrak{I} \subsetneq \mathbb{K}[\boldsymbol{x}]$, 接下来将说明如何构造一个新理想 $\mathfrak{J} \subseteq \mathbb{K}[\boldsymbol{x}]$ 使得 $\mathfrak{I} \subseteq \mathfrak{J}$ 并且 $\mathfrak{J}$ 可除 $\mathfrak{I}$. 借助由 $\mathfrak{I}$ 构造所得的这个理想 $\mathfrak{J}$, $\mathfrak{I}$ 可以分裂为 $\mathfrak{J}$ 和 $\mathfrak{I} : \mathfrak{J}$, 且这个分裂为非平凡的. 于是可以替代 $\mathfrak{I}$ 按照类似的规则继续分裂 $\mathfrak{I} : \mathfrak{J}$. 这个通过理想的商运算分裂理想的思想源自文献 [49, 第 196–197 页] 中给出的从给定代数簇中除去已知子代数簇的运算.

借助构造强特征对的算法 srcPair, 接下来讨论对于任一个理想 $\mathfrak{I} \neq \langle 1 \rangle$, 如何寻找一个强正则特征对 $(\mathcal{G}, \mathcal{C})$ 使得 $\mathrm{sat}(\mathcal{C})$ 可除 $\mathfrak{I}$.

定义 4.2 称强正则特征对 $(\mathcal{G}, \mathcal{C})$ 为理想 $\mathfrak{I} \subseteq \mathbb{K}[\boldsymbol{x}]$ 的一个强正则特征因子, 如果 $\langle \mathcal{G} \rangle = \mathrm{sat}(\mathcal{C})$ 可除 $\mathfrak{I}$.

给定理想 $\mathfrak{I} \subsetneq \mathbb{K}[\boldsymbol{x}]$, 我们希望计算 $\mathfrak{I}$ 的一个强正则特征因子 $(\mathcal{G}, \mathcal{C})$. 现假设 $\mathfrak{I} \neq \langle 1 \rangle$. 首先利用算法 srcPair 计算强正则特征对 $(\bar{\mathcal{G}}, \bar{\mathcal{C}})$ 使得 $\mathfrak{I} \subseteq \mathrm{sat}(\bar{\mathcal{C}})$. 如果 $\mathfrak{I} : \mathrm{sat}(\bar{\mathcal{C}}) \neq \mathfrak{I}$, 那么就得到了 $\mathfrak{I}$ 的一个强正则特征因子 $(\bar{\mathcal{G}}, \bar{\mathcal{C}}) \neq (\{1\}, [1])$. 否则, $\mathfrak{I} : \mathrm{sat}(\bar{\mathcal{C}}) = \mathfrak{I}$. 此时计算 $\mathfrak{I}$ 的 Gröbner 基 $\mathcal{G}^*$ 并从中提取出 $\mathfrak{I}$ 的 W 特征列 $\mathcal{C}^*$. 如果 $\mathrm{sat}(\mathcal{C}^*) = \mathfrak{I}$, 则 $\mathrm{sat}(\bar{\mathcal{C}}) = \mathrm{sat}(\mathcal{C}^*)$, 从而,

$$\mathfrak{I} : \mathrm{sat}(\bar{\mathcal{C}}) = \mathrm{sat}(\mathcal{C}^*) : \mathrm{sat}(\mathcal{C}^*) = \langle 1 \rangle \neq \mathfrak{I},$$

这与 $\mathfrak{I} : \mathrm{sat}(\bar{\mathcal{C}}) = \mathfrak{I}$ 矛盾. 所以, $\mathrm{sat}(\mathcal{C}^*) \neq \mathfrak{I}$, 因而存在多项式 $F \in \mathrm{sat}(\mathcal{C}^*)$ 且 $F \notin \mathfrak{I}$. 令

$$J = \prod_{C \in \mathcal{C}^*} \mathrm{ini}(C),$$

则存在正整数 q 使得 $FJ^q \in \langle \mathcal{C}^* \rangle \subseteq \mathfrak{I}$. 选取多项式 $H_1, \ldots, H_t \in \mathbb{K}[\boldsymbol{x}] \setminus \mathfrak{I}$ 使得

$$H_1 \cdots H_t = 0 \iff FJ^q = 0.$$

令 $(\tilde{\mathcal{G}}, \tilde{\mathcal{C}}) \neq (\{1\}, [1])$ 为对于某个 i $(1 \leqslant i \leqslant t)$, 通过算法 srcPair 由 $\langle \mathfrak{I} \cup \{H_i\} \rangle$ 计算所得的强正则特征对. (1) 如果 $\mathfrak{I} : \mathrm{sat}(\tilde{\mathcal{C}}) \neq \mathfrak{I}$, 那么 $(\tilde{\mathcal{G}}, \tilde{\mathcal{C}})$ 即为 $\mathfrak{I}$ 的一个强正则特征因子. (2) 否则, 对所有 $1 \leqslant i \leqslant t$, 都有 $\mathrm{sat}(\tilde{\mathcal{C}})$ 不可除 $\mathfrak{I}$, 这里 $(\tilde{\mathcal{G}}, \tilde{\mathcal{C}})$ 与上述情形 (1) 中相同, 是由 $\langle \mathfrak{I} \cup \{H_i\} \rangle$ 通过计算所得的. 在此情形下, 我们需要对 $\langle \mathfrak{I} \cup \{H_i, H_{ij}\} \rangle$ 做类似考虑以继续寻找 $\mathfrak{I}$ 的强正则特征因子, 这里 $H_{ij} \in \mathbb{K}[\boldsymbol{x}] \setminus \langle \mathfrak{I} \cup \{H_i\} \rangle$ 且使得

$$H_{i1} \cdots H_{it_i} = 0 \iff F_i \prod_{C \in \mathcal{C}_i^*} \mathrm{ini}(C) = 0$$

成立, $F_i \in \mathrm{sat}(\mathcal{C}_i^*) \setminus \langle \mathfrak{I} \cup \{H_i\} \rangle$, 而 $\mathcal{C}_i^*$ 为 $\langle \mathfrak{I} \cup \{H_i\} \rangle$ 的 W 特征列.

上述过程会不断循环直至找到 $\mathfrak{I}$ 的一个强正则特征因子为止. 现将这一过程提炼为算法, 其输入输出如算法 3 所示.

算法 3 计算强正则特征因子 $(\mathcal{G}, \mathcal{C}) := \mathsf{srcDivisor}(\mathfrak{I})$

输入: $\mathfrak{I} \neq \langle 1 \rangle$, $\mathbb{K}[\boldsymbol{x}]$ 中的理想.

输出: $\mathfrak{I}$ 的一个强正则特征因子.

下面的定理可以由算法 3 直接得到.

定理 4.1 ([48, 定理 19]) 对于 $\mathbb{K}[\boldsymbol{x}]$ 中的任一个理想 $\mathfrak{I} \neq \langle 1 \rangle$, 均可构造性地找到 $\mathfrak{I}$ 的一个强正则特征因子.

在算法 srcPair 和 srcDivisor 的基础上, 下面介绍通过构造可除分支和计算理想商将多项式组分解为强正则特征对的算法. 不同于其他三角分解算法, 该算法分裂理想的策略主要基于求商运算: 先找到待分裂理想的一个强正则特征因子, 然后再将此特征因子中的 W 特征列的饱和理想从待分裂的理想中除去.

考虑理想 $\mathfrak{I}$, 初始化为输入多项式组 $\mathcal{F} \subseteq \mathbb{K}[\boldsymbol{x}]$ 生成的理想. 令 Ψ 为已经得到的强正则特征对的集合, 初始化为 $\emptyset$. 若 $\mathfrak{I} \neq \langle 1 \rangle$, 则计算 $(\mathcal{G}, \mathcal{C}) := \mathsf{srcDivisor}(\mathfrak{I})$, 从而将 $\mathfrak{I}$ 分裂为 $\mathrm{sat}(\mathcal{C})$ 和 $\mathfrak{I} : \mathrm{sat}(\mathcal{C})$, 同时, 将计算得到的强正则特征对 $(\mathcal{G}, \mathcal{C}) \neq (\{1\}, [1])$ 并入集合 Ψ. 由命题 4.1 可知,

$$\sqrt{\mathfrak{I}} = \sqrt{\mathrm{sat}(\mathcal{C})} \cap \sqrt{\mathfrak{I} : \mathrm{sat}(\mathcal{C})}, \tag{4.2}$$

因此, 我们用 $\mathfrak{I} : \mathrm{sat}(\mathcal{C})$ 替换之前的 $\mathfrak{I}$, 并按照上述方式继续分裂理想 $\mathfrak{I} : \mathrm{sat}(\mathcal{C})$. 重复此分裂过程直至 $\mathfrak{I} : \mathrm{sat}(\mathcal{C}) = \langle 1 \rangle$ 时终止, 此时 Ψ 中的特征对即构成输入多项式组的一个强正则特征分解. 现将该特征分解方法提炼为算法, 其输入输出如算法 4 所示.

算法 4 强正则特征分解 $\Psi := \mathsf{srcDec}(\mathcal{F})$.

输入: 任意有限、非空多项式组 $\mathcal{F} \subseteq \mathbb{K}[\boldsymbol{x}]$.
输出: $\mathcal{F}$ 的一个强正则特征分解 Ψ.

本小节中所提到的算法的详细伪代码描述以及正确性和终止性证明可参见文献 [48].

5 特征分解算法的实施

上一节中所介绍的算法及文献 [45, 46] 中的其他算法均已在计算机代数软件 Maple 中实现. 在该 Maple 程序实现中, 算法 1 的函数名为 CharDec, 其 Gröbner 基计算主要基于专用软件包 FGb 和 Maple 自带软件包中的函数. 需要指出的是, 算法 1 主要基于定理 3.1 所揭示的约化字典序 Gröbner 基的结构性质, 而定理 3.1 成立需要满足序条件的假设 (即 W 特征列的所有参数都要比其他变元小), 当然该假设在输入多项式组生成的理想为零维的情形下总是成立的. 实验结果显示, 对于测试用的正维多项式组中大约四分之一的算例, 序条件并非总是成立. 注意到, 序条件本质上是为了确保定理 3.1 中所描述的伪整除关系成立, 而在序条件不满足的情况下, 我们可以通过临时换序的策略确保伪整除关系成立. 事实上, 对于所有用于实验的多项式组, 我们均可以通过这种策略得到伪整除关系进而完成正规特征分解. 有关该临时换序策略的细节、程序实现和实验结果, 可参见文献 [46].

为了评估算法 1 的效率, 我们将其与间接正规分解 (即首先计算正则分解, 再将所得的正则列进行正规化) 的计算效率进行了比较. 在用于对比的间接正规分解中, 首先采用 Triangularize 函数 (来自 Maple 中的 RegularChains 软件包) 和 RegSer 函数 (来自 Maple 软件库 Epsilon) 用于计算正则分解, 然后利用 normat (来自 Epsilon 软件库中的 miscel 模块) 将正则列进行正规化. 部分实验结果如表 1 所示.

在表 1 中, Label 一栏记录了例子的名称, Dim 一栏记录了例子中理想的维数, CharDec 下的 Total 一栏记录了利用算法 1 计算正规特征分解的总时间 (其中括号内记录了计算所得的正规特征对的个数), 而 GB 一栏记录了计算所有约化字典序 Gröbner 基的时间. RegSer 和 Triangularize 下的 Total 一栏和 Regular 一栏分别记录了计算间接正规分解和正则分解的时间 (其中括号内记录了计算所得的分解的分支数). 表中的 lost 和 > 4,000 分别表示软件 Maple 提示 lost kernel connections 和计算在 4,000 秒内尚未终止.

表 1 正规特征分解的计算时间

		CharDec		RegSer		Triangularize	
Label	Dim	Total	GB	Total	Regular	Total	Regular
S5	4	0.140 (8)	0.047	4.182 (31)	0.484 (19)	1.513 (9)	0.124 (1)
S7	1	0.156 (5)	0.078	0.251 (7)	0.110 (4)	0.249 (5)	0.109 (1)
S8	2	0.062 (2)	0.320	0.062 (3)	0.062 (3)	0.156 (2)	0.141 (2)
S9	2	0.125 (5)	0.078	0.483 (21)	0.140 (8)	0.188 (6)	0.094 (1)
S13	3	0.312 (13)	0.140	0.171 (8)	0.109 (8)	0.125 (2)	0.094 (1)
S16	3	0.640 (6)	0.344	0.703 (7)	0.609 (7)	4.609 (8)	4.609 (8)
nueral	1	1.826 (15)	1.514	> 4,000	> 4,000	0.233 (6)	0.140 (5)
F663	2	2.949 (6)	2.326	1.935 (16)	1.202 (15)	1.607 (6)	1.045 (4)
Dessin2	0	27.222 (1)	27.207	> 4,000	> 4,000	> 4,000	> 4,000
Wang16	0	0.203 (1)	0.171	14.555 (1)	0.437 (1)	14.086 (1)	0.156 (1)
filter9	0	0.640 (1)	0.593	> 4,000	> 4,000	lost	lost
fabrice24	0	436.7 (1)	436.7	lost	lost	lost	lost
uteshev bikker	0	3.806 (1)	3.766	lost	lost	> 4,000	> 4,000
Cyclic6	0	2.153 (25)	1.244	lost	lost	> 4,000	> 4,000

为了测评将多项式组直接分解为强正则特征对的算法 4 的效率, 我们将其在软件 Maple 中实现为函数 srcDec, 并将其与另外两种间接将多项式组分解为正则列的饱和理想的方法进行了比较. 这两种间接方法是, 简单使用 Epsilon 软件库中的 uvd 函数计算代数簇的非混合分解以及先使用 RegularChains 软件包中的 Triangularize 函数计算得到正则分解, 再计算其中每个正则列的饱和理想的 Gröbner 基. 部分实验结果如表 2 所示.

在表 2 中, srcDec 下的 Total、GB、SAT 和 QUO 各栏分别记录了利用 srcDec 算法计算强正则特征分解的总时间 (括号内记录了计算所得的强正规特征对的个数) 以及计算所有 Gröbner 基、所有饱和理想和所有理想的商所消耗的时间; uvd 下的 Total 一栏记录了计算非混合分解的总时间, 而 Triangularize 下的 Total 和 Regular 两栏分别记录了计算正则列饱和理想的 Gröbner 基的总时间和计算正则分解的时间 (括号里记录了计算所得的分支个数). 表 2 中 > 1,000 意为计算在 1,000 秒内没有终止.

从表 1 和 2 可以看出, 这两个算法中最耗时的步骤都是约化字典序 Gröbner 基的计算. 在我们的程序实现中, 这一部分的计算先是通过专用软件包 FGb 计算分次逆字典序的 Gröbner 基, 然后在零维情形用 FGLM 算法 [55]、正维情形用 Gröbner 行走算法 [56] 将 Gröbner 基的项序换为字典序. 实验表明, 软件 Maple 中 Gröbner 行走算法的实现效率不高, 使得 Gröbner 基的计算成了目前算法程序实现的瓶颈.

在基于可除分支构建和理想商除的强正则特征分解算法中, 理想商的计算同样耗费时间. 然而对于大多数例子, 饱和理想的计算并没有过分耗时, 这是因为从强正则特征分解中提取出来的正则列大多数情况下也是正规的. 同时, 作为包含于约化字典序 Gröbner 基中的极小三角列, 它们往往比那些基于伪除或子结式的三角分解算法中计算得到的正则列要简单. 这些原因都使得算法 2 中正则列的饱和理想的计算量比另外两个算法的相应计算量要小. 更重要的是, 在表 2 中, 通过 srcDec 算法计算得到的强正则特征对的个数往往比经 Triangularize 函数和 uvd 函数分解得到的分支数要少, 这是由于

表 2 强正则特征分解的计算时间

			srcDec			uvd	Triangularize	
Label	Dim	Total	GB	SAT	QUO	Total	Total	Regular
E1	1	1.450 (2)	0.564	0.221	0.632	0.867 (3)	2.041 (13)	1.709
E5	4	3.568 (1)	1.793	0.461	1.255	3.374 (1)	7.684 (7)	5.225
E11	1	0.037 (1)	0.008	0.008	0.015	0.122 (1)	0.079 (3)	0.035
E34	0	0.574 (0)	0.556	0	0	> 1,000	50.650 (0)	50.649
S7	1	0.098 (1)	0.008	0.052	0.031	0.652 (1)	0.127 (1)	0.084
S8	2	0.058 (2)	0.018	0.004	0.030	0.112 (2)	0.099 (2)	0.081
S14	2	1.024 (6)	0.372	0.299	0.235	3.767 (6)	0.184 (8)	0.109
nueral	1	1.225 (2)	0.445	0.187	0.574	> 1,000	0.222 (5)	0.115
F663	2	8.982 (1)	1.264	1.684	5.983	> 1,000	4.312 (4)	0.935
Katsura-4	0	0.353 (1)	0.254	0	0.086	209.831 (1)	6.583 (4)	5.343
nld-3-4	0	2.037 (8)	0.175	0.624	1.121	1.066 (8)	0.754 (29)	0.520
nld-8-3	0	2.464 (2)	2.254	0.207	0	3.334 (2)	17.360 (8)	0.268
Cyclic-5	0	0.497 (4)	0.101	0.058	0.285	> 1,000	1.079 (15)	0.798
geneig	0	0.566 (1)	0.135	0.003	0.417	> 1,000	–	> 1,000
redcyc6	0	36.920 (6)	0.203	0.556	35.079	> 1,000	–	> 4,000
Cyclic-6	0	368.988 (6)	2.455	332.158	33.780	> 1,000	–	> 1,000
Raksanyi	4	0.057 (1)	0.012	0.001	0.028	0.588 (1)	0.064 (2)	0.047
Gerdt 5	2	3.150 (4)	1.163	0.330	1.343	2.830 (1)	2.009 (3)	1.849

基于可除分支构建和理想商除的算法本质上利用理想的商运算避免了一些冗余分支.

6 总结与展望

本文综述了 (强) 正规和 (强) 正则特征对与特征分解的概念和性质, 介绍了计算相应特征分解的方法, 包括基于按约化字典序 Gröbner 基的内在结构关系进行分裂的正规特征分解算法、基于可除分支构建与理想商除的正则特征分解算法以及将正规与正则特征对转化为强正规与强正则特征对的强化方法. 多项式组的特征对和特征分解揭示了字典序 Gröbner 基与三角列的内在关系并为多项式理想和多项式组的零点集同时提供了两种不同形式的表示. 正规和正则特征分解对应的代数簇分解都是非混合等维分解, 因此, 特征分解也为研究多项式理想的几何性质提供了良好的工具. 上述特性使得本文介绍的算法与已有的三角分解算法有明显区别.

与多项式组特征分解有关的前沿研究问题包括 (1) 约化字典序 Gröbner 基中多项式的内在结构; (2) 理想在其 W 特征列非正则情形 Ritt 特征列的构造; (3) 从正规特征分解获得综合三角分解和综合 Gröbner 系统; (4) 强正规简单特征分解; (5) 微分多项式组的特征分解等.

参考文献

1 Grcar J F. Mathematicians of Gaussian elimination. Notices Amer Math Soc, 2011, 58: 782–792
2 Chu S-C. Siyuan Yujian (in Chinese). 1303 [朱世杰. 四元玉鉴. 1303]
3 Bézout É. Théorie Générale des Équations Algébriques. Paris: De l'Imprimerie de Ph.-D. Pierres, 1779

4 Sylvester J J. The Collected Mathematical Papers of James Joseph Sylvester. Cambridge: Cambridge University Press, 2012
5 Macaulay F S. The Algebraic Theory of Modular Systems. Cambridge: Cambridge University Press, 1916
6 Wu W-T. On the decision problem and the mechanization of theorem-proving in elementary geometry. Sci Sinica, 1978, 21: 159–172
7 Ritt J F. Differential Algebra. New York: Amer Math Soc, 1950
8 Wu W-T. Basic principles of mechanical theorem-proving in elementary geometries. J Systems Sci Math Sci, 1984, 3: 207–235
9 Wu W-T. On zeros of algebraic equations: An application of Ritt principle. Chinese Sci Bull, 1986, 31: 1–5
10 Chou S-C. Mechanical Geometry Theorem Proving. Dordrecht: D. Reidel Publishing Company, 1988
11 Chou S-C, Gao X-S. Ritt-Wu's decomposition algorithm and geometry theorem proving. In: Proceedings of the 10th International Conference on Automated Deduction. Lecture Notes in Computer Science (Lecture Notes in Artificial Intelligence), vol. 449. Berlin-Heidelberg: Springer-Verlag, 1990, 207–220
12 Yang L, Zhang J-Z. Searching dependency between algebraic equations: An algorithm applied to automated reasoning. In: Artificial Intelligence in Mathematics. Oxford: Oxford University Press, 1994, 147–156
13 Wang D. Elimination procedures for mechanical theorem proving in geometry. Ann Math Artif Intell, 1995, 13: 1–24
14 Yang L, Zhang J-Z, Hou X-R. Nonlinear Equation Systems and Automated Theorem Proving (in Chinese). Shanghai: Shanghai Scientific and Technological Education Publishing House, 1996 [杨路, 张景中, 侯晓荣. 非线性代数方程组与定理机器证明. 上海: 上海科技教育出版社, 1996]
15 Lazard D. A new method for solving algebraic systems of positive dimension. Discrete Appl Math, 1991, 33: 147–160
16 Kalkbrener M. A generalized Euclidean algorithm for computing triangular representations of algebraic varieties. J Symbolic Comput, 1993, 15: 143–167
17 Wang D. An elimination method for polynomial systems. J Symbolic Comput, 1993, 16: 83–114
18 Aubry P, Moreno Maza M. Triangular sets for solving polynomial systems: A comparative implementation of four methods. J Symbolic Comput, 1999, 28: 125–154
19 Aubry P, Lazard D, Moreno Maza M. On the theories of triangular sets. J Symbolic Comput, 1999, 28: 105–124
20 Wang D. Decomposing polynomial systems into simple systems. J Symbolic Comput, 1998, 25: 295–314
21 Wang D. Computing triangular systems and regular systems. J Symbolic Comput, 2000, 30: 221–236
22 Hubert E. Notes on triangular sets and triangulation-decomposition algorithms I: Polynomial systems. In: Symbolic and Numerical Scientific Computation. Berlin-Heidelberg: Springer-Verlag, 2003, 143–158
23 Moreno Maza M. On triangular decompositions of algebraic varieties. Presented at MEGA-2000, Bath, UK, 2000, Http://www.csd.uwo.ca/~moreno//Publications/MorenoMaza-1999-MEGA2000.ps
24 Chen C, Golubitsky O, Lemaire F, et al. Comprehensive triangular decomposition. In: Computer Algebra in Scientific Computing. Lecture Notes in Computer Science, vol. 4770. Berlin-Heidelberg: Springer-Verlag, 2007, 73–101
25 Chen C, Moreno Maza M. Algorithms for computing triangular decomposition of polynomial systems. J Symbolic Comput, 2012, 47: 610–642
26 Dellière S. D. M. Wang simple systems and dynamic constructible closure. Rapport de Recherche n° 2000-16, 2000
27 Bächler T, Gerdt V, Lange-Hegermann M, et al. Algorithmic Thomas decomposition of algebraic and differential systems. J Symbolic Comput, 2012, 47: 1233–1266
28 Amodio P, Blinkov Y, Gerdt V, et al. On consistency of finite difference approximations to the Navier-Stokes equations. In: Computer Algebra in Scientific Computing. Lecture Notes in Computer Science, vol. 8136. Cham: Springer, 2013, 46–60
29 Li X, Mou C, Wang D. Decomposing polynomial sets into simple sets over finite fields: The zero-dimensional case. Comput Math Appl, 2010, 60: 2983–2997
30 Mou C, Wang D, Li X. Decomposing polynomial sets into simple sets over finite fields: The positive-dimensional case. Theoret Comput Sci, 2013, 468: 102–113
31 Chai F, Gao X S, Yuan C. A characteristic set method for solving boolean equations and applications in cryptanalysis of stream ciphers. J Syst Sci Complex, 2008, 21: 191–208
32 Gao X S, Huang Z. Characteristic set algorithms for equation solving in finite fields. J Symbolic Comput, 2012, 47: 655–679
33 Huang Z, Lin D. Attacking Bivium and Trivium with the characteristic set method. In: Progress in Cryptology—AFRICACRYPT 2011. Lecture Notes in Computer Science, vol. 6737. Berlin-Heidelberg: Springer, 2011, 77–91
34 Gao X S, Luo Y, Yuan C. A characteristic set method for ordinary difference polynomial systems. J Symbolic Comput, 2009, 44: 242–260

35 Gao X S, Van der Hoeven J, Yuan C M, et al. Characteristic set method for differential-difference polynomial systems. J Symbolic Comput, 2009, 44: 1137–1163
36 Buchberger B. Bruno Buchberger's PhD thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal. J Symbolic Comput, 2006, 41: 475–511
37 Becker T, Weispfenning V. Gröbner Bases. New York: Springer, 1993
38 Cox D, Little J, O'Shea D. Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra. New York: Springer, 2007
39 Lazard D. Ideal bases and primary decomposition: Case of two variables. J Symbolic Comput, 1985, 1: 261–270
40 Gianni P. Properties of Gröbner bases under specializations. In: EUROCAL '87. Lecture Notes in Computer Science, vol. 378. Berlin-Heidelberg: Springer-Verlag, 1989, 293–297
41 Marinari M G, Mora T. A remark on a remark by Macaulay or enhancing Lazard structural theorem. Bull Iranian Math Soc, 2003, 29: 1–45
42 Lazard D. Solving zero-dimensional algebraic systems. J Symbolic Comput, 1992, 13: 117–131
43 Dahan X. On lexicographic Gröbner bases of radical ideals in dimension zero: Interpolation and structure. arXiv:1207.3887, 2012
44 Wang D. On the connection between Ritt characteristic sets and Buchberger-Gröbner bases. Math Comput Sci, 2016, 10: 479–492
45 Wang D, Dong R, Mou C. Decomposition of polynomial sets into characteristic pairs. Math Comp, 2020, 89: 1993–2015
46 Dong R, Mou C. Decomposing polynomial sets simultaneously into Gröbner bases and normal triangular sets. In: Computer Algebra in Scientific Computing. Lecture Notes in Computer Science, vol. 10490. Cham: Springer, 2017, 77–92
47 Dong R, Mou C. On characteristic decomposition and quasi-characteristic decomposition. In: Computer Algebra in Scientific Computing. Lecture Notes in Computer Science, vol. 11661. Cham: Springer, 2019, 122–139
48 Dong R, Wang D. Computing strong regular characteristic pairs with Gröbner bases. J Symbolic Comput, 2021, 104: 312–327
49 Wang D. Elimination Methods. Wien-New York: Springer-Verlag, 2001
50 Mishra B. Algorithmic Algebra. New York: Springer-Verlag, 1993
51 Wang D-K. Zero decomposition algorithms for systems of polynomial equations. In: Computer Mathematics—Proceedings of the Fourth Asian Symposium (ASCM 2000). Lecture Notes Series on Computing, vol. 8. Singapore: World Scientific, 2000, 67–70
52 Wang D. Elimination Methods with Applications (in Chinese). Beijing: Science Press, 2002 [王东明. 消去法及其应用. 北京: 科学出版社, 2002]
53 Gao X-S, Wang D-K, Qiu Z Y, et al. Equation Solving and Machine Proving—Problem Solving with MMP (in Chinese). Beijing: Science Press, 2006 [高小山, 王定康, 裘宗燕, 等. 方程求解与机器证明: 基于 MMP 的问题求解. 北京: 科学出版社, 2006]
54 Aubry P. Ensembles triangulaires de polynômes et résolution de systèmes algébriques: Implantation en axiom. PhD Thesis. Paris: Université Pierre et Marie Curie, 1999
55 Faugère J C, Gianni P, Lazard D, et al. Efficient computation of zero-dimensional Gröbner bases by change of ordering. J Symbolic Comput, 1993, 16: 329–344
56 Collart S, Kalkbrener M, Mall D. Converting bases with the Gröbner walk. J Symbolic Comput, 1997, 24: 465–469

附录 A　特征分解示例

本附录以一组多项式为例, 给出强正则与强正规特征分解、三角分解及代数簇等维分解算法的部分输出结果, 意在说明这些算法的功能及其计算的代数与几何对象的特征和差异. 所考虑的多项式组为 $\mathcal{F} = \{F_1, F_2, F_3\}$, 其中

$$
\begin{aligned}
F_1 &= x_3x_4^2x_5 - x_4^3 + x_2^2x_3 + x_1^2x_3,\\
F_2 &= x_2x_4^2x_5 - x_4^3 + x_2x_3^2 + x_1^2x_2,\\
F_3 &= x_1x_4^2x_5 - x_4^3 + x_1x_3^2 + x_1x_2^2
\end{aligned}
$$

(参见表 2 例 S14 及文献 [47, 例 21]). 对变元序 $x_1 < \cdots < x_5$, 算法 4 可以将 $\mathcal{F}$ 分解为 6 个强正则特征对 $(\mathcal{G}_1, \mathcal{C}_1), \ldots, (\mathcal{G}_6, \mathcal{C}_6)$ 使得

$$\sqrt{\langle \mathcal{F} \rangle} = \sqrt{\mathrm{sat}(\mathcal{C}_1)} \cap \cdots \cap \sqrt{\mathrm{sat}(\mathcal{C}_6)} = \sqrt{\langle \mathcal{G}_1 \rangle} \cap \cdots \cap \sqrt{\langle \mathcal{G}_6 \rangle}, \tag{A.1}$$

其中

$$\begin{aligned}
&\mathcal{C}_1 = [x_1, x_2, x_4^2], \quad \mathcal{G}_i = \mathrm{sat}(\mathcal{C}_i) = \mathcal{C}_i, \quad i = 1, \ldots, 4,\\
&\mathcal{C}_2 = [x_1, x_3, x_4^2], \quad \mathcal{G}_5 = \mathrm{sat}(\mathcal{C}_5) = \mathcal{C}_5 \cup \{S\},\\
&\mathcal{C}_3 = [x_2, x_3, x_4], \quad \mathcal{G}_6 = \mathrm{sat}(\mathcal{C}_6) = \{G_1, \ldots, G_5\},\\
&\mathcal{C}_4 = [x_2 - x_1, x_3 - x_1, P], \quad P = x_1x_4^2x_5 - x_4^3 + 2x_1^3, \quad Q = x_4^3 - x_1x_3^2 - x_1^2x_3,\\
&\mathcal{C}_5 = [x_2 - x_1, Q, R], \quad R = x_3^2x_5 + x_1x_3x_5 - x_3x_4 + x_1x_4,\\
&\mathcal{C}_6 = [G_1, G_2, G_3], \quad S = x_4^2x_5 - x_1x_3 + x_1^2,\\
&G_1 = (x_3 + x_2 + x_1)(x_3 - x_2)(x_3 - x_1), \quad G_2 = x_4^3 - x_1x_2^2 - x_1^2x_2,\\
&G_3 = x_1x_2^2x_5 + x_1^2x_2x_5 + x_3^2x_4 - x_1x_2x_4, \quad G_4 = x_4^2x_5 + x_3^2 - x_1x_2,\\
&G_5 = x_2x_3^2x_5 + x_1x_3^2x_5 - x_2^3x_5 - x_1^3x_5 + x_3^2x_4 - x_2x_3x_4 - x_1x_3x_4 + x_2^2x_4 - x_1x_2x_4 + x_1^2x_4.
\end{aligned}$$

容易看出: (1) 对所有 $1 \leqslant i \leqslant 6$, $\mathcal{C}_i$ 都是正规的; (2) $\langle \mathcal{F} \rangle$ 为 2 维理想; (3) 对 $1 \leqslant i \leqslant 5$, $\sqrt{\langle \mathcal{G}_i \rangle}$ 都是素理想.

用Maple 中实现的算法 1, 可以将多项式组 $\mathcal{F}$ 分解为 8 个正规特征对:

$$\begin{aligned}
&(\{x_1, x_2, x_3, x_4\}, [x_1, x_2, x_3, x_4]), \quad (\{x_1^3, x_2 - x_1, x_3, x_4\}, [x_1^3, x_2 - x_1, x_3, x_4]),\\
&(\{x_1, x_2, x_4\}, [x_1, x_2, x_4]), \quad (\{x_1, x_2^2x_3, x_2x_3^2, x_4\}, [x_1, x_2^2x_3, x_4]),\\
&(\{x_2, x_1^2x_3, x_1x_3^2, x_4\}, [x_2, x_1^2x_3, x_4]), \quad (\mathcal{G}_4, \mathcal{C}_4), \quad (\mathcal{G}_5', \mathcal{C}_5'), \quad (\mathcal{G}_6', \mathcal{C}_6'),
\end{aligned}$$

其中

$$\begin{aligned}
&\mathcal{C}_5' = [x_2 - x_1, (x_3 - x_1)Q, x_1(x_3 - x_1)R],\\
&\mathcal{G}_5' = \mathcal{C}_5' \cup \{P + x_1x_3^2 - x_1^3,\ x_3x_4^2x_5 - x_4^3 + 2x_1^2x_3\},\\
&\mathcal{C}_6' = [(x_2 - x_1)G_1, (x_2 - x_1)G_2, (x_2 - x_1)G_3],\\
&\mathcal{G}_6' = \mathcal{C}_6' \cup \{(x_3 - x_1)Q,\ (x_3 - x_1)(x_1x_3^2x_5 + x_1^2x_3x_5 - x_1x_3x_4 + x_2^2x_4), F_3, F_2, F_1\}.
\end{aligned}$$

前 3 个特征对和 $(\mathcal{G}_4, \mathcal{C}_4)$ 都是强正规的, 第 5 个和最后一个特征对可以被分别强化为 $(\mathcal{G}_3, \mathcal{C}_3)$ 和 $(\mathcal{G}_6, \mathcal{C}_6)$. 对于第 4 个和第 7 个特征对中的正规列, 虽然它们不满足序条件, 但定理 3.4 中的方法仍然可以用来对其强化, 得到强正规特征对 $(\{x_1, x_3, x_4\}, [x_1, x_3, x_4])$ 和 $(\mathcal{G}_5, \mathcal{C}_5)$.

用 Epsilon 软件库中的函数 RegSer 可将 $\mathcal{F}$ 分解为下列正则系统:

$$\begin{aligned}
&[[x_1, x_2, x_4], \emptyset], \quad [[x_1, x_3, x_4], \{x_2\}], \quad [\mathcal{C}_3, \{x_1\}], \quad [\mathcal{C}_4, \{x_1, x_4\}],\\
&[[x_2 - x_1, Q, P + x_1x_3^2 - x_1^3], \{x_1, x_3, x_3 - x_2, x_3 + x_2\}],\\
&[[G_1, G_2, F_3], \{x_1, x_2, x_2 - x_1, x_2 + x_1\}].
\end{aligned}$$

这 6 个正则系统中, 最后两个系统中的正则列不是正规的.

用 Epsilon 软件库中的函数 uvd 可将 $\mathcal{F}$ 分解为 6 组多项式 $\{x_1, x_2, x_4\}, \{x_1, x_3, x_4\}, \mathcal{G}_3, \ldots, \mathcal{G}_6$, 它们定义 6 个非混合等维代数簇.

用 Maple 软件包 RegularChains 中的函数 Triangularize 可以将 $\mathcal{F}$ 分解为下列 8 个正则列:

$$[x_1, x_2, x_4], \quad [x_1, x_3, x_4], \quad \mathcal{C}_3, \quad \mathcal{C}_4, \quad [x_2 - x_1, Q, S], \quad [x_3 - x_1, G_2, x_4^2 x_5 - x_1 x_2 + x_1^2],$$
$$[x_3 - x_2, G_2, x_4^2 x_5 + x_2^2 - x_1 x_2], \quad [x_3 + x_2 + x_1, G_2, x_4^2 x_5 + x_2^2 + x_1 x_2 + x_1^2],$$

其中最后 4 个正则列都不是正规的.

上面的一些多项式被写成其因子的乘积, 这只是为了简洁和方便阅读. 我们的特征分解算法并不需要用到多项式因子分解.

Characteristic decomposition of polynomial sets

Dongming Wang, Chenqi Mou & Rina Dong

Abstract An ordered pair $(\mathcal{G}, \mathcal{C})$ is called the characteristic pair of a polynomial ideal if $\mathcal{G}$ is the reduced lexicographic Gröbner basis of the ideal and $\mathcal{C}$ is the minimal triangular set contained in $\mathcal{G}$. A characteristic pair $(\mathcal{G}, \mathcal{C})$ is said to be regular or normal if $\mathcal{C}$ is regular or normal; it is said to be strong if the ideal generated by $\mathcal{G}$ and the saturated ideal of $\mathcal{C}$ are the same. A strong regular or normal characteristic decomposition of a polynomial set means a decomposition of the polynomial set into finitely many (strong) regular or normal characteristic pairs with an associated zero or ideal decomposition. This paper presents two algorithms for characteristic decomposition of any given polynomial set, one producing strong normal characteristic pairs with ideal splitting according to pseudo-divisibility relations between polynomials in reduced lexicographic Gröbner bases and the other producing strong regular characteristic pairs by constructing nontrivial ideals that can be divided out of given ideals by using ideal quotient. Novel theorems are established for regularizing characteristic pairs and strengthening regular and normal characteristic pairs by using ideal saturation. Strong regular or normal characteristic pairs produced by the algorithms possess nice properties and furnish two representations, one in terms of lexicographic Gröbner bases and the other in terms of triangular sets, for the zeros of the input set of multivariate polynomials. The paper includes a brief review on triangular decompositions of various kinds and discussions about inherent connections among triangular sets, Ritt characteristic sets, and reduced lexicographic Gröbner bases. Examples and experimental results are also provided to illustrate the method of characteristic decomposition and its applicability and performance.

Keywords **characteristic pair, characteristic decomposition, triangular decomposition, Gröbner basis, polynomial set**

MSC(2010) **13P10, 13P15, 68W30**

doi: 10.1360/SSM-2020-0025