复　　杂度分析：利用追踪器数据研究 F4 Gröbner 基算法

Robin Kouba、Vincent Neiger、Mohab Safey ElDin；索邦大学、
法国国家科学研究中心、LIP6实验室，法国巴黎 F-75005

arXiv:2603.16378v1 [cs.SC] 17 Mar 2026

摘要

我们针对一般零维情形下反向字典序 Gröbner 基的计算，给出了一个新的复杂度界，该结果依赖于 Moreno-Socías 猜想。首先，我们将正则序列的一项性质形式化，并由此推出一个众所周知的经验性结论，我们称之为递增次数性质。随后，我们基于 Moreno-Socías 猜想，对 F4 算法中的对的选择有了新的认识。此外，对于相关次数中的一半，我们得到了给定次数的反向字典序 Gröbner 基中元素个数的精确公式。结合这些结果，我们推导出 F4 Tracer 算法的精确复杂度公式，并分析了变量数趋于无穷时的渐近行为。这些结果使最新复杂度界得到改进，改进幅度为变量数的指数级因子。

关键词：格罗布纳基、正则序列、Syzygies、F4 算法轨迹、复杂度分析

1. 引言

格罗布纳基计算。格罗布纳基是相对于某种单项式序表示多项式理想的重要工具；有关基本定义和性质，请参阅 [8]。由于格罗布纳基可以通过多元除法算法解决理想成员问题，也可以用于对理想取“模”，因此它们也已成为解决多项式方程组的一种用途广泛且应用普遍的工具。

因此，计算格罗布纳基的复杂度已得到广泛研究。20 世纪 80 年代，研究重点主要在于给出下界（见 [38, 32]）和上界（零特征情形见 [24, 39]，正特征情形见 [9]），并确定格罗布纳基的最坏情形行为关于变量个数呈双重指数增长。在一些附加假设下（按照 Zariski 拓扑的意义，这些假设一般都成立，或被推测成立），最坏情形结果已得到显著改进；这些假设包括零维性、正则性、同时诺特位置（见 [33, 24, 2]），而它们在许多应用场景中都相当现实。

不过，这些上界与用于计算格罗布纳基的算法关系不大；它们是在当时格罗布纳基理论中只有 Buchberger 算法（见 [6]）这一算法杰作的情况下证明的。人们发现，这种算法在实践中的表现很大程度上取决于临界对的选取顺序（例如，见 [23]）；该算法的核心是反复将与临界对相关的 S多项式对当前基进行约化。人们还发现，通常大多数这类约化最终都会得到零；如果能在实际执行约化之前检测出这些零约化，就可以节省大量计算时间。

***F5*算法。**这种 F5算法 [13] 及其变体 [11]提供了一种算法框架，在某些正则性假设下可以避免所有归约为零的情况。这些算法可以与前述约化的线性代数视角相结合，通过对 Macaulay 矩阵 [35, 33]进行行阶梯形计算来实现。这样做的代价是引入与格罗布纳基计算过程中出现的多项式相关联的签名，这会大幅限制线性代数步骤中可用的行置换集合。还可以利用这些签名，借助适配准则，将多项式的结构纳入考量 [26]。（关于这些行阶梯形计算中的列置换，值得注意的是，由于 Macaulay 矩阵的构造方式以及格罗布纳基是相对于单项式序计算的这一事实，无论使用何种算法，列置换实际上都是不允许的。）

尽管如此，其中一种变体在 [2], 中有专门的复杂度分析，该分析在某些一般性假设下利用了算法的特殊设计。然而，可能是由于线性代数步骤缺乏灵活性，再加上难以高效处理签名，因此例如 F5 算法并未被应用于现有速度最快的格罗布纳基软件工具中。

F4 算法与格罗布纳轨迹。F5 的前身，即所谓的 F4 算法， [12] 在实际应用中相较于 Buchberger 算法显著提升了速度，目前也是大多数领先计算机代数软件所采用的算法。然而，据我们所知，即使在附加的一般性假设下，这种已观察到的 F4 效率也未能通过任何利用其特定设计的专门复杂度分析加以解释。事实上，在过去二十年间的研究中，我们找到的所有与 F4 相关的复杂度论述，都基于正则性假设以及对正则度的估计（用于控制 Macaulay 矩阵的数量和规模）；例如参见 [18, 19, 28, 29, 27, 7]。

在这一框架中，与 F5 不同，将矩阵化为行阶梯形时，在选择高斯消元的约化子或主元，以及应用行置换方面，都有很大的自由度。

在这一框架下，如何避免 F4 算法中的归约为零，尚无定论。在 [6] 中首次提出并在 [22] 中进一步发展的一个判据，可以检测出一定数量必然会归约为零的对，但无法检测全部。当基域足够大时，可以对行的子集进行随机线性组合，再通过约化来检测其中是否有一些行都会归约为零。这项技术最初在 Magma [5] 中引入，随后也在 Maple[36] 和 msolve [4] 中实现。尽管这项技术显著提升了速度，但即便在某些正则性假设下，它对整体计算复杂度的影响仍未得到研究。这项技术无法消除所有归约为零的情况，但确实能去除其中相当一部分。

一种更为系统地避免归约为零的方法，受到 [44] 中为 Buchberger 算法引入的追踪方法的启发，并且可直接扩展到 F4 算法的情境中。对给定的输入多项式序列运行 F4 算法，并采用规定的临界对选择策略，例如 [12] 中所谓的“正规策略”，可产生在每个次数上输入多项式所有代数组合的首项单项式结构。计算过程中生成的所有首项单项式信息称为与格罗布纳基计算相关的格罗布纳轨迹。更具体地说，使用一种用于该轨迹的数据结构，存储表明哪些行未归约为零以及使用了哪些约化子的单项式信息，就可以在对与该格罗布纳轨迹相容的输入序列计算格罗布纳基时，消除所有归约为零的情况。尽管这是一个较强的假设，但在实践中经常出现，例如通过多模方法 [44], 在有理数上求解多项式系统时，或处理参数依赖系统时（例如见 [34]）。这便引出了所谓的 F4-Tracer 算法，例如已在 Maple [36] 或 msolve 库中实现，并已展现出实际效率（见 [4]）。

本文旨在利用 *F4-Tracer* 算法的结构，在下文明确说明的一些经典一般性假设下，建立其复杂度结果。

主要结果。为了描述我们的结果，我们需要引入一些记号。全文中，我们用 $\mathcal{R}_n = \mathbb{K}[x_1, \ldots, x_n]$ 表示域 $\mathbb{K}$ 上、变量为 x_1、……、x_n 的多元多项式环，用 $\mathcal{R}_n^{(\leq \delta)}$ 表示 $\mathcal{R}_n$ 中所有次数不超过 δ 的多项式构成的子集。对于多项式 f，我们用 $\hom(f)$ 表示其最高次数齐次分量。对于多项式序列 $\boldsymbol{f} = (f_1, \ldots\ldots, f_s)$，定义 $\hom(\boldsymbol{f}) = (\hom(f_1)\ldots\ldots, \hom(f_s))$。

对于正实数 $p \in (0, 1]$ ）和整数 $\delta \geq 2$，我们定义

$$E_p(\delta) = \ln\left(\frac{1 + p(\delta - 1)}{\delta}\right) + p(\delta - 1)\ln\left(\frac{1 + p(\delta - 1)}{p(\delta - 1)}\right)$$

以及

$$L_\omega(\delta) = \frac{\delta}{1 - e^{-\frac{1}{(\omega-2)}}} - \frac{1}{1 - e^{-\frac{1}{\delta(\omega-2)}}}.$$

这里， ω 表示在 $\mathbb{K}$ 上进行矩阵乘法的指数。注意，当 $\omega = 2$ 时， $L_\omega(\delta)$ 未定义；在这种情况下，按照约定，对于所有 $\delta \geq 2$，令 $L_2(\delta) = 1$ 。此外，我们用 $\boldsymbol{\ell}(\omega)$ 表示常数 $L_\omega(2)$，并且对于任意实数 $\varepsilon > 0$，定义常数

$$\boldsymbol{c}(\varepsilon, \delta, \omega) = E_{1/2}(\delta) + E_{\boldsymbol{\ell}(\omega)+\varepsilon}(\delta).$$

如上所述，F4-Tracer 算法的输入是一个多项式序列及其对应的格罗布纳轨迹 $\mathcal{T}$，并假设二者相容。从给定的多项式序列构造该格罗布纳轨迹的算法记为算法F4B，而 F4-Tracer 算法本身记为算法F4T。

~我们使用经典记号 $\mathcal{O}$ 和 $\mathcal{O}$ 表示渐近界，其定义见 [21, 定义 25.7~和 25.8]。回顾一下，对于两个函数 f， g： $\mathbb{N} \to \mathbb{R}_{\geq 0}$，函数 $f(n)$ 属于 $\mathcal{O}(g(n))$，如果存在常数 N， c 使得

$$f(n) \leq g(n)\big(\log_2(3+g(n))\big)^c$$

对所有 $n \geq N$。

定理 1.1。 设 $\boldsymbol{f} = (f_1, \ldots, f_n)$ 是环 $\mathcal{R}_n$中的一个非零多项式序列，其中所有多项式的次数均为$\delta \geq 2$，且 $n \geq 2$。假设 δ 是固定的。设 $\mathcal{T}$为算法 F4B 以输入 $\boldsymbol{f}$ 和分次反字典序运行时返回的格罗布纳轨迹 $\succ_{\text{grevlex}}$。

存在一个扎里斯基开集 $\Omega \subset \big(\mathcal{R}_n^{(\leq \delta)}\big)^n$，使得如果 $\mathsf{hom}(\boldsymbol{f})$ 属于 Ω，那么在与 $\mathcal{T}$相容的多项式方程序列 F4T 算法的输入 $\boldsymbol{g} = (g_1, \ldots, g_n)$ 上运行算法 $\mathcal{T}$，即可计算出 $(\boldsymbol{g}, \succ_{\text{grevlex}})$ 的极小 *Gröbner* 基，使用

$$\widetilde{\mathcal{O}}\Big(\delta^{\omega n+1} e^{\boldsymbol{c}(\varepsilon,\delta,\omega)\, n}\Big)$$

对所有 $\varepsilon > 0$，在 $\mathbb{K}$ 中进行算术运算。

该结果的更精确表述见第 6.1 节的定理 6.1。扎里斯基开集Ω 非空依赖于 [40, 猜想 4。1], [20, 猜想 1。1] 以及 [40, 猜想 1。6]。

~定理 $\mathcal{O}$ 的记号中 1.1 隐藏的因子由一个关于 n 的多项式上界给出，其次数随 ω 线性增长，且不依赖于 δ 或 ε。系数 $\boldsymbol{c}(\varepsilon, \delta, \omega)$ 随 ε 增大而增大，并且对于任意 $\delta \geq 2$，都有

$$\lim_{\varepsilon \to 0^+} \boldsymbol{c}(\varepsilon, \delta, \omega) = E_{1/2}(\delta) + E_{\boldsymbol{\ell}(\omega)}(\delta). \qquad (\star)$$

例如，当 $\delta = 2$时，我们有 $(\star)$ 约等于 0.2616 （当 $\omega = 3$时），约等于 0.6743 （当$\omega = 2.81$ 时），约等于 0.7956 （当 $\omega = 2.38$时）。

对于诸如算法 F4T这样的算法，其复杂度结果取决于对三个不同量的理解。第一个量是每个步骤中发现的新元素数量，这一点已在 [2]中得到充分研究。第二个量是每个步骤中用于约化这些新多项式的约化子的数量；我们的分析正是在这一点上相较于当前最佳水平有所改进。最后，第三个量是所涉及多项式的支撑集，这是我们在此采用与当前最佳水平相同处理方式的方面。

为了更清晰地展示定理 1.1 的渐近结果，我们将其与 [2,定理 2 和第 3 节2]进行比较。该结果给出了公式 N_{F5}，它为计算 $\mathbb{K}$ 中一组一般多项式的 grevlex Gröbner 基所需的算术运算次数提供了上界$(f_1, \ldots, f_n)$，这些多项式属于 $\mathcal{R}_n$，次数为 δ，并使用 F5 算法计算。此外，对于固定的 δ，有

$$N_{F5} \in \widetilde{\mathcal{O}}\big(\delta^{3n} h(\delta)^n\big),$$

其中，对于 $\delta \geq 2$，有 $1 \leq h(\delta) \leq 3$。此外，函数 $h(\delta)$ 是递增的，并且

$$\lim_{\delta \to +\infty} h(\delta) \approx 2.814.$$

我们通过考虑以下比值，估算我们的上界在算法 F4T 算术复杂度方面相对于 F5算法 所带来的提升：

$$\frac{\delta^{3n} 2.81^n}{\delta^{\omega n} e^{n(E_{1/2}(\delta) + E_{\boldsymbol{\ell}(\omega)}(\delta))}} = \left(\frac{2.81\, \delta^{3-\omega}}{e^{E_{1/2}(\delta) + E_{\boldsymbol{\ell}(\omega)}(\delta)}}\right)^n.$$

图1 展示了这一指数级提升的底数，

$$\boldsymbol{g}(\omega, \delta) = \frac{2.81\, \delta^{3-\omega}}{e^{E_{1/2}(\delta) + E_{\boldsymbol{\ell}(\omega)}(\delta)}},$$

作为 δ 在若干取值下的 ω。图1 中的两幅图展示了同一函数在不同范围内的 δ。第一幅图展示了 δ取值较小时的行为，而第二幅图则突出了 δ较大时的渐近行为。

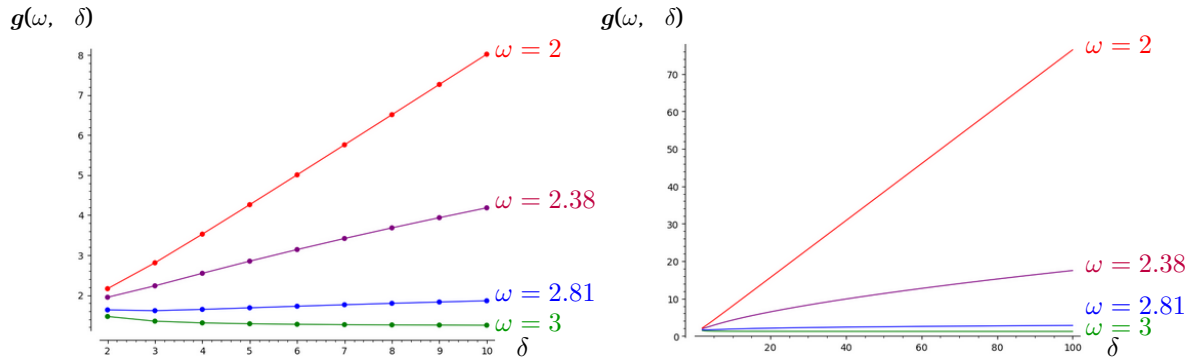

图 1：渐近情形下的指数级增益

增益可解释为 $g(\omega,\delta)^n$。例如，令 $\delta = 2$，则当 $\omega = 3$ 时，$g(\omega, 2) = 1.4687$；当 $\omega = 2.81$ 时，$g(\omega,2) = 1.6331$（Strassen）；当 $\omega = 2.38$ 时，$g(\omega, 2) = 1.9531$（略高于目前已知的最佳上界 ω）。此外，对于 $\delta = 3$，当 $\omega = 3$ 时，$g(\omega, 3)$ 等于 1.3518；对于 $\omega = 2.81$，$g(\omega, 3) = 1.6139$；对于 $\omega = 2.38$，$g(\omega, 3) = 2.2348$。更一般地，对于固定的 ω，函数 $g(\omega,\delta)$ 在 δ 趋于无穷大时渐近等价于 $t(\omega)\ \delta^{3-\omega}$，其中 $t(\omega)$ 是一个常数。

结论与展望。 据我们所知，这是首次专门针对 F4 算法某个变体进行复杂度分析，即便是在预先已知格罗布纳轨迹这一强假设以及一般性假设下也是如此。事实上，上述复杂度界给出的估计优于文献中已知的关于 [2] 所研究的 F5 算法变体的最佳估计。这或许是深入理解关于现有软件实现运行时间的普遍观察的第一步。然而，与其说这为比较这些算法提供了定论，不如说它引出了更多有待未来研究的问题。首先需要指出，我们的假设比 [2] 中的假设强得多。其次，此处比较的仅是上界，而且两者所依据的方法都会高估计算过程中出现的 Macaulay 矩阵的列数。

尽管如此，这一结果表明，分析 F4 算法概率变体的复杂度或许具有研究价值。该变体依赖前述概率线性代数步骤，并消除了大量归约为零的情况。这也解决了在 F4 算法框架下移除所有归约为零步骤的问题，同时保留其在线性代数步骤上的灵活性优势。

论文结构。 在第 2 节中，我们建立了正则序列的若干性质，这些性质蕴含了我们所称的 递增次数性质。在第 3 节中，我们证明了一个重要的原创定理，阐述如何利用 [6] 首次提出、并在 [22] 中进一步发展的判据，确定所选临界对的形式。在第 4 节中，我们展示了反向字典序的 Macaulay 矩阵的一些结构性质，并给出 [40, 推论 3。2] 的一个特定情形的定制版本。第5 节介绍算法及其主要性质，而第 6 节则着重讨论复杂度分析与比较。

致谢。 作者获法国国家研究署资助，该机构资助了 ANR-23-CE48-0003 项目 CREAM 和 ANR-25-CE39-7662 项目 PQMC；此外，作者还获得空军科学研究办公室（AFOSR）欧洲航空航天研究与发展办公室拨款 FA8655-25-1-7469 的资助。

2. 关于递增次数性质

此外，对于非零多项式 $f \in \mathcal{R}_n$，我们用 Supp(f) 表示其支撑集。对于由多项式构成的有限集合 $\boldsymbol{f}$，$\boldsymbol{f}$ 的支撑集定义为 Supp($\boldsymbol{f}$) $= \bigcup_{f\in\boldsymbol{f}}$Supp($f$) 的并集。

本节旨在证明下文陈述的命题 2.2。我们先回顾齐次正则序列的定义 [37, 第 16]节。

定义 2.1。 设 $\boldsymbol{f} = (f_1, \ldots, f_s)$ 是自然数集 $\mathcal{R}_n$ 中由非零齐次多项式构成的序列。若对于所有 $i \in \{2, \ldots, s\}$，f_i 在商环 $\mathcal{R}_n/\langle f_1, \ldots, f_{i-1}\rangle$ 中都不是零因子，则称序列 $\boldsymbol{f}$ 为正则 序列。

我们回顾一下，对于属于 $\mathcal{R}_n$ 的多项式 f，记其最高次数齐次分量为 hom(f)。对于子集 $\boldsymbol{f} \subset \mathcal{R}_n$，hom($\boldsymbol{f}$) 表示集合 $\{\text{hom}(f) \mid f \in \boldsymbol{f}\}$。

命题 2.2。 设 $\boldsymbol{f} = (f_1, \ldots, f_s)$ 是 $\mathcal{R}_n$ 中的非零多项式序列，满足 $\deg(f_i) = \delta_i$，并假设 $\mathsf{hom}(\boldsymbol{f})$ 是一个正则序列。设 d 为一个整数。对于任意组合 $w = q_1 f_1 + \cdots + q_s f_s$，其中 w、q_1、…、q_s 属于 $\mathcal{R}_n$，且满足 $\deg(w) < d$，以及对于所有 i 均有 $\deg(q_i) \leq d - \delta_i$，存在多项式 h_1、…、h_s，使得 $w = h_1 f_1 + \cdots + h_s f_s$，并且对于所有 i 均有 $\deg(h_i) < d - \delta_i$。

这一结果的一个重要推论是关于格罗布纳基计算的一条公认事实：使用 Lazard 算法等基于线性代数的算法计算分次格罗布纳基时[33], F4 [12], 或 F5 [13], 在处理临界对时，算法的格罗布纳基中新增多项式的次数严格递增。

命题 2.2 的证明依赖于下面两个辅助引理。我们先介绍后文将用到的一些记号。对于 $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ 中的 $\mathbb{N}^n$，单项式 $\prod_{i=1}^n x_i^{\alpha_i}$ 记作 $\boldsymbol{x}^{\boldsymbol{\alpha}}$。此外，令 $|\boldsymbol{\alpha}| = \sum_{i=1}^n \alpha_i$。我们用 $\mathsf{Mon}_{d,n}$ 表示 $\mathcal{R}_n$ 中次数为 d 的单项式集合，用 $\mathsf{Mon}_{\leq d,n}$（分别用 $\mathsf{Mon}_{<d,n}$）表示 $\mathcal{R}_n$ 中次数至多为 d（分别小于 d）的单项式集合。$\mathcal{R}_n$ 中所有单项式构成的集合记作 Mon_n。对于 $d \in \mathbb{N}$，我们用 $\mathcal{R}_n^{(d)}$ 表示由 $\mathcal{R}_n$ 中所有次数为 d 的齐次多项式生成的 $\mathbb{K}$-向量空间。对于 $\mathbb{K}$-向量空间中的集合 S，我们用 $\mathsf{Span}_{\mathbb{K}}(S)$ 表示由 S 生成的 $\mathbb{K}$-向量子空间。

引理 2.3。 设 $\boldsymbol{f} = (f_1, \ldots, f_s)$ 是 $\mathcal{R}_n$ 中的齐次多项式，满足 $\deg(f_i) = \delta_i$，且 d 属于 $\mathbb{N}$。那么

$$\mathsf{P}_{d,n}(\boldsymbol{f}) \;=\; \{m\, f_i \mid i \in \{1, \ldots, s\},\; m \in \mathsf{Mon}_{d-\delta_i, n}\}$$

生成了所有属于 $\langle \boldsymbol{f} \rangle$、次数为 d 的齐次多项式构成的 $\mathbb{K}$-向量空间。

证明。 令 I 表示理想 $\langle \boldsymbol{f} \rangle$。我们证明

$$I \cap \mathcal{R}_n^{(d)} \;=\; \mathrm{Span}_{\mathbb{K}}\left(\mathsf{P}_{d,n}(\boldsymbol{f})\right).$$

(⊇) 每个多项式 mf_i 都属于 $I \cap \mathcal{R}_n^{(d)}$；线性组合保持这一性质。

(⊆) 反过来，设 f 属于 $I \cap \mathcal{R}_n^{(d)}$。若 $f = 0$，则 f 属于 $\mathsf{Span}_{\mathbb{K}}(\mathsf{P}_{d,n}(\boldsymbol{f}))$. 假设 $f \neq 0$。由于 f 属于 I，我们可以写成 $f = \sum_{i=1}^s u_i f_i$，其中 $u_i \in \mathcal{R}_n$。根据假设，$f \neq 0$，因此存在 $1 \leq i \leq s$ 使得 $u_i \neq 0$。我们用 $\mathscr{Q}$ 表示这类整数的集合。

对于 $i \in \mathscr{Q}$，记

$$u_i = \sum_{\boldsymbol{x}^{\boldsymbol{\beta}} \in \mathrm{Supp}(u_i)} b_{i,\boldsymbol{\beta}}\, \boldsymbol{x}^{\boldsymbol{\beta}}, \qquad f_i = \sum_{\boldsymbol{x}^{\boldsymbol{\alpha}} \in \mathrm{Supp}(f_i)} a_{i,\boldsymbol{\alpha}}\, \boldsymbol{x}^{\boldsymbol{\alpha}},$$

其中 $a_{i,\,\boldsymbol{\alpha}}$，$b_{i,\,\boldsymbol{\beta}} \in \mathbb{K}$。于是

$$u_i f_i \;=\; \sum_{\substack{\boldsymbol{x}^{\boldsymbol{\beta}} \in \mathrm{Supp}(u_i) \\ \boldsymbol{x}^{\boldsymbol{\alpha}} \in \mathrm{Supp}(f_i)}} a_{i,\boldsymbol{\alpha}} b_{i,\boldsymbol{\beta}}\, \boldsymbol{x}^{\boldsymbol{\alpha}+\boldsymbol{\beta}}, \quad \text{so} \quad f \;=\; \sum_{i \in \mathscr{Q}} \sum_{\substack{\boldsymbol{x}^{\boldsymbol{\beta}} \in \mathrm{Supp}(u_i) \\ \boldsymbol{x}^{\boldsymbol{\alpha}} \in \mathrm{Supp}(f_i)}} a_{i,\boldsymbol{\alpha}} b_{i,\boldsymbol{\beta}}\, \boldsymbol{x}^{\boldsymbol{\alpha}+\boldsymbol{\beta}}.$$

根据 $|\boldsymbol{\beta}| = d - \delta_i$ 是否成立对各项分类，可得

$$f \;=\; \underbrace{\sum_{i \in \mathscr{Q}} \sum_{\substack{\boldsymbol{x}^{\boldsymbol{\alpha}} \in \mathrm{Supp}(f_i) \\ \boldsymbol{x}^{\boldsymbol{\beta}} \in \mathrm{Supp}(u_i), |\boldsymbol{\beta}| \neq d-\delta_i}} a_{i,\boldsymbol{\alpha}} b_{i,\boldsymbol{\beta}}\, \boldsymbol{x}^{\boldsymbol{\alpha}+\boldsymbol{\beta}}}_{\text{degree} \neq d} \;+\; \underbrace{\sum_{i \in \mathscr{Q}} \sum_{\substack{\boldsymbol{x}^{\boldsymbol{\alpha}} \in \mathrm{Supp}(f_i) \\ \boldsymbol{x}^{\boldsymbol{\beta}} \in \mathrm{Supp}(u_i), |\boldsymbol{\beta}| = d-\delta_i}} a_{i,\boldsymbol{\alpha}} b_{i,\boldsymbol{\beta}}\, \boldsymbol{x}^{\boldsymbol{\alpha}+\boldsymbol{\beta}}}_{\text{homogeneous of degree } d}.$$

由于 f 是次数为 $d \geq 0$ 的齐次多项式，上面的第一项求和为零。因此

$$f \;=\; \sum_{i \in \mathscr{Q}} \tilde{u}_i\, f_i, \quad \text{where } \tilde{u}_i \;=\; \sum_{\substack{\boldsymbol{x}^{\boldsymbol{\beta}} \in \mathrm{Supp}(u_i) \\ |\boldsymbol{\beta}| = d-\delta_i}} b_{i,\boldsymbol{\beta}}\, \boldsymbol{x}^{\boldsymbol{\beta}} \in \mathcal{R}_n^{(d-\delta_i)}.$$

由于每个 $\tilde{u}_i f_i$ 都属于 $\mathsf{Span}_{\mathbb{K}}\big(\{\, mf_i \mid i \in \{1, \ldots, s\}, m \in \mathsf{Mon}_{d-\delta_i,\; n}\}\big)$，故得证。 □

引理 2.4。 设 $\boldsymbol{f} = (f_1, \ldots, f_s)$ 是 $\mathcal{R}_n$ 中的非零多项式序列，满足 $\mathsf{次数}(f_i) = \delta_i$，并设 $\mathsf{齐次部分}(\boldsymbol{f})$ 是正则序列。对于任意组合 $w = q_1 f_1 + \cdots + q_s f_s$，其中 w、q_1、…、q_s 属于 $\mathcal{R}_n$，满足 $\mathsf{次数}(w) < d$，且对于所有 i，q_i 要么为零，要么为 $d - \delta_i$ 次齐次多项式，存在多项式 p_1、…、p_s，使得 $w = p_1 f_1 + \cdots + p_s f_s$，并且对于所有 i，$\mathsf{次数}(p_i) < d - \delta_i$。

证明。 证明的第一部分表明，对于所有 $\{1,\dots,s\}^2$ 中满足 $i \geq j$ 的 $(i,\ j)$，存在一个齐次多项式 $a_{i,\ j}$，该多项式为零或次数为 $d-\delta_i-\delta_j$，使得对于所有 $\{1,\dots,s\}$ 中的 k，我们有

$$\sum_{j=1}^{k}\left(q_j+\sum_{i=k+1}^{s}a_{i,j}\,\mathsf{hom}(f_i)\right)\mathsf{hom}(f_j)=0 \tag{1.k}$$

and

$$q_k=-\sum_{i=k+1}^{s}a_{i,k}\,\mathsf{hom}(f_i)+\sum_{j=1}^{k}a_{k,j}\,\mathsf{hom}(f_j). \tag{2.k}$$

此外，我们证明，对于所有 k 属于 $\{1,\dots,s\}$的情况，都可以将 $a_{k,\ k}$ 取为零 .

我们先证明（1.s）和（2.s）。由于 $w=\sum_{j=1}^{s}q_jf_j$ 的次数满足 $\mathsf{deg}(w)<d$，因此 w 的 d 次齐次分量为零。又因为对于所有 j 属于 $\{1,\dots,s\}$的情况，多项式 q_j 要么为零，要么是 $d-\delta_j$ 次齐次多项式，且 $\mathsf{deg}(f_j)=\delta_j$，于是可得:

$$\sum_{j=1}^{s}q_j\,\mathsf{hom}(f_j)=0. \tag{1.s}$$

这意味着 q_s 齐次(f_s) 属于理想 $\langle$齐次$(f_1)\dots,$齐次$(f_{s-1})\rangle$。由于序列 齐次$(\boldsymbol{f})$是正则的，根据定义 2.1，多项式 q_s 可以写成:

$$q_s=\sum_{j=1}^{s-1}a_{s,j}\,\mathsf{hom}(f_j)$$

其中，对于所有 j属于 $\{1,\dots,s-1\}$的情况，$a_{s,\ j}$是 $\mathcal{R}_n$的一个元素。根据假设，如果 q_s不为 0，则它是 $d-\delta_s$次齐次多项式，而 $\mathsf{hom}(f_1)\dots,\mathsf{hom}(f_{s-1})$ 分别是 $\delta_1,\ \dots,\ \delta_s$次齐次多项式。因此，根据引理 2.3，多项式 $a_{s,\ j}$ 可以取为零，或取为 $d-\delta_s-\delta_j$ 次齐次多项式，其中$1\leq j\leq s-1$。令 $a_{s,\ s}=0$，我们可以写成

$$q_s=\sum_{j=1}^{s}a_{s,j}\,\mathsf{hom}(f_j). \tag{2.s}$$

如果 q_s 为零，我们令 $a_{s,j}=0$，其中 $1\leq j\leq s$。由此可得 (1.s) 和 (2.s)。

现在我们采用递减归纳法。取 $k\in\{1,\dots,s-1\}$，并假设对于 $\{k+1,\dots,s\}$ 中所有的 ℓ，命题 (1.ℓ) 和 (2.ℓ) 都成立。我们先从 (1.k) 开始，证明 (1.k) 和 (2.k)。记 (1.$k+1$):

$$\sum_{j=1}^{k+1}\left(q_j+\sum_{i=k+2}^{s}a_{i,j}\,\mathsf{hom}(f_i)\right)\mathsf{hom}(f_j)=0. \tag{1.$k+1$}$$

利用 (2.$k+1$) 替换并分离求和中的最后一项，可得

$$\mathsf{hom}(f_{k+1})\sum_{j=1}^{k+1}a_{k+1,j}\,\mathsf{hom}(f_j)+\sum_{j=1}^{k}\left(q_j+\sum_{i=k+2}^{s}a_{i,j}\,\mathsf{hom}(f_i)\right)\mathsf{hom}(f_j)=0.$$

由于根据我们的归纳假设，$a_{k+1,k+1}=0$，这也可以表述如下:

$$\sum_{j=1}^{k}\left(q_j+\sum_{i=k+1}^{s}a_{i,j}\,\mathsf{hom}(f_i)\right)\mathsf{hom}(f_j)=0$$

由此可得 (1.k)。

现在，我们证明 (2.k)，并令 $f=q_k+\sum_{i=k+1}^{s}a_{i,k}\,\mathsf{hom}(f_i)$。由于根据 (1.$k$)，我们有

$$f\,\mathsf{hom}(f_k)=-\sum_{j=1}^{k-1}\left(q_j+\sum_{i=k+1}^{s}a_{i,j}\,\mathsf{hom}(f_i)\right)\mathsf{hom}(f_j),$$

又由于 $\mathsf{hom}(\boldsymbol{f})$ 是一个正则序列，我们推得 $f \in \langle \mathsf{hom}(f_1) \dots, \mathsf{hom}(f_{k-1}) \rangle$。由于 $a_{i,j}$（分别为 q_j）为零或次数为 $d-\delta_i-\delta_j$（分别为 $d-\delta_j$）的齐次多项式，因此多项式 f 要么为零，要么是次数为 $d-\delta_k$的齐次多项式。

因此，将引理 2.3 应用于 $\langle \mathsf{hom}(f_1) \dots, \mathsf{hom}(f_{i-1}) \rangle$，存在齐次多项式 $a_{k,\ j}$，若其不为 0，则次数为 $d-\delta_k-\delta_j$，且 $j \mathsf{in}\ \{1,\dots,j\}$，使得

$$f = \sum_{j=1}^{k-1} a_{k,j}\, \mathsf{hom}(f_j)$$

再令 $a_{k,\ k} = 0$，即可证明 $(2.k)$。

现在我们可以证明该引理的陈述。考虑多项式 $(b_{i,\ j})_{1\le i\le s,\ 1\le j\le s}$，其中当 $i \ge j$ 和 $b_{i,\ j} = -a_{j,\ i}$ 时，$b_{i,\ j} = a_{i,\ j}$；当 $j > i$ 时，取相应定义。注意，方阵 $(b_{i,\ j})_{1\le i\le s,\ 1\le j\le s}$ 是反对称的，并且对所有 $i \mathsf{in}\ \{1,\dots,s\}$:

$$q_i = \sum_{j\in\{1,\dots,s\}} b_{i,j}\, \mathsf{hom}(f_j) \tag{$*$}$$

由 $(2.i)$ 可得。

~对所有 $i \mathsf{in}\ \{1,\dots,s\}$，写作 $f_i = \mathsf{hom}(f_i) + f_i$，并且

$$\begin{aligned} w &= \sum_{i\in\{1,\dots,s\}} q_i f_i = \sum_{i\in\{1,\dots,s\}} q_i \tilde{f}_i + \sum_{i\in\{1,\dots,s\}} q_i\, \mathsf{hom}(f_i) = \sum_{i\in\{1,\dots,s\}} q_i \tilde{f}_i && (\text{by } (1.s)) \\ &= \sum_{i,j\in\{1,\dots,s\}} b_{i,j}\, \mathsf{hom}(f_j)\tilde{f}_i = \sum_{i,j\in\{1,\dots,s\}} b_{i,j} f_j \tilde{f}_i - \sum_{i,j\in\{1,\dots,s\}} b_{i,j} \tilde{f}_j \tilde{f}_i. && (\text{by } (*)) \end{aligned}$$

由于矩阵 $(b_{i,\ j})_{1\le i\le s,\ 1\le j\le s}$ 是反对称的，且 $\mathcal{R}_n$ 是交换的，因此该和~ ~$\sum_{i,\ j\in\{1,\dots,s\}} b_{i,\ j} f_j f_i$ 等于零。这意味着

$$w = \sum_{i,j\in\{1,\dots,s\}} b_{i,j} f_j \tilde{f}_i = \sum_{i,j\in\{1,\dots,s\}} b_{i,j} \tilde{f}_i f_j.$$

对于所有属于 $\{1,\dots,s\}$ 的 j，令:

$$p_j = \sum_{i\in\{1,\dots,s\}} b_{i,j} \tilde{f}_i.$$

~还需证明 $\deg(p_j) < d-\delta_j$。根据定义，$\deg(p_j) \le \max^{i\in\{1,\dots,s\}}(\deg(b_{i,\ j}) + \deg(f_i))$ ~，而对于 $1 \le i \le s$，$\deg(f_i) < \delta_i$，且 $\deg(b_{i,\ j}) \le d-\delta_i-\delta_j$。这意味着 $\deg(b_{i,\ j}) + \deg(f_i) < d-\delta_j$。由于这对所有属于 $\{1,\dots,s\}$ 的 i 都成立，因此 $\deg(p_j) < d-\delta_j$。□

现在我们可以证明命题 2.2。

命题 2.2 的证明。我们令 $E = \{i \in \{1,\dots,s\} \mid \deg(q_i) = d-\delta_i\}$ 并将 w 分解如下

$$\begin{aligned} w &= \sum_{i\in\{1,\dots,s\}} q_i f_i = \left(\sum_{i\in\{1,\dots,s\}} (q_i - \mathsf{hom}(q_i)) f_i \right) + \left(\sum_{i\in\{1,\dots,s\}} \mathsf{hom}(q_i) f_i \right) \\ &= \left(\sum_{i\in\{1,\dots,s\}} (q_i - \mathsf{hom}(q_i)) f_i \right) + \left(\sum_{i\notin E} \mathsf{hom}(q_i) f_i \right) + \left(\sum_{i\in E} \mathsf{hom}(q_i) f_i \right). \end{aligned}$$

根据假设，多项式

$$w - \left(\sum_{i\in\{1,\dots,s\}} (q_i - \mathsf{hom}(q_i)) f_i \right) - \left(\sum_{i\notin E} \mathsf{hom}(q_i) f_i \right)$$

的次数严格小于 d。然后可以将引理 2.4 应用于最后一个求和项。这得出 w的以下表达式:

$$\begin{aligned} w &= \left(\sum_{i\in\{1,\dots,s\}} (q_i - \mathsf{hom}(q_i))f_i\right) + \left(\sum_{i\notin E} \mathsf{hom}(q_i)f_i\right) + \left(\sum_{i\in\{1,\dots,s\}} p_i f_i\right) \\ &= \left(\sum_{i\notin E}(q_i + p_i)f_i\right) + \left(\sum_{i\in E}(q_i - \mathsf{hom}(q_i) + p_i)f_i\right) \end{aligned}$$

其中 $\deg(p_i) < d - \delta_{i\circ}$ 如果 i 不属于 E，那么我们有 $\deg(q_i) < d - \delta_i$，这意味着 $\deg(q_i + p_i) < d - \delta_i$，并令 $h_i = q_i + p_{i\circ}$ 如果 i 属于 E，那么 $\deg(q_i - \mathsf{hom}(q_i)) < d - \delta_i$，这意味着 $\deg(q_i - \mathsf{hom}(q_i) + p_i) < d - \delta_i$，并令 $h_i = q_i - \mathsf{hom}(q_i) + p_{i\circ}$ 至此证明完成。 □

3. 临界对

本节的主要结果陈述于定理 3.4中，并明确揭示了 Buchberger 型算法中所选对的某种结构（见 [6]）。这种结构源自 [22] 中提出的判据。

本节分为三个小节。第 3.1 节旨在证明定理 3.2，这是确立定理 3.4 的一项关键预备结果。在第3.2 节中，我们将介绍陈述定理 3.4 所需的背景和记号，并给出若干用于证明该定理的预备引理；证明见第 3.3 节。

3.1. 关于单项式阶梯

我们首先介绍定义和记号。对于 $\mathcal{R}_n$ 中的单项式 $\succ$，我们采用经典记号和术语，涉及（可容许的）单项式序，以及非零多项式 f 的首项单项式 $\mathsf{lm}_\succ(f)$、首项 $\mathsf{lt}_\succ(f)$ 和首项系数 $\mathsf{lc}_\succ(f)$（更多详情见 [8, 第 2 章第 2] 节）。对于子集 $S \subseteq \mathcal{R}_n$，我们用 $\mathsf{lm}_\succ(S)$ 表示其元素的首项单项式所构成的集合 S。

我们回顾一下，对于整数 i，集合 Mon_i 是 $\mathcal{R}_i$ 的单项式集合。设 $f_1, \dots, f_s$ 是环 $\mathcal{R}_n$ 中的多项式，并令 $I = \langle f_1, \dots, f_s\rangle$。对于 $\mathcal{R}_n$ 上给定的单项式序 $\succ$，我们首先定义

$$\mathscr{B}(I,\succ) = \mathsf{Mon}_n \setminus \mathsf{lm}_\succ(I)$$

不是 I 中多项式首项单项式的单项式集合，即 $\mathcal{R}_n/I$ 的单项式基（例如参见 [8, 第 5 章第 3 节命题 4]）。随后，通过与 Mon_i 取交集来细化此集合，定义 $\mathscr{B}_i(I,\succ) = \mathscr{B}(I,\succ) \cap \mathsf{Mon}_i$，接着再按次数细化，定义

$$\mathscr{B}_{d,i}(I,\succ) = \{m \mid m \in \mathscr{B}_i(I,\succ) \text{ and } \deg(m) = d\}.$$

注意，$\mathscr{B}(I,\succ) = \mathscr{B}_n(I,\succ)$；对于所有 $i \in \{1,\dots,n\}$，有 $\mathscr{B}_{i-1}(I,\succ) \subset \mathscr{B}_i(I,\succ)$；并且我们有$\mathscr{B}_i(I,\succ) = \bigsqcup_{d\geq 0} \mathscr{B}_{d,i}(I,\succ)$。

For 为方便读者，我们回顾稳定性的概念，参见例如 [30, 定义 4.2。2] .

定义 3.1。若 S 是 $\mathcal{R}_n$ 的单项式集合，则称其为稳定的，当且仅当对于 S 中任意单项式 m，若 m 整除 x_i，则对于所有 $j < i$，$\frac{x_j m}{x_i}$ 都属于 S。

我们用 $G(I,\succ)$ 表示 I 的约化的 $\succ$-格罗布纳基。定义以下集合:

- $G_{d,*}(I,\succ)$ 是 $G(I,\succ)$ 中次数为 d 的元素集合;
- $G_{*,i}(I,\succ)$ 是 $G(I,\succ)$ 中首项单项式属于 $\mathcal{R}_i$ but not in $\mathcal{R}_{i-1}$ 的元素集合;
- $G_{d,i}(I,\succ) = G_{d,*}(I,\succ) \cap G_{*,i}(I,\succ)$。

注意，$G(I,\succ) = \bigsqcup_{d=0}^{\infty} G_{d,*}(I,\succ) = \bigsqcup_{i=1}^{n} G_{*,i}(I,\succ) = \bigsqcup_{d\in\mathbb{N}} \bigsqcup_{i\in\{1,\dots,n\}} G_{d,i}(I,\succ)$。

我们还引入了用于表示 $G(I,\succ)$ 的首项单项式的符号:

$$\begin{aligned} \mathscr{M}_{d,i}(I,\succ) &= \{\mathsf{lm}_\succ(g) \mid g \in G_{d,i}(I,\succ)\}, \\ \mathscr{M}_{*,i}(I,\succ) &= \{\mathsf{lm}_\succ(g) \mid g \in G_{*,i}(I,\succ)\}, \\ \mathscr{M}_{d,*}(I,\succ) &= \{\mathsf{lm}_\succ(g) \mid g \in G_{d,*}(I,\succ)\} \end{aligned}$$

最后， $\mathscr{M}(I,\succ) = \mathsf{lm}_{\succ}(G(I,\succ))$。

当理想 I 和单项式序 $\succ$ 可由上下文明确时，我们将省略它们。回顾一下，理想I 称为零维的，如果商 $\mathcal{R}_n/I$ 作为一个 $\mathbb{K}$-向量空间的维数有限（见[8, 第 2 章，第 2 节，命题 4]）。

定理 3.2。 取 $\delta \geq 0$, $n \geq 1$, $s \geq 1$，并考虑序列 $\boldsymbol{f} = (f_1, \ldots, f_s)$，其中元素属于 $\mathcal{R}_n$，次数为 δ和 $I = \langle \boldsymbol{f} \rangle$。设 $\succ$ 是 $\mathcal{R}_n$的单项式上的单项式序。假设 $\mathsf{lm}_{\succ}(I)$ 稳定，且I是零维的。取 ℓ 属于 $\{1, \ldots, n\}$，并取 m 属于 $\mathscr{B}_{\ell-1}(I,\succ)$。存在整数 $\alpha_{m,\ell}$，使得：

$$\alpha_{m,\ell} = \min_{k\in\mathbb{N}}\{k \mid m\, x_\ell^k \in \mathsf{lm}_{\succ}(I)\} \quad \text{and} \quad m\, x^{\alpha_{m,\ell}} \in \mathscr{M}_{*,\ell}(I,\succ).$$

此外，映射 ψ_ℓ： $m \in \mathscr{B}_{\ell-1}(I,\succ) \longmapsto m\, x^{\alpha_{m,\ell}} \in \mathscr{M}_{*,\ell}(I,\succ)$ 是一个双射。

证明。取 $\ell \in \{1, \ldots, n\}$和 $m \in \mathscr{B}_{\ell-1}(I,\succ)$。由于 I是零维的，存在 k使得$x_\ell^k \in \mathsf{lm}_{\succ}(I)$（例如参见 [3, 命题 12.7]）。这证明了对于 $\mathscr{B}_{\ell-1}(I,\succ)$ 中任意 m，α_m、ℓ 的存在性。我们首先证明 $m\, x^{\alpha_{m,\ell}}$ 属于 $\mathscr{M}_{*,\ell}(I,\succ)$。根据定义，$m\, x^{\alpha_{m,\ell}}$ 属于 $\mathcal{R}_\ell$。此外，由于$m \notin \mathsf{lm}_{\succ}(I)$且 $m\, x^{\alpha_{m,\ell}} \in \mathsf{lm}_{\succ}(I)$，我们推得 $\alpha_{m,\ell} \geq 1$，进而 $m\, x^{\alpha_{m,\ell}}$ 不属于 $\mathcal{R}_{\ell-1}$。接下来只需证明 $mx^{\alpha_{m,\ell}}$ 是 I的约化的 $\succ$-格罗布纳基中某个元素的首项单项式。

反设情况并非如此。这意味着存在一个单项式 m_0 属于 $\mathsf{lm}_{\succ}(I)$，它整除 $m\, x^{\alpha_{m,\ell}}$ 且不等于它。根据m_0 和 $mx^{\alpha_{m,\ell}}$ 在 x_ℓ 中的次数是否相同，我们分两种情况讨论。

情况 *1*。 假设 $m_0 = m_1\, x_\ell^k$满足 $m_1 \in \mathcal{R}_{\ell-1}$ 和 $k < \alpha_{m,\ell}$。因此， m_1 整除单项式m，进而有 $m\, x_\ell^k = \frac{m}{m_1} m_0$。我们推得 $m\, x_\ell^k \in \mathsf{lm}_{\succ}(I)$，其中 $k < \alpha_{m,\ell}$（因为根据假设， $m_0 \in \mathsf{lm}_{\succ}(I)$）。这与$\alpha_{m,\ell}$的极小性矛盾。

情况 2。假设 $m_0 = m_1\, x^{\alpha_{m,\ell}}$ 满足 $m_1 \in \mathcal{R}_{\ell-1}$。因此， m_1 整除 m 和 $m \neq m_1$。由于 m和 m_1 属于 $\mathcal{R}_{\ell-1}$，存在 $j < \ell$ 使得 $m_1\, x_j$ 整除 m_0。我们已证明 $\alpha_{m,\ell} \geq 1$。于是，x_ℓ 整除 m_0。根据假设，$\mathsf{lm}_{\succ}(I)$是稳定的，因此单项式 $m_0 x_j / x_\ell = m_1\, x_j\, x^{\alpha_{m,\ell}-1}$ 属于 $\mathsf{lm}_{\succ}(I)$。由于 $m_1\, x_j$整除 m 且 $\alpha_{m,\ell} - 1 < \alpha_{m,\ell}$，我们必然要对 $(m_1\, x_j)\, x^{\alpha_{m,\ell}-1}$ 应用情况 1，并推得它不属于 $\mathsf{lm}_{\succ}(I)$。这就得出矛盾，因此我们得出结论： $m_0 \notin \mathsf{lm}_{\succ}(I)$。所有 i

n all, we h保留此 blished th在 $m\, x_\ell^{\alpha_{m,\ell}}$ lies in $\mathscr{M}_{*,\ell}(I\ \succ)$.

现在我们证明双射这一结论。对于 $\mathscr{B}_{\ell-1}(I,\succ)$中的两个不同单项式 m_1 和 m_2， $m_1\, x^{\alpha_{m_1}}$、ℓ 与 $m_2\, x^{\alpha_{m_2}}$、ℓ 在前 $\ell - 1$ 个变量上的指数不同。这足以证明ψ_ℓ 是单射。剩下要证明 ψ_ℓ 是满射函数。设 $\widetilde{m} \in \mathscr{M}_{*,\ell}(I,\succ)$，并写作$\widetilde{m} = m\, x_\ell^\alpha$，其中 $m \in \mathcal{R}_{\ell-1}$。根据$\mathscr{M}_*$的定义，$\ell(I,\succ)$成立，因此 $\alpha > 0$。由于 $\widetilde{m}$ 是 I的约化 Gröbner 基中某个元素的首项单项式，对于 $\{0, \ldots, \alpha-1\}$ 中的所有 k，单项式 $m\, x_\ell^k$都不属于 $\mathsf{lm}_{\succ}(I)$（否则将与约化 Gröbner 基的极小性矛盾）。这意味着 $m \in \mathscr{B}_{\ell-1}(I,\succ)$以及 $\psi(m) = \widetilde{m}$。因此， ψ_ℓ 是满射，因而是双射。 □

3.2. 关于协同模

我们使用标准的分次反向字典序和分次字典序单项式序；简写为反向字典序和分次字典序，更多详情请参见 [8, 第 2 章，第 2 节，定义 6]。它们是 Mon_n 上的单项式序，记作 $\succ_{\mathrm{grevlex}}$ 和 $\succ_{\mathrm{grlex}}$。这里我们采用约定 $x_1 \succ_{\mathrm{grevlex}} \cdots \succ_{\text{反向字典序}} x_n$ 和$x_1 \prec_{\text{分次字典序}} \cdots \prec_{\text{分次字典序}} x_n$。对于 Mon_n中的 $(m_1, \ldots, m_\ell)$，其最小公倍数记作 $\mathrm{lcm}(m_1, \ldots, m_\ell)$。

设 $G = \{g_1, \ldots, g_r\}$ 是 $\mathcal{R}_n$ 中的一组多项式，其关于反向字典序的首项单项式两两不同。若 G 相对于 $\succ_{\mathrm{ap}}$ 有序，则称：

$$\forall (i,j) \in \{1, \ldots, r\}^2, \quad i < j \iff \mathsf{lm}_{\succ_{\mathrm{grevlex}}}(g_i) \prec_{\mathrm{grlex}} \mathsf{lm}_{\succ_{\mathrm{grevlex}}}(g_j).$$

让我们回顾一下在 [22, 命题 3.5] 中引入的 G 中元素的首项单项式的协同模的基 $L^\star(G)$ 的定义。对于 i, j, $k \in \{1, \ldots, r\}$，记

$$\boldsymbol{\lambda}_G(i) = \mathsf{lm}_{\succ_{\mathrm{grevlex}}}(g_i), \quad \boldsymbol{\lambda}_G(i,j) = \mathrm{lcm}(\boldsymbol{\lambda}_G(i), \boldsymbol{\lambda}_G(j)), \quad \text{and } \boldsymbol{\lambda}_G(i,j,k) = \mathrm{lcm}(\boldsymbol{\lambda}_G(i), \boldsymbol{\lambda}_G(j), \boldsymbol{\lambda}_G(k)).$$

$\mathcal{R}_n$中元素首项单项式的 Syzygies 模为 G

$$S^{(1)}(G) = \left\{ (p_1, \ldots, p_r) \,\middle|\, p_i \in \mathcal{R}_n \text{ and } \sum_{i=1}^{r} p_i \boldsymbol{\lambda}_G(i) = 0 \right\}.$$

对于所有 k 属于 $\{1,\dots,r\}$，令 $\boldsymbol{e}_k=(0,\ \dots\dots,\ 1,\ \dots\dots,\ 0)$ 为 $\mathbb{K}^r$ 第 k 个坐标向量。根据 [22, 第 3 节，2], 模 $S^{(1)}(G)$ 有一个泰勒基 $\mathscr{T}_{(1)}(G)=\{S_{i,j}\mid 1\le i<j\le r\}$，其中

$$S_{i,j}=\frac{\boldsymbol{\lambda}_G(i,j)}{\boldsymbol{\lambda}_G(i)}\boldsymbol{e}_i-\frac{\boldsymbol{\lambda}_G(i,j)}{\boldsymbol{\lambda}_G(j)}\boldsymbol{e}_j.$$

我们将下列序记为 $\succ_{\mathrm{syz}}$：在 $\mathscr{T}_{(1)}(G)$ 上，对于 $i<j$ 和 $k<\ell$，

$$\begin{array}{c} S_{i,j}\prec_{\mathrm{syz}} S_{k,\ell}\\ \Updownarrow\\ \boldsymbol{\lambda}_G(i,j)\prec_{\mathrm{grlex}}\boldsymbol{\lambda}_G(k,\ell)\ \text{or}\ \left(\boldsymbol{\lambda}_G(i,j)=\boldsymbol{\lambda}_G(k,\ell)\ \text{and}\ \left(j<\ell\ \text{or}\ \left(j=\ell\ \text{and}\ i<k\right)\right)\right).\end{array}$$

我们将 $\mathcal{B}(G)$ 定义为满足以下条件的 $S_{i,j}$（其中 $i<j$）的集合：存在 $k\in\{1,\dots,r\}\setminus\{i,j\}$，使得 (T$_1$) $\boldsymbol{\lambda}_G(i,j,k)=\boldsymbol{\lambda}_G(i,j)$，并且
(T$_2$) $S_{i,j}=\max_{\succ_{\mathrm{syz}}}\{S_{i,j},S_{\alpha,\beta},S_{\gamma,\delta}\}$，其中 $\alpha=\min(i,k)$ $\beta=\max(i,k)$ $\gamma=\min(j,k)$，且 $\delta=\max(j,k)$。
根据 [22, 命题 3.5], ，协同模 $S^{(1)}(G)$ 由以下元素生成

$$\mathscr{T}^\star(G)=\{S_{i,j}\mid 1\le i<j\le r, S_{i,j}\notin\mathcal{B}(G)\}.$$

对于任意非零多项式 f，我们将其变量指标 $\mathsf{idx}(f)$ 定义为唯一的整数 i，满足 $\{1,\dots,n\}$ 中的 $\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(f)$ 属于 $\mathcal{R}_i\setminus\mathcal{R}_{i-1}$。

定义 3.3. 设 $(t,f)\in\mathsf{Mon}_n\times\mathcal{R}_n$。若 $t=x_j$ 满足 $j<\mathsf{idx}(f)$，则称元组 (t,f) 为特殊的。

我们将 $\mathcal{A}_{\delta,\ n,\ s}$ 记为满足 $\boldsymbol{f}=(f_1,\dots,f_s)$ 的次数为 δ、属于 $\mathcal{R}_n$ 且满足 [40, 猜想 4。1]的齐次多项式序列集合。现在可以陈述定理3.4。

定理 3.4。 设 $\boldsymbol{f}$ 属于 $\mathcal{A}_{\delta,\ n,\ s}$、$\delta\ge 0$ 为非零整数，且 n、s 为非零整数，$I=\langle\boldsymbol{f}\rangle$ 假设为零维。设 $G=(g_1,\dots,g_r)$ 是 I 的约化 $\succ_{\mathrm{grevlex}}$-格罗布纳基，按 $\succ_{\mathrm{ap}}$ 有序排列。那么，对于任意满足 $S_{i,\ j}$ 属于 $\mathscr{T}^\star(G)$ 的 $1\le i<j\le r$，元组 $\begin{pmatrix}\boldsymbol{\lambda}_{G(i,\ j)}\boldsymbol{\lambda}_G(j) & g_j\end{pmatrix}$ 是特殊的。

我们先给出证明定理 3.4 所需的四个辅助引理。本节结束之前，我们沿用该定理陈述中的记号。

以下引理明确指出，当按次数递增考察生成元时，单项式阶梯会逐维闭合。

引理 3.5. 假设 $\boldsymbol{f}$ 属于 $\mathcal{A}_{\delta,n,s}$。设 i 和 j 属于 $\{1,\dots,n\}$，且满足 $i<j$。设 d 和 e 属于 $\mathbb{N}$，且满足 $d<e$。若 $G_{d,j}(I,\succ_{\mathrm{grevlex}})$ 非空，则 $G_{e,i}(I,\succ_{\mathrm{grevlex}})$ 为空。

证明。固定 j 属于 $\{1,\dots,n\}$ 且 d 属于 $\mathbb{N}$，并假设 $G_{d,j}(I,\succ_{\mathrm{grevlex}})$ 非空。取 m 为 $G_{d,j}(I,\succ_{\mathrm{grevlex}})$ 中任意元素关于 $\succ_{\mathrm{grevlex}}$ 的首项单项式。根据构造，m 属于 $\mathsf{Mon}_{d,j}\setminus\mathsf{Mon}_{d,j-1}$。根据反向字典序序的定义，对于所有 $\widetilde{m}$ 属于 $\mathsf{Mon}_{d,j-1}$ 的元素，我们有 $\widetilde{m}\prec_{\mathrm{grevlex}} m$。

设 c 为 $\sharp G_{d,\ *}(I,\ \succ_{\mathrm{grevlex}})$ 的基数。由于 $\boldsymbol{f}$ 属于 $\mathcal{A}_{\delta,\ n,\ s}$，因此可以应用 [40, 猜想 4.1]，并推得其中最大的单项式

$$\mathscr{E}=(\mathscr{B}(I,\succ_{\mathrm{grevlex}})\cap\mathsf{Mon}_{d,*})\bigsqcup\mathscr{M}_{d,*}(I,\succ_{\mathrm{grevlex}})$$

是 $G_{d,\ *}(I,\ \succ_{\mathrm{grevlex}})$ 的单项式。设 $\widetilde{m}$ 属于 $\mathsf{Mon}_{d,\ j-1}$。注意，若 $\widetilde{m}$ 不属于 $\mathscr{E}$，则根据 $\mathscr{B}(I,\ \succ_{\mathrm{grevlex}})$ 的定义，它属于 $\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(I)$。若 $\widetilde{m}$ 属于 $\mathscr{E}$，则它属于 $G_{d,\ *}(I,\ \succ_{\mathrm{grevlex}})$，因为对于 $\succ_{\mathrm{grevlex}}$，它大于 m。由于根据定义，$G_{d,\ *}(I,\ \succ_{\mathrm{grevlex}})$ 包含于 $\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(I)$，我们再次推得 $\widetilde{m}$ 属于 $\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(I)$。

令 $i<j$，并反设 $G_{e,\ i}(I,\ \succ_{\mathrm{grevlex}})$ 对某个 $e>d$ 非空。令 g 属于 $G_{e,\ i}(I,\ \succ_{\mathrm{grevlex}})$，于是 $\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(g)\in\mathsf{Mon}_{e,\ j-1}$。由假设，$e>d$，存在一个单项式 $\widetilde{m}$ 属于 $\mathsf{Mon}_{d,\ j-1}$，使得 $\widetilde{m}$ 整除 $\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(g)$，且 $\widetilde{m}\neq\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(g)$。根据上一段，$\widetilde{m}$ 属于 $\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(I)$。这与 g 属于 I 的约化的 $\succ_{\mathrm{grevlex}}$-格罗布纳基这一事实矛盾。 □

引理 3.6。 设 $\boldsymbol{f}$ 属于 $\mathcal{A}_{\delta,\ n,\ s}$，$\delta\ge 0$ 和 n,s 为非零整数，且 $I=\langle\boldsymbol{f}\rangle$。令 $G=(g_1,\dots,g_r)$ 为 I 的约化的 $\succ_{\mathrm{grevlex}}$-格罗布纳基，关于 $\succ_{\mathrm{ap}}$ 排序。对于满足 $1\le i<j\le r$ 的任意整数 i,j，有 $\mathsf{idx}(g_i)\le\mathsf{idx}(g_j)$。

证明。 记 $d = \deg(\boldsymbol{\lambda}_G(i))$ 和 $e = \deg(\boldsymbol{\lambda}_G(j))$。根据假设，我们有 $\boldsymbol{\lambda}_G(i) \prec_{\text{grlex}} \boldsymbol{\lambda}_G(j)$，因此$d \leq e$。

若 $e = d$，根据分次字典序的定义，有$\mathsf{idx}(g_i) \leq \mathsf{idx}(g_j)$。若 $d < e$，则$G_{d,\mathsf{idx}(g_i)}$和$G_{e,\mathsf{idx}(g_j)}$均非空。由引理3.5可知，$\mathsf{idx}(g_i) \leq \mathsf{idx}(g_j)$。 □

Lemm命题 3.7。设 $k < i < j$是 $\{1, \ldots, r\}$中的整数。若 $\boldsymbol{\lambda}_G(k)$ 整除 $\boldsymbol{\lambda}_G(i, j)$，则$S_{i,j} \notin \mathscr{T}^\star(G)$.

证明。假设 $\boldsymbol{\lambda}_G(k)$整除 $\boldsymbol{\lambda}_G(i, j)$。这意味着 $\boldsymbol{\lambda}_G(i, j) = \boldsymbol{\lambda}_G(k, i, j)$，并且 $\boldsymbol{\lambda}_G(k, i)$整除 $\boldsymbol{\lambda}_G(i, j)$。因此，$\deg(\boldsymbol{\lambda}_G(k, i)) < \deg(\boldsymbol{\lambda}_G(i, j))$或 $\boldsymbol{\lambda}_G(k, i) = \boldsymbol{\lambda}_G(i, j)$。首先，若不等式$\deg(\boldsymbol{\lambda}_G(k, i)) < \deg(\boldsymbol{\lambda}_G(i, j))$成立，则$S_{k,i} \prec_{\text{syz}} S_{i,j}$。若 $\boldsymbol{\lambda}_G(k, i) = \boldsymbol{\lambda}_G(i, j)$，利用$i < j$这一事实，我们也有$S_{k,i} \prec_{\text{syz}} S_{i,j}$。对$S_{k,j}$ 和$S_{i,j}$作类似论证，并利用 $k < i$这一事实，可得$S_{i,j} = \max_{\succ_{\text{syz}}}(S_{k,i}, S_{k,j}, S_{i,j})$。因此，根据 $\mathcal{B}(G)$和 $\mathscr{T}^\star(G)$的定义，Syzygy $S_{i,j}$ 不属于$\mathscr{T}^\star(G)$。 □

多项式 f 关于变量 x_i 的次数记作 $\deg_{x_i}(f)$。

引理 3.8. 设 $\boldsymbol{f}$属于 $\mathcal{A}_{\delta,n,s}$, $\delta \geq 0$和 n, s均为非零整数，且 $I = \langle \boldsymbol{f} \rangle$。设 $G = (g_1, \ldots, g_r)$是 I的约化的 $\succ_{\text{grevlex}}$- 格罗布纳基，关于 $\succ_{\text{ap}}$ 有序。考虑 $1 \leq i < j \leq r$，并令a 表示 $\mathsf{idx}(g_j)$。则有如下不等式:

$$\deg_{x_a}(\boldsymbol{\lambda}_G(i)) \leq \deg_{x_a}(\boldsymbol{\lambda}_G(j)).$$

证明。首先，引理 3.6 证明了 $\mathsf{idx}(g_i) \leq \mathsf{idx}(g_j) = a$。若 $\mathsf{idx}(g_i) < a$，则根据定义，$\deg_{x_a}(\boldsymbol{\lambda}_G(j)) > 0$ 且 $\deg_{x_a}(\boldsymbol{\lambda}_G(i)) = 0$，因此 $\deg_{x_a}(\boldsymbol{\lambda}_G(i)) < \deg_{x_a}(\boldsymbol{\lambda}_G(j))$。在证明的其余部分，我们考虑 $\mathsf{idx}(g_i) = a$ 的情形。由于 $G(I, \succ_{\text{grevlex}})$ 关于 $\succ_{\text{ap}}$有序，因此有 $\boldsymbol{\lambda}_G(i) \prec_{\text{grlex}} \boldsymbol{\lambda}_G(j)$，这意味着 $\deg(\boldsymbol{\lambda}_G(i)) \leq \deg(\boldsymbol{\lambda}_G(j))$。

首先，假设 $\deg(\boldsymbol{\lambda}_G(i)) = \deg(\boldsymbol{\lambda}_G(j))$。由于 $\mathsf{idx}(g_i) = \mathsf{idx}(g_j) = a$，单项式 $\boldsymbol{\lambda}_G(i)$ 和$\boldsymbol{\lambda}_G(j)$ 都属于 $\mathcal{R}_a \setminus \mathcal{R}_{a-1}$；再结合 $\boldsymbol{\lambda}_G(i) \prec_{\text{grlex}} \boldsymbol{\lambda}_G(j)$，可得 $\deg_{x_a}(\boldsymbol{\lambda}_G(i)) \leq \deg_{x_a}(\boldsymbol{\lambda}_G(j))$。

现在假设 $\deg(\boldsymbol{\lambda}_G(i)) < \deg(\boldsymbol{\lambda}_G(j))$。则存在一个属于 $\mathcal{R}_a$ 、整除$\boldsymbol{\lambda}_G(j)$的单项式 m ，使得 $\deg(m) = \deg(\boldsymbol{\lambda}_G(i))$。反设 $\deg_{x_a}(\boldsymbol{\lambda}_G(i)) > \deg_{x_a}(\boldsymbol{\lambda}_G(j))$。于是有 $\deg_{x_a}(\boldsymbol{\lambda}_G(i)) > \deg_{x_a}(\boldsymbol{\lambda}_G(j)) \geq \deg_{x_a}(m)$, 从而 $m \succ_{\text{grevlex}} \boldsymbol{\lambda}_G(i)$。由 $\boldsymbol{\lambda}_G(i) \in \mathrm{lm}_{\succ_{\text{grevlex}}}(G(I, \succ_{\text{grevlex}}))$ 以及 $\boldsymbol{f} \in \mathcal{A}_{\delta,n,s}$, 可推出 m 属于 $\mathrm{lm}_{\succ_{\text{grevlex}}}(I)$。由于$m$ 整除 $\boldsymbol{\lambda}_G(j)$且不同于它，这与 $\succ_{\text{grevlex}}$-格罗布纳基$G(I, \succ_{\text{grevlex}})$的极小性矛盾。

□

备注 *3.9*。假设 $\boldsymbol{f} \in \mathcal{A}_{\delta,n,s}$ ，即可推出 $lm_{\succ_{\text{grevlex}}}(\langle \boldsymbol{f} \rangle)$ 的稳定性。事实上，设 I 是由一个序列 $\boldsymbol{f}$ 生成的理想，且该序列属于 $\mathcal{A}_{\delta,n,s}$。根据 *[30,* 引理 *4.2.3]*，我们只需验证 $\mathscr{M}(I, \succ_{\text{grevlex}})$ 中单项式的稳定性。设 m 属于 $\mathscr{M}(I, \succ_{\text{grevlex}})$，且满足 x_i 整除 m。那么，关于反向字典序，带有 $j < i$ 的单项式 $\widetilde{m} = \frac{x_j m}{x_i}$ 大于带有 $j < i$ 的 m。由于 $\boldsymbol{f}$ 属于 $\mathcal{A}_{\delta,n,s}$, 因此 $\overline{\widetilde{m}}$ 属于 $lm_{\succ_{\text{grevlex}}}(I)$。于是 $lm_{\succ_{\text{grevlex}}}(I)$ 是稳定的。

3.3. 定理证明*3.4*

对于单项式 $m = x_1^{\epsilon_1} \cdots x_n^{\epsilon_n}$ 和自然数集中的整数 i，令 $\pi_i(m)$ 表示 $x_1^{\epsilon_1} \cdots x^{\epsilon}{}_i{}^{i}$.

取 $S_{i,\ j}$ 其中 $1 \leq i < j \leq r$。在证明的其余部分，我们采用以下记 号:

$$\mathsf{idx}(g_i) = a, \quad \boldsymbol{\lambda}_G(i) = \prod_{t=1}^{a} x_t^{\alpha_t} \quad \text{and} \quad \mathsf{idx}(g_j) = b, \quad \boldsymbol{\lambda}_G(j) = \prod_{t=1}^{b} x_t^{\beta_t}.$$

由于多项式序列 $\boldsymbol{f}$ 属于 $\mathcal{A}_{\delta,\ n,\ s}$，因此可应用引理 3.6 推得 有 $a \leq b$。

引理 3.10。 在上述记号和假设下，有 $\boldsymbol{\lambda}_{G(i,\ j)}\, \boldsymbol{\lambda}_G(j) \in \mathcal{R}_a$。

证明。 若 $a = b$，显然有 $\boldsymbol{\lambda}_{G(i,\ j)}\, \boldsymbol{\lambda}_G(j) \in \mathcal{R}_a$。 若 $a < b$，则

$$\frac{\boldsymbol{\lambda}_G(i, j)}{\boldsymbol{\lambda}_G(j)} = \left(\prod_{t=1}^{a} x_t^{\max(\alpha_t, \beta_t) - \beta_t} \right) \left(\prod_{t=a+1}^{b} x_t^{\max(\alpha_t, \beta_t) - \beta_t} \right).$$

因为根据定义，对于所有的 $t > a$、 $\alpha_t = 0$，我们可以推出 $\boldsymbol{\lambda}_{G(i,j)}\, \boldsymbol{\lambda}_G(j) = \left(\prod_{t=1}^{a} x^{\max(\alpha_t, \beta_t}{}_t{}^{-\beta_t} \right)$，它属于 $\mathcal{R}_a$。 □

我们来证明，或者 $\left(\boldsymbol{\lambda}_{G(i,j)}\, \boldsymbol{\lambda}_G(j) \quad g_j \right)$ 是特殊的，或者 $S_{i,j}$ 不属于 $\mathscr{T}^\star(G)$。我们进行若干分类讨论，首先考察 a 和 b 是否相等（回想一下，我们已经证明了 $a \leq b$）。

情况 *1*： $a < b$。由于 g_i 和 g_j 是一个极小 $\succ_{\text{grevlex}}$-格罗布纳基的元素， $\boldsymbol{\lambda}_G(i)$ 不整除$\boldsymbol{\lambda}_G(j)$。由此可知，存在 c 属于 $\{1,\ldots,a\}$，使得 $\alpha_c > \beta_c$。这意味着 x_c 整除$\boldsymbol{\lambda}_{G(i,j)}$ $\boldsymbol{\lambda}_{G(j)}$。考虑：

$$\mu = \pi_a\left(x_c\boldsymbol{\lambda}_G(j)\right) = x_c\prod_{t=1}^{a} x_t^{\beta_t}.$$

显然，单项式 μ 属于 $\mathcal{R}_a$。根据 μ 属于 $\mathscr{B}_a(I,\ \succ_{\text{grevlex}})$ 还是属于 $\text{lm}^{\succ_{\text{grevlex}}}(I)$，我们分情况讨论。

情况 1.1： μ **属于** $\mathscr{B}_a$ $(I,\ \succ_{\text{grevlex}})$。由于 $\boldsymbol{f}$ 属于 $\mathcal{A}_{\delta,\ n,\ s}$，根据备注 3.9 可推知 $\text{lm}^{\succ_{\text{grevlex}}}$是稳定的。 $_{\text{x}}(I)$ 此外， I 根据假设是零维的。

因此，我们可以应用定理 3.2，令 $\ell = a+1$，并将 μ 在映射下的像记为 ν_{a+1}

$$\psi_{a+1} : m \in \mathscr{B}_a(I,\succ_{\text{grevlex}}) \mapsto m\ x_{a+1}^{\sigma_{m,\,a+1}} \in \mathscr{M}_{*,a+1}(I,\succ_{\text{grevlex}})$$

其中 $\sigma_{m,\ a+1} = \min_{k\in\mathbb{N}}\{k \mid mx_{a+1}^k \in \text{lm}^{\succ_{\text{grevlex}}}(I)\}$。

我们反复使用这一构造来定义一个单项式序列： μ_a、 μ_{a+1}、 ……， 以 $\mu_a = \mu$ 开始。该序列的后续元素递归定义如下。对于 $\ell \in \{a+1,\ldots,b\}$，有 $\deg_{x_\ell}(x_c\ \boldsymbol{\lambda}_G(j)) = \beta_\ell$。此外，对于该序列中属于 $\mathscr{B}_\ell$ $(I,\succ_{\text{grevlex}})$ 的元素 μ_ℓ，我们将 μ_ℓ 在映射 $\psi_{\ell+1}$ 下的像记为 $\nu_{\ell+1}$ （其中 $\psi_{\ell+1}$ 由定理 3.2 定义）。给定 μ_ℓ，我们将 $\mu_{\ell+1}$ 定义为：

(i) 若 $\beta_{\ell+1} < \deg_{x_{\ell+1}}(\nu_{\ell+1})$，则 $\mu_{\ell+1} = \mu_\ell\ x_{\ell+1}^{\beta_{\ell+1}}$；*(ii)* 否则， $\mu_{\ell+1} = \nu_{\ell+1}$ 不属于 $\mathscr{B}_{\ell+1}(I,$ $\succ_{\text{grevlex}})$，且该序列在$\mu_{\ell+1}$处稳定。

引理 3.11。我们沿用上述记号和假设。存在 $\mathfrak{e} \in \{a+1,\ldots,b\}$，使得该序列在 $\mu_{\mathfrak{e}}$ 处稳定，且对所有 $a \le \ell \le \mathfrak{e}-1$，都有 $\mu_\ell = \pi_\ell\left(x_c\boldsymbol{\lambda}_G(j)\right) = x_c\left(\prod_{t=1}^{\ell} x_t^{\beta_t}\right)$。此外，对于 $a \le \ell \le \mathfrak{e}-1$，单项式 μ_ℓ 属于 $\mathscr{B}_\ell(I,$ $\succ_{\text{grevlex}})$。

证明。根据序列 $\mu_a, \mu_{a+1}, \ldots$ 的定义，如果对某个 $\ell > a$，单项式 μ_ℓ 由 (ii) 定义，那么该序列中所有后续单项式也满足这一性质。我们将 $\mathfrak{e}$ 称为该序列中第一个由 (ii) 定义的单项式的指标；若从未出现这种情况，则令 $\mathfrak{e} = +\infty$。

显然，对于 $a \le \ell \le \mathfrak{e}-1$，单项式 μ_ℓ 属于 $\mathscr{B}_\ell(I,\ \succ_{\text{grevlex}})$。

现在，我们用归纳法证明，对于 $a \le \ell < \mathfrak{e}$， $\mu_\ell = \pi_\ell(x_c\boldsymbol{\lambda}_G(j))$。根据构造，该命题对 $\ell = a$成立。现在假设，对于满足 $a \le \ell < \mathfrak{e}$的 ℓ，有 $\mu_{\ell-1} = \pi_{\ell-1}(x_c\boldsymbol{\lambda}_G(j))$。由于我们有 $\ell < \mathfrak{e}$，根据构造可知，存在 $\mu_\ell = \mu_{\ell-1}x_\ell^{\beta_\ell}$，使得 $\beta_\ell = \deg_{x_\ell}(x_c\boldsymbol{\lambda}_G(j))$。由于我们有$\mu_{\ell-1} = \pi_{\ell-1}(x_c\boldsymbol{\lambda}_G(j))$且 $c \le a < \ell$，根据 $\boldsymbol{\lambda}_G(j)$的定义，结论得证。

剩下要证明 $\mathfrak{e}$属于 $\{a+1,\ldots,b\}$。为导出矛盾，假设情况并非如此。则 $\mathfrak{e} > b$。这意味着 $\mu_b = \pi_b\left(x_c\boldsymbol{\lambda}_G(j)\right)$ $= x_c\boldsymbol{\lambda}_G(j)$属于 $\mathscr{B}_b(I,\ \succ_{\text{grevlex}})$。这与 $\boldsymbol{\lambda}_G(j)$属于 $\mathscr{M}(I,\ \succ_{\text{grevlex}})$这一事实矛盾。因此， $\mathfrak{e}$属于 $\{a+1,\ldots,b\}$。 □

根据定理 3.2，单项式 $\mu_{\mathfrak{e}}$ 属于 $\mathscr{M}_{*,\mathfrak{e}}(I,\succ_{\text{grevlex}})$。因此，存在一个整数 k 属于$\{1,\ldots,r\}$，使得 $\boldsymbol{\lambda}_G(k) = \mu_{\mathfrak{e}}$。我们证明 $S_{i,j}$ 不属于 $\mathscr{T}^*(G)$，从而证明 T_1 和 T_2 均成立，使用指标 k。

根据引理 3.11， $\mu_{\mathfrak{e}-1} = \pi_{\mathfrak{e}-1}(x_c\boldsymbol{\lambda}_G(j)) = x_c\prod_{t=1}^{\mathfrak{e}-1} x_t^{\beta_t}$并且根据定义，我们有

$$\boldsymbol{\lambda}_G(k) = \mu_{\mathfrak{e}} = \psi_{\mathfrak{e}}\left(\mu_{\mathfrak{e}-1}\right) = \mu_{\mathfrak{e}-1}x_{\mathfrak{e}}^{\sigma} = x_c\left(\prod_{t=1}^{\mathfrak{e}-1} x_t^{\beta_t}\right)x_{\mathfrak{e}}^{\sigma}$$

其中， σ 是满足 $\mu_{\mathfrak{e}} \in \text{lm}^{\succ_{\text{grevlex}}}(I)$ 的最小整数。

由于 $\mu_{\mathfrak{e}}$ 是由 (ii) 定义的序列中的一个单项式，这意味着 $\sigma \le \beta_{\mathfrak{e}}$。由上面的表达式，我们可以推得 $\boldsymbol{\lambda}_G$ $(k,\ j) = x_c\boldsymbol{\lambda}_G(j)$。此外，根据定义，由于 c， $\boldsymbol{\lambda}_G(k)$ 整除 $\boldsymbol{\lambda}_G(i,\ j)$，我们推得 $\boldsymbol{\lambda}_G(i,\ j) = \boldsymbol{\lambda}_G(i,\ k,\ j)$。

根据引理 3.11， $a = \text{idx}(g_i) < \mathfrak{e} = \text{idx}(g_k)$。这意味着 $i < k$，特别是 $i \ne k$。此外，由于 $\deg_{x_c}(\boldsymbol{\lambda}_G(k))$ $= \deg_{x_c}(\boldsymbol{\lambda}_G(j)) + 1$， $\boldsymbol{\lambda}_G(k) \ne \boldsymbol{\lambda}_G(j)$，由此可得 $k \ne j$。至此，T_1 的证明完成。

现在，我们证明 $S_{i,\ j} \succ_{\text{syz}} S_{i,\ k}$ 和 $S_{i,\ j} \succ_{\text{syz}} S_{k,\ j}$，即 T_2。为此，只需证明 $\deg\left(\boldsymbol{\lambda}_G(k,j)\right) <$ $\deg\left(\boldsymbol{\lambda}_G(i,j)\right)$ 且 $\deg\left(\boldsymbol{\lambda}_G(i,k)\right) < \deg\left(\boldsymbol{\lambda}_G(i,j)\right)$；根据$\succ_{\text{syz}}$的定义，这就足够了。

我们在上一段中证明了 $\boldsymbol{\lambda}_G(k,j) = x_c\boldsymbol{\lambda}_G j$。事实上，根据定义，有 $x_c\boldsymbol{\lambda}_G(j) = x_c\prod_{t=1}^{b} x_t^{\beta_t} = \mu_a\prod_{t=a+1}^{b} x_t^{\beta_t}$。此外，回顾定义，$x_c$ 整除 $\boldsymbol{\lambda}_G(i,j)\boldsymbol{\lambda}_G(j)$。由此可得，$\boldsymbol{\lambda}_G(i,j) =$最小公倍数$(\boldsymbol{\lambda}_G(i)\ x_c\boldsymbol{\lambda}_G(j))$。于是有 $\boldsymbol{\lambda}_G(i,j) = \left(\prod_{t=a+1}^{b} x_t^{\beta_t}\right)$最小公倍数$(\boldsymbol{\lambda}_G(i)\ \mu_a)$。由于根据假设，$\mu_a \in \mathscr{B}_a(I,\succ_{\text{grevlex}})$ 且 $\boldsymbol{\lambda}_G(i) \in \text{lm}_{\succ_{\text{grevlex}}}(I)$，因此在 $\mathcal{R}_a$ 中存在一个正次数单项式 ν，使得最小公倍数 $(\boldsymbol{\lambda}_G(i)\ \mu_a) = \mu_a\nu$。由此可得 $\boldsymbol{\lambda}_G(i,j) = \left(\prod_{t=a+1}^{b} x_t^{\beta_t}\right)\mu_a\nu = x_c\boldsymbol{\lambda}_G(j)\ \nu$，进而 $\deg(\boldsymbol{\lambda}_G(k,j)) < \deg(\boldsymbol{\lambda}_G(i,j))$，如所要求。

回忆一下，$\boldsymbol{\lambda}_G(k) = \mu_{\mathfrak{e}} = x_c\left(\prod_{t=1}^{\mathfrak{e}-1} x_t^{\beta_t}\right)x_{\mathfrak{e}}^{\sigma} = \mu_a\left(\prod_{t=a+1}^{\mathfrak{e}-1} x_t^{\beta_t}\right)x_{\mathfrak{e}}^{\sigma}$，其中 $\mathfrak{e} > a$ 和 σ 已在上文定义，且 $\boldsymbol{\lambda}_G(i) = \prod_{t=1}^{a} x_t^{\alpha_t}$。因此，$\boldsymbol{\lambda}_G(i,k) = \text{lcm}(\boldsymbol{\lambda}_G(i)\ \boldsymbol{\lambda}_G(k)) = \text{lcm}(\boldsymbol{\lambda}_G(i)\ \mu_a)\left(\prod_{t=a+1}^{\mathfrak{e}-1} x_t^{\beta_t}\right)x_{\mathfrak{e}}^{\sigma}$。根据上文对 ν 的定义，我们可推得 $\text{lcm}(\boldsymbol{\lambda}_G(i)\ \boldsymbol{\lambda}_G(k)) = \nu\mu_a\left(\prod_{t=a+1}^{\mathfrak{e}-1} x_t^{\beta_t}\right)x_{\mathfrak{e}}^{\sigma} = \nu\boldsymbol{\lambda}_G(k)$。我们在上一段中证明了 $\boldsymbol{\lambda}_G(i,j) = x_c\boldsymbol{\lambda}_G(j)\nu$。因此，要证明 $\deg(\boldsymbol{\lambda}_G(i,k)) < \deg(\boldsymbol{\lambda}_G(i,j))$，只需证明不等式 $\deg(\boldsymbol{\lambda}_G(k)) < \deg(x_c\boldsymbol{\lambda}_G(j))$。根据构造，$\boldsymbol{\lambda}_G(k)$ 整除 $x_c\boldsymbol{\lambda}_G(j)$。由于 $\boldsymbol{\lambda}_G(k)$ 和 $\boldsymbol{\lambda}_G(j)$ 是一个极小基的首项单项式，$\boldsymbol{\lambda}_G(k)$ 不等于 $x_c\boldsymbol{\lambda}_G(j)$。这便推出了次数不等式，并完成了证明。

情形 1.2： μ **不属于** $\mathscr{B}_a(I,\ \succ_{\text{grevlex}})$。这意味着存在一个整数 k 属于 $\{1,\dots,r\}$，使得 $\boldsymbol{\lambda}_G(k)$ 整除 μ。此外，由于 μ 属于 $\mathcal{R}_a$，因此单项式 $\boldsymbol{\lambda}_G(k)$ 属于 $\mathcal{R}_a$，进而 $\text{idx}(g_k) \le a$。令 e 表示 $\text{idx}(g_k)$。

我们首先证明，当 $k \in \{i,j\}$、$\left(\underline{\boldsymbol{\lambda}_G(i,j)\,\boldsymbol{\lambda}_G(j)}\ \ g_j\right)$ 是特殊的。根据假设，$a < b$ 且 $e \le a$，因此我们有 $k \ne j$ 和 $k = i$。由于 $k = i$，所以 $\boldsymbol{\lambda}_G(i)$ 整除 μ。根据定义，μ 整除 $x_c\boldsymbol{\lambda}_G(j)$。于是，$\boldsymbol{\lambda}_G(i)$ 整除 $x_c\boldsymbol{\lambda}_G(j)$。我们推得 $\boldsymbol{\lambda}_G(i,j)$ 整除 $x_c\boldsymbol{\lambda}_G(j)$。由于 $\boldsymbol{\lambda}_G(j)$ 整除 $\boldsymbol{\lambda}_G(i,j)$，且 $\boldsymbol{\lambda}_G(j) \ne \boldsymbol{\lambda}_G(i,j)$（因为 G 是一个极小的 $\succ_{\text{grevlex}}$-格罗布纳基），所以 $\boldsymbol{\lambda}_G(i,j) = x_c\boldsymbol{\lambda}_G(j)$。由于 $1 \le c \le a$ 和 $a < b$，元组 $\left(\underline{\boldsymbol{\lambda}_G(i,j)\,\boldsymbol{\lambda}_G(j)}\ \ g_j\right)$ 是特殊的。

现在，我们证明，当 k 不能在 $\{i,j\}$ 中选取时，性质 T_1 和 T_2 成立，即 $S_{i,\,j} \notin \mathscr{T}^{\star}(G)$。我们从 T_2 开始。

我们有 $e \le a < b$。由于 $\boldsymbol{f}$ 位于 $\mathcal{A}_{\delta,\ n,\ s}$ 中，由引理 3.6 可知 $k < j$。由于 $\boldsymbol{\lambda}_G(k)$ 整除 μ，而 μ 整除 $x_c\boldsymbol{\lambda}_G(j)$，故 $\boldsymbol{\lambda}_G(k)$ 整除 $x_c\boldsymbol{\lambda}_G(j)$。我们推出 $\boldsymbol{\lambda}_G(k,j)$ 整除 $x_c\boldsymbol{\lambda}_G(j)$。注意，$\boldsymbol{\lambda}_G(i,j) = \text{lcm}(\boldsymbol{\lambda}_G(j)\ \boldsymbol{\lambda}_G(j)) = \left(\prod_{t=a+1}^{b} x_t^{\beta_t}\right)\text{lcm}\left(\boldsymbol{\lambda}_G(i)\ \prod_{t=1}^{a} x_t^{\beta_t}\right)$。根据 c 的定义，我们有最小公倍数 $\left(\boldsymbol{\lambda}_G(i)\ \prod_{t=1}^{a} x_t^{\beta_t}\right)$ =最小公倍数 $\left(\boldsymbol{\lambda}_G(i)\ x_c\prod_{t=1}^{a} x_t^{\beta_t}\right)$ =最小公倍数 $(\boldsymbol{\lambda}_G(i)\ \mu)$。根据假设，$\boldsymbol{\lambda}_G(i)$ 不整除 μ 和 $\mu \ne \boldsymbol{\lambda}_G(i)$。此外，由于 $\mu \in \text{lm}_{\succ_{\text{grevlex}}}(I)$，而 $\boldsymbol{\lambda}_G(i) \in \text{lm}_{\succ_{\text{grevlex}}}(G)$ 和 $\mu \ne \boldsymbol{\lambda}_G(i)$，我们推出 μ 不整除 $\boldsymbol{\lambda}_G(i)$。因此，存在一个单项式 ν，使得表达式最小公倍数 $\left(\boldsymbol{\lambda}_G(i)\ \prod_{t=1}^{a} x_t^{\beta_t}\right) = \nu x_c\prod_{t=1}^{a} x_t^{\beta_t}$，且 $\deg(\nu) \ge 1$ 成立。这意味着 $\boldsymbol{\lambda}_G(i,j) = \nu x_c\boldsymbol{\lambda}_G(j)$。由于 $\boldsymbol{\lambda}_G(k,j)$ 整除 $x_c\boldsymbol{\lambda}_G(j)$，我们推出不等式 $\deg(\boldsymbol{\lambda}_G(k,j)) < \deg(\boldsymbol{\lambda}_G(i,j))$ 成立。由此可得 $S_{k,\ j} \prec_{\text{syz}} S_{i,\ j}$。

由于 $\boldsymbol{\lambda}_G(k)$ 整除 μ，因此 $\boldsymbol{\lambda}_G(i,k)$ 整除 $\text{lcm}(\boldsymbol{\lambda}_G(i)\ \mu)$。此外，我们已经证明 $\boldsymbol{\lambda}_G(i,j) = \left(\prod_{t=a+1}^{b} x_t^{\beta_t}\right)\text{lcm}(\boldsymbol{\lambda}_G(i)\ \mu)$ 且 $\beta_b > 0$，由此可得 $\deg\ \boldsymbol{\lambda}_G(i,k) < \deg(\boldsymbol{\lambda}_G(i,j))$。因此，$S_{i,k} \prec_{\text{syz}} S_{i,j}$，且 $S_{i,j} = \max_{\succ_{\text{syz}}}\{S_{i,k}, S_{k,j}, S_{i,j}\}$。由此完成了对 T_2 的证明。

现在我们证明 T_1。只需证明单项式 $\boldsymbol{\lambda}_G(k)$ 整除 $\boldsymbol{\lambda}_G(i,j)$。由于 $\boldsymbol{\lambda}_G(k)$ 整除$x_c\prod_{t=1}^{a} x_t^{\beta_t}$，且根据 c 的定义，$x_c\prod_{t=1}^{a} x_t^{\beta_t}$ 整除 $\boldsymbol{\lambda}_G(i,j)$，因此可得 $\boldsymbol{\lambda}_G(i,k,j) = \boldsymbol{\lambda}_G(i,j)$。

情况 *2*：$a = b$。由于 $G(I,\ \succ_{\text{grevlex}})$ 是约化的，因此有 $\sharp(G_{*,\,1}(I,\ \succ_{\text{grevlex}})) \le 1$。由此可得$a \ge 2$（因为 $i < j$）。考虑 $\pi_{a-1}(\boldsymbol{\lambda}_G(i)) = \prod_{t=1}^{a-1} x_t^{\alpha_t}$以及 $\pi_{a-1}(\boldsymbol{\lambda}_G(j)) = \prod_{t=1}^{a-1} x_t^{\beta_t}$，并令 $\boldsymbol{\lambda}$ 为它们的最小公倍数。

首先假设 $\boldsymbol{\lambda} \notin \mathscr{B}_{a-1}(I,\succ_{\text{grevlex}})$。那么它属于 $\text{lm}_{\succ_{\text{grevlex}}}(I)$，并且存在 $k \in \{1,\dots,r\}$，使得 $\boldsymbol{\lambda}_G(k)$ 整除 $\boldsymbol{\lambda}$，且 $\text{idx}(g_k) < a$。由于 $\boldsymbol{f}$ 属于 $\mathcal{A}_{\delta,n,s}$，根据引理 3.6，可得 $k < i < j$。注意到 $\boldsymbol{\lambda}_G(k)$ 整除 $\boldsymbol{\lambda}_G(i,j)$。然后，根据引理 3.7，$S_{i,\ j}$ 不属于 $\mathscr{T}^{\star}(G)$。

现在，假设 $\boldsymbol{\lambda} \in \mathscr{B}_{a-1}(I,\ \succ_{\text{grevlex}})$。由于 $\boldsymbol{f}$ 属于 $\mathcal{A}_{\delta,\ n,\ s}$，引理 3.8 推出 $\alpha_a \le \beta_a$。这意味着 $\boldsymbol{\lambda}_G(i,\ j)\boldsymbol{\lambda}_G(j)$ 属于 $\mathcal{R}_{a-1}$。我们假设 $\left(\underline{\boldsymbol{\lambda}_G(i,\ j)\,\boldsymbol{\lambda}_G(j)}\ \ g_j\right)$ 不是特殊的，并证明 $S_{i,\ j}$ 不属于 $\mathscr{T}^{\star}(G)$。

由于 $\boldsymbol{\lambda}_G(i,j)\boldsymbol{\lambda}_G(j)$ 属于 $\mathcal{R}_{a-1}$，且 $\left(\underline{\boldsymbol{\lambda}_G(i,j)\,\boldsymbol{\lambda}_G(j)}\ \ g_j\right)$ 不是特殊的，因此 $\deg\left(\underline{\boldsymbol{\lambda}_G(i,j)\,\boldsymbol{\lambda}_G(j)}\right) \ge 2$。于是，可以将 $\underline{\boldsymbol{\lambda}_G(i,j)\,\boldsymbol{\lambda}_G(j)}$ 写成两个单项式 τ 和 κ 在 $\mathcal{R}_{a-1}$ 中的乘积，其中 τ 的次数为 2。

那么，存在一个变量 x_c，它整除单项式 τ，且 $c \in \{1, \dots a-1\}$。

注意到，根据假设，$\boldsymbol{\lambda} = \pi_{a-1}(\boldsymbol{\lambda}_G(i,j)) = \pi_{a-1}(\tau\kappa\boldsymbol{\lambda}_G(j))$ 属于 $\mathscr{B}_{a-1}(I, \succ_{\text{grevlex}})$。我们推得 $\pi_{a-1}(x_c\boldsymbol{\lambda}_G(j)) \in \mathscr{B}_{a-1}(I, \succ_{\text{grevlex}})$，因为它整除 $\pi_{a-1}(\tau\kappa\boldsymbol{\lambda}_G(j))$。由于 $\boldsymbol{f}$ 属于 $\mathcal{A}_{\delta,n,s}$，根据备注 3.9，我们推得 $\text{lm}_{\succ_{\text{grevlex}}}(I)$ 是稳定的。此外，根据假设，I 是零维的。因此，根据定理 3.2，存在 k 属于 $\{1, \dots, r\}$，使得 $\boldsymbol{\lambda}_G(k) = \psi_a(\pi_{a-1}(x_c\boldsymbol{\lambda}_G(j)))$。现在，我们证明 T_1。

可以将 $\boldsymbol{\lambda}_G(k) = \left(x_c \prod_{t=1}^{a-1} x_t^{\beta_t}\right) x_a^{\gamma}$ 写成某个 $\gamma > 0$。由于 $1 \le c \le a-1$，这意味着 $k \neq j$。另请注意，$\gamma < \beta_a$，因为 $\boldsymbol{\lambda}_G(j) \in \text{lm}_{\succ_{\text{grevlex}}}(G)$。我们推得 $\boldsymbol{\lambda}_G(j, k) = x_c\boldsymbol{\lambda}_G(j)$。

注意到 $\boldsymbol{\lambda}_G(k,i,j) = \text{lcm}(\boldsymbol{\lambda}_G(i,j)\ \boldsymbol{\lambda}_G(j,k))$，其中 $\boldsymbol{\lambda}_G(i,j) = \kappa\tau\boldsymbol{\lambda}_G(j)$，且 $\boldsymbol{\lambda}_G(j,k) = x_c\boldsymbol{\lambda}_G(j)$。这两者的最小公倍数是 $\kappa\tau\boldsymbol{\lambda}_G(j)$，因为 x_c 整除 τ。这证明了 T_1，，前提是 $k \notin \{i, j\}$，下面我们证明这一点。

由于 $\gamma < \beta_a$ 和 G 按照 $\succ_{\text{ap}}$ 排序，我们可以推出 $k < j$。由于 $\left(\underline{\boldsymbol{\lambda}_{G(i,\ j)}\boldsymbol{\lambda}_G(j)}\ \ g_j\right)$ 不是特殊的，且 $\boldsymbol{\lambda}_G(j,\ k) = x_c\boldsymbol{\lambda}_G(j)$，因此有 $i \neq k$。至此，T_1 的证明完成。

尚需证明 T_2。由上述段落可知，下列不等式成立

$$\deg(\boldsymbol{\lambda}_G(i,j)) \ge 2 + \deg(\boldsymbol{\lambda}_G(j)) > 1 + \deg(\boldsymbol{\lambda}_G(j)) \ge \deg(\boldsymbol{\lambda}_G(k,j))$$

这意味着 $S_{i,\ j} \succ_{\text{syz}} S_{k,\ j}$。

还要注意，$\boldsymbol{\lambda}_G(i,k) = \text{lcm}\left(\boldsymbol{\lambda}_G(i)\left(x_c \prod_{t=1}^{a-1} x_t^{\beta_t}\right) x_a^{\gamma}\right)$。根据 c 的定义，可知 $\boldsymbol{\lambda}_G(i,k)$ 等于 $\text{lcm}\left(\boldsymbol{\lambda}_G(i)\left(\prod_{t=1}^{a-1} x_t^{\beta_t}\right) x_a^{\gamma}\right) = x_a^{\sigma}\boldsymbol{\lambda}$，其中 $\sigma = \max(\gamma, \alpha_a)$。由于此前已证明 $\gamma < \beta_a$ 和 $\alpha_a \le \beta_a$，我们可以推出 $\boldsymbol{\lambda}_G(i,k)$ 整除 $\boldsymbol{\lambda}x_a^{\beta_a}$。因此，$\boldsymbol{\lambda}_G(i,k)$ 整除 $\boldsymbol{\lambda}_G(i,j)$。我们已经证明了 $j > k$。于是可得 $S_{i,\ j} \succ_{\text{syz}} S_{i,k}$。至此，$\mathsf{T}_2$ 的证明完成。

4. 关于单项式阶梯的形状

本节旨在证明定理 4.6，该定理明确描述了由 $\succ_{\text{grevlex}}$-格罗布纳基生成的某个极小 n 一般多项式中的若干首项单项式。

4.1. 截断多项式的格罗布纳基

我们先介绍一个辅助结果（下文的定理 4.1 ）。

对于齐次多项式 $f \in \mathcal{R}_n$，我们对 $1 \le j \le n-1$ 定义多项式 $\phi(f,j) \in \mathcal{R}_j$，即将其变量 $x_{j+1}, \dots, x_n$ 设为 0 后得到的多项式。按照约定，$\phi(f,n) = f$。注意，对于所有 $1 \le j \le n$，多项式 $\phi(f,j)$ 都是齐次多项式，且次数与 f 相同。对于一列

$$\text{q}_{\text{序列}}\ \boldsymbol{f} = (f_1, \dots f_s)\ \text{of poly}_{\text{名式}}\ ,\ {}^{\text{我们设定}}$$

$$\phi(\boldsymbol{f}, j) = (\phi(f_1, j), \dots, \phi(f_s, j))$$

对 j 在 $\{1, \dots n\}$。我们用 $I_j(\boldsymbol{f})$ 表示由 $\phi(\boldsymbol{f},\ j$ 的元素生成的 $\mathcal{R}_j$ 的 $\langle\phi(\boldsymbol{f},\ j)\rangle$).

定理 4.1。设 $\boldsymbol{f} = (f_1, \dots, f_s)$ 是 δ 次齐次多项式在 $\mathcal{R}_n$ 中构成的序列。设 $G(I, \succ_{\text{grevlex}})$ 是 $I = \langle\boldsymbol{f}\rangle$ 的约化 $\succ_{\text{grevlex}}$-格罗布纳基。设 j 是 $\{1, \dots, n\}$ 中的一个整数。

则理想 $I_j(\boldsymbol{f})$ 在 $\mathcal{R}_j$ 中的约化 $\succ_{\text{grevlex}}$-格罗布纳基 $G(I_j(\boldsymbol{f}) \succ_{\text{grevlex}})$ 为集合：

$$\{\phi(g,j) \mid g \in \bigsqcup_{i=0}^{j} G_{*,i}(I, \succ_{\text{grevlex}})\}.$$

定理 4.1 的证明依赖于下文的引理 4.3 和引理 4.4 以及对 Macaulay 矩阵性质的分析。

设 $\boldsymbol{f}$ 是 $\mathcal{R}_n$ 的一个有限子集，并按照 $\succ_1$ 赋予序；设 T 是按 $\succ_2$ 赋予序的单项式有限集合。矩阵 $\text{Mac}_{\succ_1,\ \succ_2}(\boldsymbol{f},\ T)$ 定义如下：其行由 $\boldsymbol{f}$ 中的元素索引，其列由 T 中按递减序排列的单项式索引。$\boldsymbol{f}$ 中行 f 与 T 中列 t 交叉处的元素，是多项式 f 中单项式 t 的系数。当上下文已确定这些序时，我们使用记号 $\text{Mac}(\boldsymbol{f},\ T)$。

在本文余下部分，我们采用如下约定：行阶梯形或行约化阶梯形矩阵的主元位于左侧。

注 4.2. 将 *Macaulay* 矩阵的一行 L 视为一个子矩阵。注意， L 是行阶梯形。矩阵 L 表示一个关联多项式 f。 L 的主元列对应于 f的首项单项式，所依据的是用于各列的单项式序。

令 $\boldsymbol{f} = (f_1, \dots, f_s)$ 为多项式序列，且 $\deg(f_i) = \delta$。对于 e 属于 $\mathbb{N}$的情形，如引理 2.3 中所述，我们定义集合

$$\mathsf{P}_{e,n}(\boldsymbol{f}) = \{m\ f_i \mid i \in \{1, \dots, s\}, m \in \mathsf{Mon}_{e-\delta,n}\},$$

该集合按下文定义的序 $\succ_{\boldsymbol{f}}$ 排列：

$$m_1\ f_{i_1} \succ_{\boldsymbol{f}} m_2\ f_{i_2} \iff m_1 \succ_{\text{grevlex}} m_2 \quad \text{or} \quad (m_1 = m_2 \quad \text{and} \quad i_1 > i_2).$$

在本小节余下部分中，我们假设对于所有 j 属于 $\mathbb{N}$ 且 d 属于 $\mathbb{N}$的情形，单项式集合 $\mathsf{Mon}_{d,j}$均按反向字典序排列。同样，集合 $\mathsf{P}_{e,n}(\boldsymbol{f})$ 按 $\succ_{\boldsymbol{f}}$排列。

引理 4.3。 令 $\boldsymbol{f} = (f_1, \dots, f_s)$ 为 $\mathcal{R}_n$中的次数为 δ 的齐次多项式序列，并令$e \in \mathbb{N}$。设 $G = G(I, \succ_{\text{grevlex}})$ 为理想 $I = \langle \boldsymbol{f} \rangle$的约化 $\succ_{\text{grevlex}}$-格罗布纳基。我们用E_e 表示矩阵的行最简阶梯形

$$\text{Mac}(\mathsf{P}_{e,n}(\boldsymbol{f}), \mathsf{Mon}_{e,n}).$$

那么，以下断言成立。

1. 矩阵 E_e 的行包含 G 中所有满足 $\deg(g) = e$ 的多项式 g。*2.* 设 g 是由 E_e 的某一行表示的非零多项式。多项式 g 属于 G， 当且仅当不存在由 E_d 的某一行表示且满足 $d < e$ 的多项式 h， 使得 $\mathsf{lm}_{\succ_{\text{grevlex}}}(h)$ 整除 $\mathsf{lm}_{\succ_{\text{grevlex}}}(g)$。

证明。 第一个断言已在 [33, 第 2] 节中提出；为求完整起见，我们在附录中给出一个明确的证明。

现在证明第二个断言。设 g 是由 E_e 的某一行表示的多项式。注意，根据引理 2.3 和 [31, 第 1.4 节, 定理 5], 对所有 $d \in \mathbb{N}$， E_d 的行生成了 $\mathbb{K}$-向量空间，即 d 中次数为 I的齐次多项式空间。因此，对于任意由 E_d 的某一行表示且满足 $d \le e$的 h， 都有 $h \in I$。

($\Longrightarrow$) 我们假设 g 属于 G。现在，考虑由 E_d 中对应于$d < e$的一行表示的多项式 h。反设 $\mathsf{lm}_{\succ_{\text{grevlex}}}(h)$ 整除 $\mathsf{lm}_{\succ_{\text{grevlex}}}(g)$。如前所述，多项式 h 属于 I。根据格罗布纳基的定义，存在多项式 p 属于 G， 使得 $\mathsf{lm}_{\succ_{\text{grevlex}}}(p)$ 整除 $\mathsf{lm}_{\succ_{\text{grevlex}}}(h)$。根据反向字典序的定义，有 $\deg(p) \le d$。由此可知，多项式 p 和 g 不可能相等，且 $\mathsf{lm}_{\succ_{\text{grevlex}}}(p)$ 整除 $\mathsf{lm}_{\succ_{\text{grevlex}}}(g)$。这是一个矛盾，因为 p 和 g 都属于 G，而假设 G是约化的。因此，这样的多项式 h 不可能存在。

($\Longleftarrow$) 假设不存在由 E_d 中的一行表示、且满足 $d < e$ 的多项式 h， 使得 $\mathsf{lm}_{\succ_{\text{grevlex}}}(h)$ 整除 $\mathsf{lm}_{\succ_{\text{grevlex}}}(g)$。由于 I中次数为 d的齐次多项式构成的 $\mathbb{K}$-向量空间，恰好由 E_d的各行生成，因此， E_d的主元列所对应的所有单项式，都是 I中次数为 d的所有可能的首项单项式。根据假设，这些首项单项式中，没有一个能整除所有 $d < e$对应的 $\mathsf{lm}_{\succ_{\text{grevlex}}}(g)$；然而， g 属于由所有次数为 e的齐次多项式构成的 $\mathbb{K}$-向量空间。这意味着， I 中的多项式没有任何首项单项式能整除 $\mathsf{lm}_{\succ_{\text{grevlex}}}(g)$，除 $\mathsf{lm}_{\succ_{\text{grevlex}}}(g)$本身外。由此可知，存在多项式 f 属于 G， 且 $\mathsf{lm}_{\succ_{\text{grevlex}}}(f) = \mathsf{lm}_{\succ_{\text{grevlex}}}(g)$。根据引理的第一条断言，$f$ 由 E_e中的一行表示。由于它们的首项单项式相同，且 E_e 处于行阶梯形，因此这一行与表示 g 的那一行相同。由此，正如所述， $f = g$和 g 属于 G。 □

令 $\boldsymbol{f} = (f_1, \dots, f_s)$ 是一个多项式序列。对于 $d \in \mathbb{N}$和 $j \in \{1, \dots, n\}$，我们定义集合

$$\mathsf{TP}_{d,j}(\boldsymbol{f}) = \{m\ \phi(f_i, j) \mid i \in \{1, \dots, s\}, m \in \mathsf{Mon}_{d-\delta,j}\},$$

我们按如下方式对其排序：

$$m_1\ \phi(f_{i_1}, j) \succ_{\boldsymbol{f}} m_2\ \phi(f_{i_2}, j)$$

若 $m_1 \succ_{\text{grevlex}} m_2$ 或 $m_1 = m_2$ 且 $i_1 > i_2$。

本节余下部分中，我们使用上文定义的序来排列 Macaulay 矩阵的行。

引理 4.4。 设 $\boldsymbol{f}=(f_1,\dots,f_s)$ 是一个次数为 δ、属于 $\mathcal{R}_n$ 的多项式序列。对于固定的 $d\geq 0$ 和 $j\in\{2,\dots,n\}$，*Macaulay* 矩阵 $\mathrm{Mac}(\mathsf{TP}_{d,j-1}(\boldsymbol{f}),\mathsf{Mon}_{d,j-1})$ 是 $\mathrm{Mac}(\mathsf{TP}_{d,j}(\boldsymbol{f}),\mathsf{Mon}_{d,j})$ 的一个子矩阵，构造方式如下：

$$\mathrm{Mac}(\mathsf{TP}_{d,j}(\boldsymbol{f}),\mathsf{Mon}_{d,j})=\begin{array}{c}\overbrace{\phantom{\mathrm{Mac}(\mathsf{TP}_{d,j-1}(\boldsymbol{f}),\mathsf{Mon}_{d,j-1})}}^{\mathsf{Mon}_{d,j-1}}\\ \left(\begin{array}{c|c}\mathrm{Mac}(\mathsf{TP}_{d,j-1}(\boldsymbol{f}),\mathsf{Mon}_{d,j-1}) & \\ \hline 0\ \cdots\ 0 & \\ \vdots\ \ \vdots & * \\ 0\ \cdots\ 0 & \end{array}\right)\\ \underbrace{\phantom{\mathrm{Mac}(\mathsf{TP}_{d,j-1}(\boldsymbol{f}),\mathsf{Mon}_{d,j-1})}}_{\mathsf{Mon}_{d,j}}\end{array}.$$

证明。首先，矩阵 $\mathbf{Mac}(\mathbf{TP}_{d,j}(\boldsymbol{f}),\mathbf{Mon}_{d,j})$ 的列以集合 $\mathbf{Mon}_{d,j}$ 的元素为索引，并按反向字典序排列。设 m_1 是 $\mathbf{Mon}_{d,j-1}$ 中的一个单项式，m_2 是 $\mathbf{Mon}_{d,j}\setminus\mathbf{Mon}_{d,j-1}$中的一个单项式。单项式 m_1 和 m_2 的次数相同，且对于所有 $\ell>j$，等式 $\deg_{x_\ell}(m_1)=\deg_{x_\ell}(m_2)=0$ 成立。此外，不等式 $\deg_{x_j}(m_1)<\deg_{x_j}(m_2)$ 成立，因为 $\deg_{x_j}(m_1)=0$ 且 $\deg_{x_j}(m_2)>0$。因此，我们得到 $m_1\succ_{\mathrm{grevlex}}m_2$。由此可推得，$\mathbf{Mon}_{d,j-1}$ 是 $\mathbf{Mon}_{d,j}$ 的一个子集，其中的元素都大于 $\mathbf{Mon}_{d,j}\setminus\mathbf{Mon}_{d,j-1}$中的任意元素。

接下来，我们定义以下多项式集合

$$S=\{m\ \phi(f_i,j)\mid i\in\{1,\dots,s\},\ m\in\mathsf{Mon}_{d-\delta,j-1}\}.$$

设 $m_1\ \phi(f_{i_1},j)$ 属于 S，且 $m_2\ \phi(f_{i_2},j)$ 属于 $\mathbf{TP}_{d,j}(\boldsymbol{f})\setminus S$。由于单项式 m_1 属于 $\mathbf{Mon}_{d-\delta,j-1}$，且 m_2 属于 $\mathbf{Mon}_{d-\delta,j}\setminus\mathbf{Mon}_{d-\delta,j-1}$，我们已经证明 $m_1\succ_{\mathrm{grevlex}}m_2$。由此可知，按照我们在 $\mathbf{TP}_{d,j}(\boldsymbol{f})$ 上使用的序，$m_1\ \phi(f_{i_1},j)$ 大于 $m_2\ \phi(f_{i_2},j)$。我们推得，S 是 $\mathbf{TP}_{d,j}(\boldsymbol{f})$ 的子集，其中的元素均大于 $\mathbf{TP}_{d,j}(\boldsymbol{f})$ 中的任一元素 $\setminus S$。

还需证明另外两个事实。

首先，我们证明由行索引为 S 中元素、列索引为 $\mathbf{Mon}_{d,\,j-1}$ 中元素所定义的子矩阵，是矩阵 $\mathbf{Mac}(\mathbf{TP}_{d,\,j-1}(\boldsymbol{f}),\ \mathbf{Mon}_{d,\,j-1})$。如上所证，集合 S 和 $\mathbf{Mon}_{d,\,j-1}$ 分别是为 $\mathbf{Mac}(\mathbf{TP}_{d,\,j}(\boldsymbol{f}),\ \mathbf{Mon}_{d,\,j})$ 的前几行和前几列编索引的元素集合。设 $m\ \phi(f_i,\ j)$ 属于 S。由行 $m\ \phi(f_i,\ j)$ 以及列 $\mathbf{Mon}_{d,\,j-1}$ 中元素所定义的多项式为：

$$\begin{aligned}(m\times\phi(f_i,j))(x_1,\dots,x_{j-1},0)&=m\times((\phi(f_i,j))(x_1,\dots,x_{j-1},0))\qquad(\text{因为 } m \text{ 属于 } \mathcal{R}_{j-1})\\&=m\times\phi(f_i,j-1).\end{aligned}$$

因此，矩阵 $\mathbf{Mac}(\mathbf{TP}_{d,\,j-1}(\boldsymbol{f}),\ \mathbf{Mon}_{d,\,j-1})$ 是 Macaulay 矩阵 $\mathbf{Mac}(\mathbf{TP}_{d,\,j}(\boldsymbol{f}),\ \mathbf{Mon}_{d,\,j})$ 左上角的一个子矩阵。

最后，我们证明此子矩阵下方的所有行，在对应于由 $\mathbf{Mon}_{d,\,j-1}$ 索引的列的元素中均为零。设 $m\ \phi(f_i,\ j)$ 是其中一行。那么，单项式 m 属于集合 $\mathbf{Mon}_{d-\delta,\,j}\setminus\mathbf{Mon}_{d-\delta,\,j-1}$。这意味着 $m\ \phi(f_i,\ j)$ 的支撑集中的每个单项式都能被 x_j 整除。因此，其支撑集与 $\mathbf{Mon}_{d,\,j-1}$ 不相交，相应的元素为零。 □

现在，我们可以证明定理 4.1。

定理 *4.1* 的证明。 设 j属于 $\{1,\dots,n\}$，且 d属于 $\mathbb{N}$。根据 [31, 第 1.4 节，定理 5],，存在一个可逆方阵 $U_{d,\,j}$，使得

$$U_{d,j}\,\mathrm{Mac}(\mathsf{TP}_{d,j}(\boldsymbol{f}),\mathsf{Mon}_{d,j})=E_{d,j}$$

其中$E_{d,\,j}$ 为行最简阶梯形。利用引理4.4中所述矩阵的包含关系，我们考虑以下矩阵乘积：

$$\left(\begin{array}{c|c}U_{d,j-1} & *\\ \hline 0\cdots 0 & \\ \vdots\ \ \vdots & Id\\ 0\cdots 0 & \end{array}\right)\left(\begin{array}{c|c}\mathrm{Mac}(\mathsf{TP}_{d,j-1}(\boldsymbol{f}),\mathsf{Mon}_{d,j-1}) & \\ \hline 0\ \cdots\ 0 & \\ \vdots\ \ \vdots & *\\ 0\ \cdots\ 0 & \end{array}\right)$$

$$= \left(\begin{array}{ccc|c} & E_{d,j-1} & & \\ \hline 0 & \cdots & 0 & * \\ \vdots & & \vdots & \\ 0 & \cdots & 0 & \end{array}\right)$$

$$= \left(\begin{array}{ccc|c} & E & & * \\ \hline 0 & \cdots & 0 & \\ \hline 0 & \cdots & 0 & \\ \vdots & & \vdots & B \\ 0 & \cdots & 0 & \end{array}\right)$$

其中， E 是由E_d的非零行组成的矩阵，$j-1$。

因此 ， $\mathrm{Mac}(\mathrm{TP}_{d,j}(\boldsymbol{f}), \mathrm{Mon}_{d,j})$ 的行最简阶梯形 $E_{d,j}$ 可表示如下 s:

$$E_{d,j} = \left(\begin{array}{ccc|c} & E_{d,j-1} & & \\ \hline 0 & \cdots & 0 & * \\ \vdots & & \vdots & \\ 0 & \cdots & 0 & \end{array}\right). \qquad (*)$$

令 G_j 表示约化的 $\succ_{\mathrm{grevlex}}$-格罗布纳基 $G(I_j(\boldsymbol{f}) \succ_{\mathrm{grevlex}})$。现在，我们证明

$$G_j = \{\phi(g,j) \mid g \in \bigsqcup_{i=0}^{j} G_{*,i}(I, \succ_{\mathrm{grevlex}})\}.$$

($\supseteq$) 设 $f = \phi(g,j)$，其中 g属于$G = \bigsqcup_{i=0}^{j} G_{*,i}(I, \succ_{\mathrm{grevlex}})$。我们证明 f属于集合 G_j。考虑整数 D ，它是 I的约化的 $\succ_{\mathrm{grevlex}}$-格罗布纳基中元素的最大次数。由于 g 属于 I的约化的 $\succ_{\mathrm{grevlex}}$-格罗布纳基，根据引理 4.3，存在 e属于 $\{\delta, \ldots, D\}$，使得 g由 $E_{e,n}$ 的某一行表示。由于 g属于$\bigsqcup_{i=0}^{j} G_{*,i}(I)$，其首项单项式属于 $\mathcal{R}_j$，这意味着 f 不可能为零。利用 (∗)，我们推得 f 是 $E_{e,j}$ 的一个非零行。

根据引理4.3， f 属于 G_j 当且仅当不存在这样的多项式 h ： 它由E_d中的一行表示，j 且满足 $d < e$ ，使得 $\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(h)$ 整除 $\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(f)$。反设这样的 h存在。根据（$*$），存在一个多项式 η ，它由E_d中的一行表示，n 并且满足 $h = \phi(\eta, \ j)$。由于 $\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(\eta)$ 和 $\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(g)$ 位于 $\mathcal{R}_j$中，注意到

$$\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(\eta) = \mathrm{lm}_{\succ_{\mathrm{grevlex}}}(h) \quad \text{and that} \quad \mathrm{lm}_{\succ_{\mathrm{grevlex}}}(g) = \mathrm{lm}_{\succ_{\mathrm{grevlex}}}(f).$$

由于$\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(h)$ 整除$\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(f)$，我们可推出$\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(\eta)$ 整除$\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(g)$。由于 $d < e$，根据引理4.3 的第二个假设，这与以下事实相矛盾： g 属于 G。因此，这样的多项式h 不可能存在。由此可知， f 属于 G_j。

($\subseteq$) 令 f属于 G_j。我们证明，存在一个多项式 g属于$\bigsqcup_{i=0}^{j} G_{*,\ i}(I, \ \succ_{\mathrm{grevlex}})$，使得$f = \phi(g, \ j)$。

考虑整数 D_j ，它是 G_j中元素的最大次数。根据引理 4.3，存在 e 属于 $\{\delta, \ldots, D_j\}$，使得 f是 $E_{e,j}$的一行。根据 (∗)， f具有 $\phi(g,j)$ 的形式，其中 g是 $E_{e,n}$的一个非零行。根据注 4.2和 (∗)，我们有

$$\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(g) = \mathrm{lm}_{\succ_{\mathrm{grevlex}}}(\phi(g,j)) = \mathrm{lm}_{\succ_{\mathrm{grevlex}}}(f).$$

为了证明 g属于 G，我们证明不存在一个多项式 h，它由 $E_{d,\ n}$ 的一行表示，且满足 $d < e$ ，使得 $\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(h)$ 整除 $\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(g)$。

反设存在 d属于 $\{\delta, \ldots, e-1\}$，使得由 E_d 的一行表示的某个多项式 h 的首项单项式整除 $\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(g)$。由于 $\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(g)$ 属于 $\mathcal{R}_j$，单项式 $\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(h)$ 属于 $\mathcal{R}_j$。因此，多项式 $\phi(h,j)$ 是 E_d 的一个非零行，其 $\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(\phi(h,j))$ 整除 $\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(f)$。由于 $f \in G_j$，根据引理 4.3，这产生矛盾。因此，不存在这样的多项式 h。由引理 4.3 可知， g 属于 G。此外，由于 $\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(g)$ 属于 $\mathcal{R}_j$，多项式 g 属于$\bigsqcup_{i=0}^{j} G_{*,i}(I, \succ_{\mathrm{grevlex}})$。 □

下面的推论是定理 4.1的直接推论。

推论 **4.5.** 设 $\boldsymbol{f} = (f_1, \dots, f_s)$ 是 $\mathcal{R}_n$ 中次数为 δ 的齐次多项式序列。*Let* d 属于 $\mathbb{N}$ 并且 j 属于 $\{1, \dots, n\}$。令 $I = \langle \boldsymbol{f} \rangle$。那么我们有

$$\mathscr{B}_{d,j}(I, \succ_{\mathrm{grevlex}}) = \mathscr{B}_{d,j}(I_j(\boldsymbol{f}), \succ_{\mathrm{grevlex}}).$$

证明。 根据定义，我们有

$$\begin{aligned}
\mathscr{B}_{d,j}(I, \succ_{\mathrm{grevlex}}) &= \mathsf{Mon}_{d,j} \setminus \left(\mathsf{Mon}_{d,j} \cap \langle \bigsqcup_{i=0}^{j} \mathscr{M}_{*,i}(I, \succ_{\mathrm{grevlex}}) \rangle \right) \\
&= \mathsf{Mon}_{d,j} \setminus \left(\mathsf{Mon}_{d,j} \cap \langle \bigsqcup_{i=0}^{j} \mathscr{M}_{*,i}(I_j(\boldsymbol{f}), \succ_{\mathrm{grevlex}}) \rangle \right) && \text{(Using Theorem 4.1)} \\
&= \mathscr{B}_{d,j}(I_j(\boldsymbol{f}), \succ_{\mathrm{grevlex}}). && \text{(by definition)}
\end{aligned}$$

□

4.2. 泛型单项式阶梯的最后一个维度

本小节旨在证明定理 4.6。该定理是 [40, 推论 3.2], 的一个具体特例；该推论刻画了由一列 n 齐次多项式生成的理想的单项式阶梯的一般形态。我们以更精确的形式重述这一结果，因为原陈述比此处考虑的情形更为一般。此外，原定理有若干结论，并在 [40, 推论 3.2]中以两个不同版本呈现。一个关键区别在于，在我们的设定中，所有多项式的次数都相同。若不作此假设，则会出现更多微妙之处，详见 [40]。此外，我们专门考虑生成多项式的数量等于变量数量的情形。注意，本小节仅讨论齐次多项式。对于给定的整数对 (δ, n)，我们用 $\mathcal{D}_{\delta,n}$ 表示满足 [40, 推论 3.2]所述性质的齐次多项式序列 $(f_1, \dots, f_n)$ 的扎里斯基开集，其中多项式的次数为 δ，且属于 $\mathcal{R}_n$。集合 $\mathcal{D}_{\delta,n}$ 扎里斯基稠密这一事实依赖于 [40, 猜想 1.2 和 1.6]。我们先回顾一些概念。

与级数 $\sum_{d=0}^{+\infty} a_d$ 的 [42, 定义 2.1], 中一样，我们定义

$$\left[\sum_{d=0}^{+\infty} a_d \right]_+ = \sum_{d=0}^{+\infty} b_d,$$

其中

$$\begin{cases} b_d = a_d & \text{if } a_i > 0 \text{ for all } i \leq d, \\ b_d = 0 & \text{otherwise.} \end{cases}$$

令 $n \in \mathbb{N}$，并令 I 为由齐次多项式生成的 $\mathcal{R}_n$ 的一个理想。回顾一下，其希尔伯特级数定义为

$$\mathrm{HS}_I(z) = \sum_{d=0}^{+\infty} \beta_d z^d$$

其中 $\beta_d = \sharp(\mathscr{B}_{d,n}(I, \succ_{\mathrm{grevlex}}))$。严格来说，这是商环 $\mathcal{R}_n/I$ 的希尔伯特级数，但我们沿用上述记法，并宽泛地称之为“I 的希尔伯特级数”。

回顾一下，对于整数 d，我们用 $\mathcal{R}_n^{(d)}$ 表示由 $\mathcal{R}_n$ 中所有次数为 d 的齐次多项式生成的 $\mathbb{K}$-向量空间。令 n, δ 和 s 为三个整数；若 $\boldsymbol{f} = (f_1, \dots, f_s)$ 是 $\mathcal{R}_n^{(\delta)}$ 中的多项式序列，则称其为半正则序列，当且仅当

$$\mathrm{HS}_{\langle \boldsymbol{f} \rangle}(z) = \left[\frac{(1 - z^\delta)^s}{(1 - z)^n} \right]_+.$$

我们用 $\mathcal{S}_{\delta,n,s}$ 表示由 $\mathcal{R}_n^{(\delta)}$ 中的多项式构成的所有半正则序列 $(f_1, \dots, f_s)$ 的集合。若 $s \leq n$，则集合 $\mathcal{S}_{\delta,n,s}$ 是由 $\mathcal{R}_n^{(\delta)}$ [41, Proposition1] 中的多项式构成的所有正则序列 $(f_1, \dots, f_s)$ 的集合。在这种情况下，已知集合 $\mathcal{S}_{\delta,n,s}$ 是扎里斯基稠密的。反之，若 $s > n$，则 $\mathcal{S}_{\delta,n,s}$ 是扎里斯基稠密的这一陈述就是 [40, Conjecture 1.2], ，最初以 [20, Conjecture 1.1] 的形式提出。

定理 4.6（[40, Corollary 3.2] 的变体）。设 $\delta \geq 1$ 和 $n \geq 2$ 为整数。设 $\boldsymbol{f}$ 属于 $\mathcal{D}_{\delta,n}$，并令 $I = \langle \boldsymbol{f} \rangle$。假设 $\phi(\boldsymbol{f}, n-1)$ 属于 $\mathcal{S}_{\delta,n-1,n}$。我们定义 $\mathbb{D} = n(\delta-1)+1$ 和 $\mathbb{D}_{n-1} = \left\lfloor \frac{\mathbb{D}-1}{2} \right\rfloor + 1$。我们还将系数 β_d 定义为 $\left[\frac{1}{(1-z^\delta)^{n-1}}\right]_+ = \sum_{d=0}^{\mathbb{D}_{n-1}-1} \beta_d z^d$。那么对于 $\{\mathbb{D}_{n-1}+1, \ldots, \mathbb{D}\}$ 中的任意整数 d，有

1) $\mathscr{M}_{d,n}(I, \succ_{\mathrm{grevlex}}) = \{x_n^{2d-\mathbb{D}} m \mid m \in \mathscr{B}_{\mathbb{D}-d,n-1}(I, \succ_{\mathrm{grevlex}})\}$；
2) $\sharp(G_{d,n}(I, \succ_{\mathrm{grevlex}})) = \beta_{\mathbb{D}-d}$。

为说明我们对该定理的表述，我们将我们的记号与 [40, 推论 3.2]中的记号联系起来。齐次理想 I 是零维的，当且仅当 $\mathrm{HS}_I(z)$ 是关于 z的多项式。在这种情况下，I 的正则度等于 $\deg(\mathrm{HS}_I(z)) + 1$。整数 $\mathbb{D}_{n-1}$ 和 $\mathbb{D}$ 分别对应于 [40, 推论 3.2]中的 σ 和 δ。如上述推论所述，整数 $\mathbb{D}_{n-1}$ 表示由$\mathcal{S}_{\delta,n-1,n}$中的一个序列生成的理想的正则度。

此外，我们明确给出 μ 的定义，该定义在 [40, 第 2], 节中给出，其公式为

$$\mu = \mathbb{D} - 1 - 2(\mathbb{D}_{n-1} - 1) = \mathbb{D} - 2\left\lfloor \frac{\mathbb{D}-1}{2} \right\rfloor - 1.$$

这意味着，在我们的情形下，$\mu \in \{0, 1\}$。

[40, 推论 3.2] 的第二种表述指出，对于任意属于 $\{\mathbb{D}_{n-1}+1, \ldots, \mathbb{D}\}$ 的次数 d，$\mathscr{M}_{d,*}(I, \succ_{\mathrm{grevlex}})$ 中的元素的次数等于 x_n $2d - \mathbb{D}$，并且

$$\sharp\left(\mathscr{M}_{d,n}(I, \succ_{\mathrm{grevlex}})\right) = \beta_{\mathbb{D}-d}.$$

此外，对于这样的整数 d，我们有 $\mathscr{M}_{d,*}(I, \succ_{\mathrm{grevlex}}) = \mathscr{M}_{d,n}(I, \succ_{\mathrm{grevlex}})$，因为 $2d - \mathbb{D} \geq 2$。这证明了定理 4.6的第二个断言。现在转而证明第一个断言。

我们已经证明

$$\mathscr{M}_{d,n}(I, \succ_{\mathrm{grevlex}}) \subseteq \{x_n^{2d-\mathbb{D}} m \mid m \in \mathscr{B}_{\mathbb{D}-d,n-1}(I, \succ_{\mathrm{grevlex}})\}.$$

此外，我们知道 $\sharp(\mathscr{M}_{d,n}(I, \succ_{\mathrm{grevlex}})) = \beta_{\mathbb{D}-d}$。因此，剩下要证明的是

$$\sharp\left(\{x_n^{2d-\mathbb{D}} m \mid m \in \mathscr{B}_{\mathbb{D}-d,n-1}(I, \succ_{\mathrm{grevlex}})\}\right) = \beta_{\mathbb{D}-d}.$$

看起来，条件 $\boldsymbol{f} \in \mathcal{D}_{\delta,n}$ 已经意味着 $\phi(\boldsymbol{f}, n-1) \in \mathcal{S}_{\delta,n-1,n}$。尽管如此，我们仍使用推论 4.5给出进一步说明。

$$\begin{aligned}
\sharp\left(\{x_n^{2d-\mathbb{D}} m \mid m \in \mathscr{B}_{\mathbb{D}-d,n-1}(I, \succ_{\mathrm{grevlex}})\}\right) &= \sharp\left(\mathscr{B}_{\mathbb{D}-d,n-1}(I, \succ_{\mathrm{grevlex}})\right) \\
&= \sharp\left(\mathscr{B}_{\mathbb{D}-d,n-1}(I_{n-1}(\boldsymbol{f}), \succ_{\mathrm{grevlex}})\right) \quad \text{(using Corollary 4.5)} \\
&= \beta_{\mathbb{D}-d}. \qquad \text{(since } \phi(\boldsymbol{f}, n-1) \text{ lies in } \mathcal{S}_{\delta,n-1,n}\text{)}
\end{aligned}$$

由此可得

$$\mathscr{M}_{d,n}(I, \succ_{\mathrm{grevlex}}) = \{x_n^{2d-\mathbb{D}} m \mid m \in \mathscr{B}_{\mathbb{D}-d,n-1}(I, \succ_{\mathrm{grevlex}})\},$$

如所述。

5. 算法及其性质

在第 5.1 节中，我们对 F4 算法的一个变体作了整体描述。正如引言中所强调的，该变体将 Buchberger 判据与 Macaulay 矩阵的行阶梯形计算相结合，以计算格罗布纳基。请注意，这些矩阵可能不是满秩的。计算出它们的行阶梯形后，将对应于非零行的多项式加入当前基。在计算过程中得到的所有首项单项式构成了我们所说的与格罗布纳基计算相关联的格罗布纳轨迹。

第 5.2节首先介绍算法 F4B，它本质上是经过扩展的 F4 算法，其中增加了一些步骤，将部分数据存储在某个对象 $\mathcal{T}$中，我们称之为 轨迹。该轨迹特别提供了一些秩信息，使我们能够定位 F4 所处理矩阵中的满秩子矩阵。由此，我们得以推导出算法 F4T，随后可用于计算与该轨迹相容的多项式方程组的格罗布纳基。最后，第 5.4 节确立了这些算法的结构性质。

5.1. F4 算法的总体描述

我们先回顾 [12] 中 F4 算法的基本原理。设 (f,g) 是 $\mathcal{R}_n$ 中的两个非零多项式，并设 $t=\mathrm{lcm}(\mathsf{lm}_{\succ_{\mathrm{grevlex}}}(f),\mathsf{lm}_{\succ_{\mathrm{grevlex}}}(g))$。按照 [12, 定义 2.5],，我们定义与 (f,g) 相关联的对如下：

$$p_{f,g}=\left(t,\frac{t}{\mathsf{lm}_{\succ_{\mathrm{grevlex}}}(f)},f,\frac{t}{\mathsf{lm}_{\succ_{\mathrm{grevlex}}}(g)},g\right).$$

根据定义，对 $p_{f,\ g}$ 这一对的次数为 $\deg(t)$。此外，我们将相应的 S-多项式记为

$$\mathsf{sp}(f,g)=\frac{t}{\mathsf{lt}_{\succ_{\mathrm{grevlex}}}(f)}f-\frac{t}{\mathsf{lt}_{\succ_{\mathrm{grevlex}}}(g)}g.$$

算法的终止性基于以下命题。设 I 是由集合 $G=\{g_1,\ldots,g_r\}$ 生成的 $\mathcal{R}_n$ 理想。如 [8, 第6节第 2] 章的定理 6 所示， [6]， G 构成 I 的一个 $\succ_{\mathrm{grevlex}}$- 格罗布纳基，当且仅当对于每一对 $\{i,j\}$，用 G 除 $\mathsf{sp}(g_i,\ g_j)$ 所得的余式为零。这种除法也称为约化，除法中使用的 G 中的多项式称为约化子。这种除法是使用单项式序的欧几里得除法的多元版本。其描述见 [8, 第 2] 章第 3 节。然而，约化子集合的构造涉及一些选择。

从多项式序列 $\boldsymbol{f}$ 出发，F4 算法构造所有对的集合 P，并对这些对进行约化。在 Buchberger 算法中，这些约化是按顺序执行的，每次处理一对。相比之下，F4 算法会同时执行多次约化。为了确定在同一步骤中对哪些对进行约化，引入了一个选择函数 $\mathsf{Sel}(\cdot)$。给定一个对集 P，函数 $\mathsf{Sel}(P)$ 返回 P 的一个子集，当且仅当 $P=\emptyset$ 时，$\mathsf{Sel}(P)=\emptyset$。此外，我们选择一个按次数筛选对的特定选择函数：

$$\mathrm{Sel}(P)=\{p\in P\mid \deg(p)=\min_{\rho\in P}(\deg(\rho))\}.$$

然后，算法选取 $\mathsf{Sel}(P)$ 中的对，并将它们从 P 中移除。接着，算法使用结合高斯消元的 Macaulay 矩阵对这些对进行约化。得到的余式是多项式，可能为零：非零余式会被加入 $\boldsymbol{f}$，所有新生成的对则会被加入 P。当 P 为空时， $\boldsymbol{f}$ 是理想 I 的一个 $\succ_{\mathrm{grevlex}}$-格罗布纳基。

现在让我们考察 S-多项式是如何被约化的。考虑算法中某一步给定的集合 $P_1=\mathsf{Sel}(P)$。定义 S-多项式的集合：

$$S=\{\mathsf{sp}(f,g)\mid p_{f,g}\in P_1\}.$$

一个名为 SymbolicPreprocessing 的子程序构造了一个 R 约化子的集合，其中每个约化子都具有 mh 的形式，其中m 是一个单项式， h 属于当前基。该子程序最早在 [12, 第 2 节3], 中介绍，它会针对每个单项式 $\widetilde{m}\in\mathsf{Supp}(S)$ 检查 $\widetilde{m}$ 是否属于单项式理想 $\langle\mathsf{lm}_{\succ_{\mathrm{grevlex}}}(\boldsymbol{f})\rangle$。如果属于，则存在一个单项式 m 和一个多项式 $h\in\boldsymbol{f}$，使得 $\mathsf{lm}_{\succ_{\mathrm{grevlex}}}(mh)=\widetilde{m}$。于是，多项式 mh 被插入 R 中，作为一个约化子。此外，对于每个被添加到 R中的约化子 mh，子程序 SymbolicPreprocessing 会对其中 $\mathsf{Supp}(mh)$ 中的任意单项式执行与 $\widetilde{m}$ 相同的步骤。根据 [12, 定理 22], 这一过程保证会终止。可以注意到，约化子的选择具有灵活性。在我们的分析中，我们不偏向于任何特定的选择策略。

因此，在算法的这一阶段，我们有一个待约化多项式集合 S，以及一个约化子集合 R。约化步骤通过对与 S 和 R 中的多项式相关联的 Macaulay 矩阵进行高斯消元来完成。这里，我们考虑列以按反向字典序排列的单项式为索引的 Macaulay 矩阵。矩阵列的所有单项式索引集合都按反向字典序排列；因此，我们称它们为序列。我们不明确指定行排序，因为它不会影响我们的复杂度分析。

我们定义序列 $L=S\cup R$。回想一下，$\mathrm{Mac}(L,\mathrm{Supp}(L))$ 可能不是满秩的（而且通常确实如此）。S 中多项式的排序无关紧要。但请注意，可以对 R 中的多项式进行排序，使得 $\mathrm{Mac}(R,\mathrm{Supp}(L))$ 呈行阶梯形。这样的排序确实存在，因为SymbolicPreprocessing 不会两次处理同一个单项式。这一性质将在第 6 节所给出的复杂度分析中发挥关键作用。

在第5.3节中，我们将介绍算法约化，该算法以矩阵$\mathrm{Mac}(S,\mathrm{Supp}(L))$、矩阵$\mathrm{Mac}(R,\mathrm{Supp}(L))$（其为行阶梯形）以及单项式序列 $\mathbb{M}$作为输入，并返回一个行

阶梯形Mac(L,Supp(L))，允许对行进行置换。两个输入矩阵的列数必须等于 $\mathbb{M}$ 的基数，使得每一列都以$\mathbb{M}$中的某个单项式为索引。算法约化是一种特定算法，它以特定方式计算阶梯形，以获得我们的复杂度结果。该算法本身使用一个名为EchelonForm$(\cdot)$的基础线性代数子程序，该子程序以矩阵 $\mathscr{M}$ （其元素属于 $\mathbb{K}$ ）为输入，并返回 $\mathscr{M}$的行阶梯形。此外，由于Mac(R,Supp(L)) 已经是行阶梯形，因此第5.3 节的输出形式为

$$\begin{pmatrix} \mathrm{Mac}(R, \mathrm{Supp}(L)) \\ \mathscr{N} \end{pmatrix}.$$

考虑一个矩阵 $\mathscr{M}$，其系数取自 $\mathbb{K}$，以及一个单项式序列 $\mathbb{M}$，使得 $\mathscr{M}$的每一列都由一个单项式索引。我们定义Pol($\mathscr{M}, \mathbb{M}$) 为一个子程序，它以 $\mathscr{M}$和 $\mathbb{M}$ 为输入，并返回由 $\mathscr{M}$的各行表示的非零多项式集合。将运行算法约化后得到的矩阵记为 $\mathscr{E}$，集合Pol($\mathscr{E}$,)中那些首项单项式不能被当前基中某个多项式的首项单项式整除的多项式，将被加入当前基。

接下来，我们假设约化算法执行顶端约化，即计算得到的行阶梯形不一定是约化的。

此外，在约化的每一步之前，我们都会使用 [22, 第 3 节4] 中引入的判据（见第9行），以减少待约化的对的数量。构造出集合 $S = \mathrm{Sel}(P)$ 后，所有满足p_{g_i,g_j} 且(i, j) 属于 $\mathcal{B}(G)$ （定义见第3.2 节）的对都会从中移除。

现在我们可以描述 F4（算法 1），总体而言，它在每个步骤（记为 ι）中：

- 按上述方式选择对，
- 对由这些对关联的 S-多项式及例程 SymbolicPreprocessing 确定的约化子所定义的 Macaulay 矩阵进行行约化，得到阶梯形，
- 存储由阶梯化矩阵编码且具有新的首项单项式的新非零多项式，
- 相应地更新对集。

重复此过程，直到对集变为空集。

算法 1 F4($f_1, \ldots, f_s$)

输入： $\mathcal{R}_n$**中多项式的一个序列** $f = (f_1, \ldots, f_s)$**。输出：** $\langle f \rangle$ **的一个** $\succ_{\mathrm{grevlex}}$**-格罗布纳基。1：** $\iota = 0$**2：** $\mathscr{E} =$ **EchelonForm(Mac(**f**, Supp(**f**))) 3：** $G =$ **Pol(**$\mathscr{E}$**, Supp(**f**)) 4：** $P = \{p_{f,g} \mid f, g \in G$ **其中** $f \neq g\}$**5：当** $P \neq \emptyset$ **时执行 6：** $\iota = \iota + 1$**7：** $P_\iota =$ **Sel(**P**) 8：** $P = P \setminus P_\iota$**9：** $P_\iota = \{p_{g_i,g_j} \in P_\iota \mid (i, j) \notin \mathcal{B}(G)\}$**10：** $S_\iota = \{$**sp(**f, g**)** $\mid p_{f,g} \in P_\iota\}$**11：** $R_\iota =$ **SymbolicPreprocessing(**S_ι, G**) 12：** $\mathscr{S} =$ **Mac(**S_ι**, Supp(**$S_\iota \cup R_\iota$**)) 13：** $\mathscr{R} =$ **Mac(**R_ι**, Supp(**$S_\iota \cup R_\iota$**)) 14：** $\mathbb{M} =$ **Supp(**$S_\iota \cup R_\iota$**) 15：** $\begin{pmatrix} \mathscr{R} \\ \mathscr{N} \end{pmatrix} =$ **Reduction(**$\mathscr{S}, \mathscr{R}$**, $\mathbb{M}$) 16：对于 Pol(**$\mathscr{N}, \mathbb{M}$**) 中的** f**，执行 17：** $G = G \cup \{f\}$**18：** $P = P \cup \{p_{f,g} \mid g \in G\}$**19：返回** G

如上所述，在第 ι （第 17 行）新加入的多项式的首项单项式构成了我们所称的该格罗布纳基计算的轨迹。

5.2. 算法 F4B 和算法 F4T

算法 F4B 的目标是对 F4 算法稍作修改，以便构建一种称为格罗布纳轨迹的附加数据结构，该结构取决于输入多项式序列 $\boldsymbol{f} = (f_1, \ldots, f_s)$。这条轨迹使我们能够得到算法 F4T，它通过仅构建满秩麦考利矩阵，为与该轨迹相容的多项式序列计算格罗布纳基。该轨迹类似于 [44]，中引入的轨迹，在 [4, 5, 36] 中也有所提及或应用。

格罗布纳轨迹 $\mathcal{T} = (\Gamma, \Sigma, \Theta)$ 的定义如下：
(1) Γ 是由单项式集合组成的序列 Γ_ι。序列 Γ 旨在包含计算过程中新获得的所有首项单项式。(2) Σ 是由正整数组成的序列 Σ_ι。序列 Σ 记录计算过程中未约化为零的那些对。(3) Θ 是由单项式元组组成的序列 Θ_ι。Θ_ι 中的每个元素都具有 (m_1, m_2) 的形式。序列 Σ 记录计算过程中使用的约化子。

现在我们介绍算法 F4B 其目的是在执行 F4 算法期间构建这样的轨迹。

算法 2 F4B$(f_1, \ldots, f_s)$

输入：多项式序列 $\boldsymbol{f} = (f_1, \ldots, f_s)$，其中多项式属于 $\mathcal{R}_n$。输出：$\langle \boldsymbol{f} \rangle$ 的 $\succ_{\text{grevlex}}$-格罗布纳基以及格罗布纳轨迹 $\mathcal{T}$。1： $\iota = 0$ **和** $\mathcal{T} =$ **() 2：** $\mathscr{E} =$ **EchelonForm(Mac(**$\boldsymbol{f}$**, Supp(**$\boldsymbol{f}$**)))** **3：** $G =$ **Pol(**$\mathscr{E}$**, Supp(**$\boldsymbol{f}$**)) 4：** $\mathcal{T} =$ **Update**Γ**(**$\mathcal{T}$**, lm(**G**)) 5：** $P = \{p_{f,g} \mid f, g \in G$**，其中** $f \neq g\}$ **6：当** $P \neq \emptyset$ **时执行 7：** $\iota = \iota + 1$ **8：** $P_\iota =$ **Sel(**P**) 9：** $P = P \setminus P_\iota$ **10：** $P_\iota = \{p_{g_i,g_j} \in P_\iota \mid$ **(**i, j**)** $\notin \mathcal{B}$**(**G**)**$\}$ **11：** $S_\iota = \{$**sp(**f, g**)** $\mid p_{f,g} \in P_\iota\}$ **12：** $(R_\iota, \Theta_\iota) =$ **SymbolicPreprocessingTracer(**S_ι, G**) 13：** $\mathcal{T} =$ **Update**Θ**(**$\mathcal{T}$**,** Θ_ι**) 14：** $\mathscr{S} =$ **Mac(**S_ι**, Supp(**$S_\iota \cup R_\iota$**)) 15：** $\mathscr{R} =$ **Mac(**R_ι**, Supp(**$S_\iota \cup R_\iota$**)) 16：** $\mathbb{M} =$ **Supp(**$S_\iota \cup R_\iota$**) 17：** $\begin{pmatrix} \mathscr{R} \\ \mathscr{N} \end{pmatrix} =$ **Reduction(**$\mathscr{S}, \mathscr{R}, \mathbb{M}$**) 18：** $\mathcal{T} =$ **Update**Σ**(**$\mathcal{T}, \mathscr{N}$**) 19：** $\Gamma_\iota = \{\}$ **20：对于 Pol(**$\mathscr{N}, \mathbb{M}$**) 中的** f**，执行 21：** $\Gamma_\iota = \Gamma_\iota \cup \{$**lm(**$f$**)**$\}$**22：** $G = G \cup \{f\}$**23：** $P = P \cup \{p_{f,g} \mid g \in G\}$**24：** $\mathcal{T} =$ **Update**Γ**(**$\mathcal{T}$**,** Γ_ι**) 25：返回** G **和** $\mathcal{T}$

注意，矩阵 $\mathscr{S}$（第 14 行）和 $\mathscr{N}$（第 17 行）中的各行与第 P_ι 10 行的对集一一对应。此外，这一映射是隐式定义的。

格罗布纳迹构造基于三个子程序：

- 更新Γ，它以当前轨迹 $\mathcal{T} = (\Gamma, \Sigma, \Theta)$（其中有 $\Gamma = \Gamma_0, \ldots, \Gamma_\iota$）和一个单项式集合 $\Gamma_{\iota+1}$ 作为输入，并将 Γ 替换为 $\Gamma_0, \ldots, \Gamma_\iota, \Gamma_{\iota+1}$ 在 $\mathcal{T}$ 中。它用于第 4 行和第 24 行，将新加入当前基的多项式的首项单项式存储起来。

- 更新Σ，它以当前轨迹 $\mathcal{T} = (\Gamma, \Sigma, \Theta)$（其中有 $\Sigma = \Sigma_0, \ldots, \Sigma_\iota$）和一个行阶梯形矩阵 $\mathscr{N}$ 作为输入。它确定 $\Sigma_{\iota+1}$ 中用于标记非零多项式的指标集合 $\mathscr{N}$，并将 Σ 替换为 $(\Sigma_0, \ldots, \Sigma_\iota, \Sigma_{\iota+1})$ 在 $\mathcal{T}$ 中。此子程序用于第 18行。

- 更新Θ 该子程序以当前轨迹 $\mathcal{T} = (\Gamma, \Sigma, \Theta)$ (其中 $\Theta = \Theta_1, \ldots, \Theta_\iota$) 以及一个由单项式元组构成的集合 $\Theta_{\iota+1}$ 作为输入，并将 Θ 替换为 $\Theta_0, \ldots, \Theta_\iota, \Theta_{\iota+1}$，在 $\mathcal{T}$中。此过程用于第 13 行。

为了构造序列 Θ，我们引入子程序 SymbolicPreprocessingTracer，它是SymbolicPreprocessing 的一个变体，可返回额外信息。此过程用于第 12 行。它以两组多项式作为输入： S_ι (即 S-多项式）和 G（即当前的基元素）。它返回一个约化子的集合 R_ι 以及一个由单项式元组构成的集合 Θ_ι。输出 Θ_ι 按如下方式构造：

- 每个约化子 R_ι 的形式均为 $m_1 g$，其中 $g \in G$;
- 对于 R_ι中的每个约化子 $m_1 g$，我们将元组（m_1，lm(g)）添加到 Θ_ι中。因此，集合 Θ_ι 精确描述了 SymbolicPreprocessingTra 所作的约化子选择 cer.

注意，应用 UpdateΣ 可以确定 $\mathscr{S}$ 中哪些行（算法 14 第 F4B 行）不会被约化为 0。这些行来自算法 P_ι 第 10 行的 F4B 中的对集。因此，我们定义以下子程序：

- RemoveUselessPairs 接受一个对集 P、一个格罗布纳轨迹 $\mathcal{T} = (\Gamma, \Sigma, \Theta)$（其中$\Sigma = (\Sigma_0, \ldots, \Sigma_\iota)$）以及一个整数 ι 作为输入，并返回 P的子集，该子集对应于 Σ_ι。

此外，移除无用对之后，一些约化子也可能变得无用。应用 UpdateΘ 的目的是避免考虑这些在第 11 行引入的约化子。因此，我们定义以下子程序：

- ConstructReductors 接受一个格罗布纳轨迹 $\mathcal{T} = (\Gamma, \Sigma, \Theta)$、$\Gamma = (\Gamma_0, \ldots, \Gamma_\iota)$ 和$\Theta = (\Theta_1, \ldots, \Theta_\iota)$、一个整数 ι 以及一个多项式集合 G 作为输入。它返回一个多项式约化子集合 R。首先，它会考虑 Θ_ι 中的每个元素 (m_1, m_2)。由于我们处于顶端约化情形，它会验证 $m_1 m_2 \succ_{\text{反向字典序}} \min_{\succ_{\text{反向字典序}}}(\Gamma_\iota)$。若条件成立，则将元素 $m_1 g$ 添加到 R，其中 g 属于 G，且 $\text{lm}(g) = m_2$。

算法 3 F4T($f_1, \ldots, f_s, \mathcal{T}$)

输入： 一个由 $\boldsymbol{f} = (f_1, \ldots, f_s)$ 构成的多项式序列，元素属于 $\mathcal{R}_n$，以及一个格罗布纳轨迹 $\mathcal{T}$。输出： 若未失败，则返回一个多项式集合 G。

1: $\iota = 0$ **2:** $\mathscr{E} =$ **EchelonForm(Mac($\boldsymbol{f}$, Supp($\boldsymbol{f}$))) 3:** $G =$ **Pol($\mathscr{E}$, Supp($\boldsymbol{f}$)) 4:** $\iota_{\max} =$ **max** $\{\iota \in \mathbb{N} \mid \Sigma_\iota \neq \emptyset\}$ **5: 对于** $\iota = 1$ **到** $\iota = \iota_{\max}$，**执行 6: 如果** $\Sigma_\iota \neq \emptyset$，**则 7:** $P_\iota =$ **Sel(P) 8:** $P = P \setminus P_\iota$ **9:** $P_\iota = \{p_{g_i, g_j} \in P_\iota \mid (i, j) \notin \mathcal{B}(G)\}$ **10:** $P_\iota =$ **RemoveUselessPairs($\mathcal{T}$, P_ι, ι) 11:** $S_\iota = \{$**sp(f, g)** $\mid p_{f,g} \in P_\iota\}$ **12:** $R_\iota =$ **ConstructReductors($\mathcal{T}, G, \iota$) 13:** $\mathscr{S} =$ **Mac(S_ι,Supp($S_\iota \cup R_\iota$)) 14:** $\mathscr{R} =$ **Mac(R_ι, Supp($S_\iota \cup R_\iota$)) 15:** $\mathbb{M} =$ **Supp($S_\iota \cup R_\iota$) 16:** $\begin{pmatrix} \mathscr{R} \\ \mathscr{N} \end{pmatrix} =$ **约化($\mathscr{S}, \mathscr{R}, \mathbb{M}$) 17:** $\mathbb{L} = \{\}$ **18: 对于** f **属于 Pol($\mathscr{N}, \mathbb{M}$)，执行 19:** $\mathbb{L} = \mathbb{L} \cup \{$**lm($f$)**$\}$ **20:** $G = G \cup \{f\}$ **21: 如果** $\mathbb{L} \neq \mathcal{T}_\iota$，**则 22: 返回 False 23: 返回** G

现在我们可以介绍算法F4T ，它利用与某个多项式序列 $\boldsymbol{f}$相关联的格罗布纳轨迹，以计算与该轨迹相容的多项式系统的格罗布纳基，同时避免所有归约为零以及无用的约化子。

算法 F4T 的正确性显而易见，且已在 [4]中进行过说明。

5.3. 约化算法的详细内容考虑以下矩阵：

$$M = \begin{pmatrix} \mathscr{R} \\ \hline \mathscr{S} \end{pmatrix} = \begin{pmatrix} \mathrm{Mac}(R, \mathrm{Supp}(L)) \\ \hline \mathrm{Mac}(S, \mathrm{Supp}(L)) \end{pmatrix}.$$

算法约化在顶端约化情形中，是指计算矩阵的行阶梯形M。我们回顾一下，矩阵 $\mathscr{R}$ 已经处于行阶梯形。因此， $\mathscr{R}$ 将是该子程序输出的子矩阵。

对于矩阵 M、行索引集合 J_1 和列索引集合 J_2 ，我们将相应的子矩阵记为 $M_{J_1,\ J_2}$ 。我们还将所有列（分别为所有行）的指标属于 J_2 （分别属于 J_1）的子矩阵记为 $M_{*,\ J_2}$ （分别为 $M_{J_1,\ *}$）。设 $\mathscr{S}$ 和 $\mathscr{R}$ 是两个元素属于 $\mathbb{K}$ 且列数相同的矩阵。假设 $\mathscr{R}$ 处于没有零行的行阶梯形。那么，存在唯一的矩阵 $\mathscr{N}$ 和 $\mathscr{Q}$ ，使得

$$\mathscr{S} = \mathscr{Q}\mathscr{R} + \mathscr{N}$$

并且 $\mathscr{N}$ 中与 $\mathscr{R}$ 的主元位于相同列的元素为零。这个矩阵 $\mathscr{N}$ 称为关于 $\mathscr{S}$的规范形 相对于 $\mathscr{R}$ ，记作 *al*

$$\mathscr{N} = \mathrm{NF}(\mathscr{S}, \mathscr{R}).$$

记 J 为 $\mathscr{R}$ 中包含用于约化的主元的列的指标集合。假设 $\mathscr{R}$ 满行秩，则子矩阵 $\mathscr{R}_{*,\ J}$ 可逆。容易验证 $\mathscr{Q}$ 等于$\mathscr{S}_{*,\ J}(\mathscr{R}_{*,\ J})^{-1}$。我们在算法 标准形 约化中使用子程序 ，它以两个具有相同列数的矩阵 $\mathscr{S}$ 和 $\mathscr{R}$ 为输入，其中 $\mathscr{R}$ 为行阶梯形，并返回NF $(\mathscr{S},\ \mathscr{R})$。

现在我们介绍算法 约化 ，它用于计算这样的标准形 $\mathscr{N}$。首先介绍一些记号。考虑一个矩阵 M、一个 $\mathbb{M}$ 由单项式构成的集合，其基数等于 M的列数，以及一个 $\mathbb{M}_1$ 的子集 $\mathbb{M}$。集合 $\mathbb{M}$ 按照反向字典序排列，矩阵 M 的每一列都按降序以 $\mathbb{M}$ 中的一个元素作为指标。我们将$\Psi(M,\ \mathbb{M},\ \mathbb{M}_1)$ 记为 M的子矩阵，它由主元位于以 $\mathbb{M}_1$中元素为指标的列中的那些行组成。

现在的目标是使用行子矩阵进行约化，这些子矩阵的主元从 $\mathbb{M}$ 的某些子集中选取。我们引入以下记号来描述这些子集。设 i 是 $\{1, \ldots, n\}$ 中的一个整数，令 $d = \max_{m \in \mathbb{M}} \deg(m)$ 表示 $\mathbb{M}$ 中元素的最大次数。我们用 $\zeta(\mathbb{M}, i)$ 表示子集 $\mathbb{M} \cap (\mathrm{Mon}_{d,i} \setminus \mathrm{Mon}_{d,i-1})$。此外，我们用 $\zeta(\mathbb{M}, 0)$ 表示子集 $\mathbb{M} \cap \mathrm{Mon}_{\leq d-1}$。注意，$\mathbb{M} = \bigsqcup_{i=0}^{n} \zeta(\mathbb{M}, i)$，但 $\mathbb{M} = \{1\}$ 的情形除外；这种情形在我们的设定中不会出现。我们定义子程序「修改」，其输入为矩阵 M、一个由单项式组成且基数等于 M 的列数的集合 $\mathbb{M}$ 、 $\mathbb{M}$ 的一个子集 $\mathbb{M}_1$ ，以及一个与 $\Psi(M, \mathbb{M}, \mathbb{M}_1)$ 维数相同的矩阵 N 。该子程序返回矩阵 M，其中子矩阵 $\Psi(M, \mathbb{M}, \mathbb{M}_1)$ 已被替换为 N。

为了证明算法约化的正确性，我们建立如下结果。

引理 5.1. 设 $\mathscr{S}$ 和 $\mathscr{R}$ 是两个元素属于 $\mathbb{K}$ 且列数相同的矩阵。假设 $\mathscr{R}$ 是行阶梯形。考虑矩阵 $\mathscr{E}$ 为 $\mathscr{N} = \mathrm{NF}(\mathscr{S}, \mathscr{R})$的一个行阶梯形。

Then the matrix $\begin{pmatrix} \mathscr{R} \\ \hline \mathscr{E} \end{pmatrix}$ *is a row echelon form of* $\begin{pmatrix} \mathscr{R} \\ \hline \mathscr{S} \end{pmatrix}$ *up to a permutation of its rows.*

证明。 设 $J_{\mathscr{R}}$（分别为 $J_{\mathscr{E}}$）表示包含 $\mathscr{R}$（分别为 $\mathscr{E}$）主元的列的指标集合。我们证明，经过对其行进行置换后，矩阵 $\begin{pmatrix} \mathscr{R} \\ \hline \mathscr{E} \end{pmatrix}$ 是行阶梯形。首先，注意矩阵 $\mathscr{R}$ 和 $\mathscr{E}$ 是行阶梯形。因此，只需证明对于每个 $j \in J_{\mathscr{R}}$， $\mathscr{E}$ 的第 j 列不包含主元。

根据定义， $\mathscr{N}$的第 j 列是一列零。由于矩阵 $\mathscr{E}$ 的行是矩阵 $\mathscr{N}$ 各行的线性组合，因此 $\mathscr{E}$ 的第 j 列也为零列。由此可得，矩阵 $\begin{pmatrix} \mathscr{R} \\ \hline \mathscr{E} \end{pmatrix}$ 经过行置换后为行阶梯形。

算法 4约化

输入：两个矩阵 $\mathscr{S}$ 和 $\mathscr{R}$，其元素属于 $\mathbb{K}$，列数相同，且 R 为行阶梯形。一个由单项式构成的集合 $\mathbb{M}$，其基数等于 $\mathscr{S}$ 和 $\mathscr{R}$的列数。输出：将 S 和 R的各行合并后得到的矩阵的行阶梯形。1：$\mathscr{S}' = \mathscr{S}$2：对于 $i = 1$ 到 $i = n$，执行 3：$\mathbb{M}_i = \zeta(\mathbb{M}, i)$ 4：$N =$ 标准形$(\Psi(\mathscr{S}', \mathbb{M}, \mathbb{M}_i) \quad \Psi(\mathscr{R}, \mathbb{M}, \mathbb{M}_i))$ 5：$\mathscr{S}' =$ 修改$(\mathscr{S}', \mathbb{M}, \mathbb{M}_i, N)$ 6：$E =$ EchelonForm$(\Psi(\mathscr{S}', \mathbb{M}, \mathbb{M}_i))$ 7：$\mathscr{S}' =$ 修改$(\mathscr{S}', \mathbb{M}, \mathbb{M}_i, E)$ 8：$\mathbb{M}_0 = \zeta(\mathbb{M}, 0)$ 9：$N =$ 标准形$(\Psi(\mathscr{S}', \mathbb{M}, \mathbb{M}_0) \quad \Psi(\mathscr{R}, \mathbb{M}, \mathbb{M}_0))$ 10：$\mathscr{S}' =$修改$(\mathscr{S}', \mathbb{M}, \mathbb{M}_0, N)$ 11：$E =$ EchelonForm$(\Psi(\mathscr{S}', \mathbb{M}, \mathbb{M}_0))$ 12：$\mathscr{S}' =$修改$(\mathscr{S}', \mathbb{M}, \mathbb{M}_0, E)$ 13：返回 $\begin{pmatrix} \mathscr{R} \\ \mathscr{S}' \end{pmatrix}$.

由于两个矩阵 $\mathscr{S}$ 和 $\mathscr{E}$ 的行数相同，只需证明矩阵 $\begin{pmatrix} \mathscr{R} \\ \mathscr{E} \end{pmatrix}$ 和 $\begin{pmatrix} \mathscr{R} \\ \mathscr{S} \end{pmatrix}$ 的行生成相同的 $\mathbb{K}$-向量空间。由于矩阵 $\mathscr{N}$和 $\mathscr{E}$ 的行生成相同的 $\mathbb{K}$-向量空间，因此矩阵 $\begin{pmatrix} \mathscr{R} \\ \mathscr{N} \end{pmatrix}$ 和 $\begin{pmatrix} \mathscr{R} \\ \mathscr{E} \end{pmatrix}$ 的行生成相同的$\mathbb{K}$-向量空间。我们考虑变换矩阵 $\mathscr{Q}$，使得 $\mathscr{S} = \mathscr{Q}\mathscr{R} + \mathscr{N}$。于是可得如下表达式

$$\begin{pmatrix} \mathscr{R} \\ \mathscr{N} \end{pmatrix} = \left(\begin{array}{c|c} \mathscr{I} & 0 \\ -\mathscr{Q} & \mathscr{I} \end{array}\right)\begin{pmatrix} \mathscr{R} \\ \mathscr{S} \end{pmatrix}$$

其中 $\mathscr{I}$ 表示相应阶数的单位矩阵。由于该变换矩阵可逆，因此矩阵 $\begin{pmatrix} \mathscr{R} \\ \mathscr{S} \end{pmatrix}$ 和 $\begin{pmatrix} \mathscr{R} \\ \mathscr{N} \end{pmatrix}$ 的行生成相同的 $\mathbb{K}$-向量空间。证明完毕。 □

引理 5.2. 输入 $\mathscr{R}$ 和 $\mathscr{S}$，算法 约化 返回矩阵 $\begin{pmatrix} \mathscr{R} \\ \mathscr{E} \end{pmatrix}$，该矩阵是一行 *echelon form of* $\begin{pmatrix} \mathscr{R} \\ \mathscr{S} \end{pmatrix}$.

证明。 算法 n 的循环中有 约化 第 2 行的步骤。循环后的步骤对应第 9 行和第 11 行，包含与前面步骤相同的运算，但为了记号上的方便，将其放在循环之外。

记 $\Psi(\mathscr{S}, \mathbb{M}, \mathbb{M}_1)$ 为 $\mathscr{S}_1$，记 $\Psi(\mathscr{R}, \mathbb{M}, \mathbb{M}_1)$ 为 $\mathscr{R}_1$。我们先进行第一步，然后通过迭代得出结论。

考虑由 $\mathscr{S}$ 和 $\mathscr{R}$ 的行构成的输入矩阵。我们可以根据需要重新排列这些行，以便更清楚地观察算法 约化

$$\mathscr{M}_1 = \left(\begin{array}{ccc|c|c|c} \overbrace{0 & \cdots & 0}^{\mathbb{M}_1} & \overbrace{*}^{\mathbb{M}_2} & \cdots & \overbrace{*}^{\mathbb{M}_0} \\ \vdots & \ddots & \vdots & * & \cdots & * \\ 0 & \cdots & 0 & * & \cdots & * \\ \hline & * & & * & \cdots & * \\ \hline & * & & * & \cdots & * \end{array}\right) \begin{matrix} \\ \\ \\ \}\mathscr{R}_1 \\ \}\mathscr{S}_1 \end{matrix}.$$

在第 2 行循环的第一次迭代中，初始矩阵 $\mathscr{S}_1$ 被转换为矩阵$\mathscr{E}_1 =$ EchelonForm$(\mathrm{NF}(\mathscr{S}_1, \mathscr{R}_1))$。由于 $\mathscr{R}$已经是行阶梯形，因此 $\mathscr{R}_1$也具有相同性质。因此，可以应用引理 5.1 推导出矩阵 $\begin{pmatrix} \mathscr{R}_1 \\ \mathscr{E}_1 \end{pmatrix}$ 是该矩阵的行阶梯形

矩阵 $\begin{pmatrix} \mathscr{R}_1 \\ \mathscr{S}_1 \end{pmatrix}$。因此，在第 2 行循环的第一次迭代结束时，矩阵 $\mathscr{M}_1$ 变为$\widetilde{\ }$以下矩阵 $\mathscr{M}_1$ （至行置换）

$$\widetilde{\mathscr{M}_1} = \begin{array}{c} \overbrace{}^{\mathbb{M}_1} \overbrace{}^{\mathbb{M}_2} \overbrace{}^{\mathbb{M}_0} \\ \left(\begin{array}{ccc|c|c} 0 & \cdots & 0 & * & \cdots & * \\ \vdots & \ddots & \vdots & * & \cdots & * \\ 0 & \cdots & 0 & * & \cdots & * \\ \hline & * & & * & \cdots & * \\ \hline & * & & * & \cdots & * \end{array}\right) \begin{array}{l} \}\mathscr{R}_1 \\ \}\mathscr{E}_1 \end{array} \end{array}$$

其中，$\begin{pmatrix} \mathscr{R}_1 \\ \mathscr{E}_1 \end{pmatrix}$ 是 $\begin{pmatrix} \mathscr{R}_1 \\ \mathscr{S}_1 \end{pmatrix}$的行阶梯形。因此，$\mathscr{M}_1$ 和 $\widetilde{\mathscr{M}_1}$ 的各行生成相同的$\mathbb{K}$-向量空间。

$\mathscr{E}_1$中有两类行：主元位于由 $\mathbb{M}_1$中的元素索引的列中的行，以及其余的行。这两类行分别对应矩阵 $\mathscr{E}_{1,1}$ 和$\mathscr{E}_{1,2}$。$\widetilde{\ }$通过适当置换 $\mathscr{M}_1$的行，可得到以下矩阵：

$$\begin{array}{l} \mathscr{M}_2 \left\{ \right. \\ \\ \end{array} \begin{array}{c} \overbrace{}^{\mathbb{M}_1} \overbrace{}^{\mathbb{M}_2} \overbrace{}^{\mathbb{M}_0} \\ \left(\begin{array}{ccc|c|c} 0 & \cdots & 0 & * & \cdots & * \\ \vdots & \ddots & \vdots & * & \cdots & * \\ 0 & \cdots & 0 & * & \cdots & * \\ \hline & 0 & & * & \cdots & * \\ \hline & * & & * & \cdots & * \\ \hline & * & & * & \cdots & * \end{array}\right) \begin{array}{l} \}\mathscr{E}_{1,2} \\ \}\mathscr{R}_1 \\ \}\mathscr{E}_{1,1} \end{array} \end{array}$$

其中，$\begin{pmatrix} \mathscr{R}_1 \\ \mathscr{E}_1 \end{pmatrix}_{,1}$ 为行阶梯形，其主元位于由 $\mathbb{M}_1$中的元素索引的列中。第2 行循环的第二次迭代仅变换矩阵 $\mathscr{M}_2$，并考察由 $\mathbb{M}_2$索引的列。由于第2 行的每个步骤都处理一组列，且这些组的并集最终涵盖 $\mathscr{M}_1$的所有列，因此该算法返回 $\mathscr{M}_1$的行阶梯形。

□

注5.3. 令 d 表示集合 $\mathbb{M}$中元素的最高次数。假设矩阵 $\mathscr{R}$ 的所有主元都位于由次数为 d 的单项式所标记的列中。那么，算法 *Reduction* 的第 *9* 行和第 11 行不会执行。

下一个结论给出了计算此类标准形的复杂度界。其证明依赖于 [25, 引理 8.8]，并间接依赖于 [10, 引理 3.1]。回顾一下，ω 表示在 $\mathbb{K}$上进行矩阵乘法的常数。

命题 5.4. 设 M_1、M_2、C_1、C_2 为构成分块矩阵的矩阵

$$\left(\begin{array}{c|c} M_1 & M_2 \\ \hline C_1 & C_2 \end{array}\right),$$

其中 M_1 是 $\mathbb{K}^{a\times a}$中的可逆上三角矩阵，矩阵 M_2 属于 $\mathbb{K}^{a\times b}$，矩阵 C_1 属于 $\mathbb{K}^{c\times a}$，矩阵 C_2 属于 $\mathbb{K}^{c\times b}$。计算舒尔补

$$\mathrm{NF}\left(\begin{pmatrix} C_1 \mid C_2 \end{pmatrix}, \begin{pmatrix} M_1 \mid M_2 \end{pmatrix}\right) = \begin{pmatrix} 0 \mid C_2 - C_1 M_1^{-1} M_2 \end{pmatrix}$$

takes:

- $\mathcal{O}\left(a^2c^{\omega-2} + \frac{cab}{\min(c,b)^{3-\omega}}\right)$ *operations in* $\mathbb{K}$ *if* $c \le a$,
- $\mathcal{O}\left(ca^{\omega-1} + \frac{cab}{\min(a,b)^{3-\omega}}\right)$ *operations in* $\mathbb{K}$ *if* $a \le c$.

证明。计算这种标准形的算术复杂度与计算乘积 $C_1M_1^{-1}M_2$ 的算术复杂度相同。我们将该乘积分解为 $(C_1M_1^{-1})M_2$。计算 $(C_1M_1^{-1})$ 与 M_2 的乘积，其复杂度等于 $\mathcal{O}\left(\begin{smallmatrix} acb \\ a\ c \end{smallmatrix}\min(,,b)^{\omega}\right)$。此外，由于 M_1 是可逆上三角矩阵，可以应用 [25, 引理 8。8]，证明计算$C_1M_1^{-1}$的算术复杂度在 $c \le a$ 时为 $\mathcal{O}\left(a^2c^{\omega-2}\right)$，在 $a \le c$ 时为 $\mathcal{O}\left(ca^{\omega-1}\right)$。

□

5.4. 结构性质

此外，我们假设输入多项式的变量 n 数量和最大次数 δ 均大于或等于 2。我们用 G_0 表示 G 在算法 F4B 中第 6 行 while 循环之前的集合。

引理 5.5。设 $\boldsymbol{f} = (f_1, \ldots, f_s)$ 是环 $\mathcal{R}_n$ 中的非零多项式序列，满足 $(\mathrm{hom}(f_1), \ldots, \mathrm{hom}(f_s))$ 属于非空扎里斯基开集 $\mathcal{S}_{\delta,n,s}$（在第 4.2 节中引入），且 $s \leq n$。对于所有 $d \geq \delta$，令

$$W_d = \mathrm{Span}_{\mathbb{K}}(\{mf_i \mid i \in \{1, \ldots, s\}, m \in \mathsf{Mon}_{\leq d-\delta,n}\}).$$

那么，在算法 F4B中，对于所有多项式 g，在 G_0中，有 $\deg(g) = \delta$，并且满足以下等式：

$$W_d = \mathrm{Span}_{\mathbb{K}}(\{mg \mid g \in G_0, m \in \mathsf{Mon}_{\leq d-\delta,n}\})$$

对于所有 $d \geq \delta$。

证明。令 $\mathscr{M} = \mathsf{Mac}(\boldsymbol{f}, \mathrm{Supp}(\boldsymbol{f}))$ 表示与 $\boldsymbol{f}$ 相关且关于反向字典序的 Macaulay 矩阵，并考虑其行最简阶梯形 $\mathscr{E} = \mathrm{EchelonForm}(M)$。根据定义，我们有 $G_0 = \mathsf{Pol}(\mathscr{E}, \mathrm{Supp}(\boldsymbol{f}))$，因此有 $W_\delta = \mathrm{Span}_{\mathbb{K}}(G_0)$。

L且 $g \in G_0$。注意，根据构造，$g \neq 0$。于是，存在系数 $q_i \in \mathbb{K}$ 使得 t

$$g = \sum_{i=1}^{s} q_i f_i.$$

由于 g 是次数为 δ 的多项式的线性组合，因此 $\deg(g) \leq \delta$。反设 $\deg(g) < \delta$。由于 $(\mathrm{hom}(f_1), \ldots, \mathrm{hom}(f_s))$ 属于 $\mathcal{S}_{\delta,n,s}$，且 $s \leq n$ 和 $\deg(q_i) \leq 0$，我们可以应用命题 2.2。这表明存在多项式 $(h_i)_{i\in\{1,\ldots,s\}}$ 属于 $\mathcal{R}_n$，使得对所有 i，均有 $\deg(h_i) < 0$，

$$g = \sum_{i=1}^{s} h_i f_i.$$

显然，这迫使每个属于 $\{1, \ldots, s\}$ 的 i 都满足 $h_i = 0$，从而推出 $g = 0$。由于 g 非零，我们得到矛盾。因此，$\deg(g) = \delta$ 成立。

现在，设 $d \geq \delta$ 是一个整数，且 $m \in \mathsf{Mon}_{\leq d-\delta,n}$。我们可以写成

$$mg = m \sum_{i=1}^{s} q_i f_i,$$

因此 $mg \in W_d$。反向包含关系可用相同的推理得出。因此，我们得到

$$W_d = \mathrm{Span}_{\mathbb{K}}(\{mg \mid g \in G_0, m \in \mathsf{Mon}_{\leq d-\deg(g),n}\}). \qquad \square$$

对于任意整数 $\iota \geq 1$，令 G_ι 表示 while 循环第 6 行第 $(\iota+1)$ 次迭代开始时 G 的值，准确地说，就是执行 F4B 算法第 7 行时生效的值。由于 F4B 算法只会向 G 中添加元素，因此对于所有 $\iota \in \mathbb{N}$，都有 $G_\iota \subset G_{\iota+1}$。按照约定，我们令 $G_{-1} = \emptyset$。此外，对于任意整数 $\iota \geq 1$，令 $P(\iota)$ 表示 while 循环第 6 行第 ι 次迭代期间 P 的值，准确地说，就是执行第 7 行时生效的值。对于所有 $\iota \geq 1$，我们用 $d(\iota) = \min^{p\in P(\iota)}(\deg(p))$ 表示当前对的最小次数。我们令 $d(0) = \delta$，并令 $d(-1) = -1$。

引理 5.6. 设 $\boldsymbol{f} = (f_1, \ldots, f_s)$ 是环 $\mathcal{R}_n$ 中的一个多项式序列，使得其关联序列 $(\mathrm{hom}(f_1), \ldots, \mathrm{hom}(f_s))$ 属于 $\mathcal{S}_{\delta,n,s}$，其中 $s \leq n$。以下断言对所有 $\iota \geq 0$ 均成立。

1. $\mathcal{H}_1(\iota)$：$d(\iota) > d(\iota-1)$。（2）$\mathcal{H}_2(\iota)$：对于所有 $g \in G_\iota \backslash G_{\iota-1}$，$\deg(g) = d(\iota)$。（3）$\mathcal{H}_3(\iota)$：对于所有 $(g_1, g_2) \in G_\iota \times G_\iota$ with $g_1 \neq g_2$，$\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(g_1)$ 不整除 $\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(g_2)$。（4）$\mathcal{H}_4(\iota)$：对于所有属于 $P(\iota+1)$ 的 p，$\deg(p) > d(\iota)$。~（5）$\mathcal{H}_5(\iota)$：等式 $V_\iota = \widetilde{V}_\iota$ 成立，其中：

$$V_\iota = \mathrm{Span}_{\mathbb{K}}(\{mf_i \mid i \in \{1, \ldots, s\}, m \in \mathsf{Mon}_{\leq d(\iota)-\delta,n}\})$$

and

$$\widetilde{V}_\iota = \mathrm{Span}_{\mathbb{K}}(\{mg \mid g \in G_\iota, m \in \mathsf{Mon}_{\leq d(\iota)-\deg(g),n}\}).$$

证明。我们的证明是对 ι 使用归纳法。

我们开始证明 $\mathcal{H}_1(0)$、$\mathcal{H}_2(0)$、$\mathcal{H}_3(0)$、$\mathcal{H}_4(0)$ 和 $\mathcal{H}_5(0)$ 成立。首先，由于 δ 为正，我们有 $\mathcal{H}_1(0)$。根据定义，集合 $G_0 \setminus G_{-1}$ 等于 G_0。由于序列 $(\hom(f_1) \ldots, \hom(f_s))$ 属于 $\mathcal{S}_\delta$，n，s 且满足 $s \leq n$，因此可以应用引理 5.5。由此可知，对于所有属于 G_0 的 g，都有 $\deg(g) = \delta$。这证明了 $\mathcal{H}_2(0)$。

此外，我们知道存在一个元素取自 $\mathbb{K}$、处于行阶梯形的矩阵 $\mathscr{E}$，使得 $G_0 = \mathrm{Pol}(\mathscr{E}, \mathrm{Supp}(\boldsymbol{f}))$。由于由 $\mathscr{E}$ 的某一行表示的多项式的首项单项式由其主元所在的列决定，因此 G_0 中不可能有两个相同的首项单项式。此外，利用 $\mathcal{H}_1(0)$，对于所有属于 G_0 的 g，都有 $\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(g) = \delta$。因此，$\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(G_0)$ 中的所有元素都互不相同且次数相同。这就证明了 $\mathcal{H}_3(0)$。

考虑 $p \in P(1)$ 中的一个对，则有 $p = p_{g_1,g_2}$，其中 g_1 和 g_2 属于 G_0。我们将单项式 $t = \mathrm{lcm}\left(\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(g_1), \mathrm{lm}_{\succ_{\mathrm{grevlex}}}(g_2)\right)$ 记为 $t =$。我们知道 $\deg(p) = \deg(t)$。由于 $\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(g_1)$ 和 $\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(g_2)$ 不同，且次数为 δ，因此单项式 t 的次数大于 δ。由此得到$\mathcal{H}_4(0)$。

由于 $d(0) = \delta$，注意到 $\mathcal{H}_5(0)$ 是引理 5.5 $(d = \delta)$的一个特例。

现在我们继续进行归纳法。设 ι 为正整数，并假设对于所有 $\tilde{\iota} < \iota$，$\mathcal{H}_1(\tilde{\iota})$、$\mathcal{H}_2(\tilde{\iota})$、$\mathcal{H}_3(\tilde{\iota})$、$\mathcal{H}_4(\tilde{\iota})$ 和 $\mathcal{H}_5(\tilde{\iota})$ 均成立。我们证明 $\mathcal{H}_1(\iota)$、$\mathcal{H}_2(\iota)$、$\mathcal{H}_3(\iota)$、$\mathcal{H}_4(\iota)$ 和 $\mathcal{H}_5(\iota)$ 成立。

首先，我们回顾一下，$d(\iota) = \min_{p \in P(\iota)}(\deg(p))$。根据 $\mathcal{H}_4(\iota - 1)$，我们有 $d(\iota) > d(\iota - 1)$，这恰好就是 $\mathcal{H}_1(\iota)$。

现在，我们通过证明对于所有 g in $G_\iota \setminus G_{\iota-1}$，都有 $\deg(g) = d(\iota)$，来证明 $\mathcal{H}_2(\iota)$ 成立。设 g'be in $G_\iota \setminus G_{\iota-1}$。根据 $\mathrm{Sel}(P(\iota))$ 的定义，P_ι 中的所有对的次数均为 $d(\iota)$。由此可得 $\deg(g') \leq d(\iota)$。反设 $\deg(g') < d(\iota)$，则会导致矛盾。

首先，我们证明 g' 可以表示如下：$g' = \sum_{g \in G_{\iota-1}} u_g g$，其中 u_g 是一个多项式，且 $\deg(u_g) \leq d(\iota) - \deg(g)$。

由于 g' 属于 $G_\iota \setminus G_{\iota-1}$，因此可将其视为在第 14 行和第 15 行构造的矩阵 $\begin{pmatrix} \mathscr{R} \\ \mathscr{S} \end{pmatrix}$ 的阶梯形中的一行。

因此，多项式 g' 是由 $\mathbb{K}$ 对 $\mathscr{S}$ 和 $\mathscr{R}$ 的各行所表示的多项式构成的线性组合。$\mathscr{S}$ 的各行表示来自 P_ι 中的对所对应的 S-多项式。如前所述，这些对的次数为 $d(\iota)$，并且由 $G_{\iota-1}$ 中的两个多项式构造而成。由此可得，$\mathscr{S}$ 的各行所表示的多项式属于由 $\{mg \mid g \in G_{\iota-1}, m \in \mathrm{Mon}_{\leq d(\iota)-\deg(g)}\}$ 生成的 $\mathbb{K}$-向量空间。此外，根据 SymbolicPreprocessing 的定义，$\mathscr{R}$ 的各行具有如下形式：mg，其中 g 属于 $G_{\iota-1}$，且 m 属于 $\mathrm{Mon}_{\leq d(\iota)-\deg(g)}$。

我们推得，g' 可以表示如下：$g' = \sum_{g \in G_{\iota-1}} u_g g$ 其中，u_g 是一个满足 $\deg(u_g) \leq d(\iota) - \deg(g)$ 的多项式。

此外，可以将 g' 分解如下：

$$
\begin{aligned}
g' &= \sum_{g \in G_{\iota-1}} \left(\sum_{m \in \mathrm{Supp}(u_g)} \lambda_{m,g} mg \right) \\
&= \sum_{g \in G_{\iota-1}} \left(\sum_{\substack{m \in \mathrm{Supp}(u_g) \\ \deg(m) \leq d(\iota-1)-\deg(g)}} \lambda_{m,g} mg + \sum_{\substack{m \in \mathrm{Supp}(u_g) \\ \deg(m) > d(\iota-1)-\deg(g)}} \lambda_{m,g} mg \right).
\end{aligned}
$$

根据 $\mathcal{H}_1(\iota - 1)$，我们有 $d(\iota) > d(\iota - 1)$。因此，我们推得 $\deg(g) > d(\iota - 1) - \deg(g)$。由此，可以改写为

$$
g' = p_1 + \sum_{\substack{m \in \mathrm{Mon}_{\leq d(\iota)-d(\iota-1),n} \\ m \neq 1}} m p_m = \sum_{m \in \mathrm{Mon}_{\leq d(\iota)-d(\iota-1),n}} m p_m
$$

~其中，对于所有 $m \in \mathrm{Mon}_{\leq d(\iota)-d(\iota-1),n}$，$p_m$ 都属于 $V_{\iota-1}$。利用 $\mathcal{H}_5(\iota - 1)$，多项式 p_m（对于所有 $m \in \mathrm{Mon}_{\leq d(\iota)-d(\iota-1),n}$）都属于 $V_{\iota-1}$。我们推得，g' 可以写成：

$$
g' = \sum_{i=1}^{s} q_i f_i
$$

其中 $\deg(q_i) \leq d(\iota) - \delta$。

由于该序列 $(\mathsf{hom}(f_1)\ldots,\mathsf{hom}(f_s))$ 属于 $\mathcal{S}_{\delta,\ n,\ s}$ 并且 $\deg(g')\ <\ d(\iota)$ 根据假设，可以应用命题2.2将 g' 表示如下

$$g'=\sum_{i=1}^{s}h_if_i$$

且$\deg(h_i)\ <d(\iota)\ -\delta$。根据引理 5.5，多项式 g' 属于

$$\mathrm{Span}_{\mathbb{K}}(\{mg\mid g\in G_0,m\in\mathsf{Mon}_{<d(\iota)-\delta,n}\})\subset\mathrm{Span}_{\mathbb{K}}(\{mg\mid g\in G_{\iota-1},m\in\mathsf{Mon}_{<d(\iota)-\deg(g),n}\})$$

如 $G_0\subset G_{\iota-1}$。

根据这一隶属关系，可以将 g' 写成如下形式:

$$g'=\sum_{\substack{g\in G_{\iota-1}\\ m\in\mathsf{Mon}_{<d(\iota)-\deg(g),n}}}c_{m,g}mg\qquad(*)$$

其中 $c_{m,\ g}\in\mathbb{K}\setminus\{0\}$。由于 g' 属于 $G_\iota\setminus G_{\iota-1}$，因此 $\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(g')\notin\langle G_{\iota-1}\rangle$。我们使用 (*) 对和式排序，并将 g' 写成如下形式

$$g'=\sum_{\upsilon\in\Upsilon}\sum_{j=0}^{\ell_\upsilon}p_{\upsilon,j}$$

其中 $p_{\upsilon,\ j}$ 的形式为 $c_{m,\ g}mg$，且 $g\in G_{\iota-1}$、$m\in\in\mathsf{Mon}_{<d(\iota)-\deg(g),\ n}$，并且 $m\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(g)=\upsilon$。因此，单项式集合 Υ 是 $\mathsf{Mon}_{<d(\iota),\ n}$的子集。此外，我们有 $\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(p_{\upsilon,\ j})=\upsilon$。集合 Υ 的选取还满足：对于 Υ中的所有 υ，都有 $\{0,\ldots,\ell_\upsilon\}\neq\emptyset$。由于 g'不为零，考虑 Υ 中关于反向字典序的最大单项式 $\upsilon_1\in\Upsilon$。首先，利用 g' 的最后一个表达式以及 υ_1的定义，显然有 $\upsilon_1\succeq_{\mathrm{grevlex}}\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(g')$。如果 $\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(g')=\upsilon_1$，那么 $\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(g')$ 属于 $\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(G_{\iota-1})$，这是不可能的。因此，我们必须有 $\upsilon_1\succ_{\mathrm{grevlex}}\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(g')$。这意味着 $\upsilon_1\succ_{\mathrm{grevlex}}\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(\sum_{j=0}^{\ell_{\upsilon_1}}p_{\upsilon_1,\ j})$。利用 [8, 第 2 章、第6节、引理 5],，我们推得 $\sum_{j=0}^{\ell_{\upsilon_1}}p_{\upsilon_1,\ j}$是由 $(p_{\upsilon_1,\ j})_{0\le j\le\ell_{\upsilon_1}}$构成的 S-多项式的 $\mathbb{K}$-线性组合。此外，这些 S-多项式各自的首项单项式在反向字典序下都小于υ_1。考虑其中一个。设 j_1和 j_2属于 $\{0,\ldots,\ell_{\upsilon_1}\}$。记作$p_{\upsilon_1,\ j_1}=c_{m_1,\ g_1}m_1g_1$ 以及 $p_{\upsilon_1,\ j_2}=c_{m_2,\ g_2}m_2g_2$。那么，$\mathsf{sp}(p_{\upsilon_1,\ j_1},\ p_{\upsilon_1,\ j_2})$具有如下形式：$\lambda\mu\mathsf{sp}(g_1,\ g_2)$，其中$\lambda\in\mathbb{K}$、$\mu\in\in\mathsf{Mon}_n$，且 $\mu\mathrm{lcm}(\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(g_1),\ \mathrm{lm}_{\succ_{\mathrm{grevlex}}}(g_2))=\upsilon_1$。此外，我们有 $\deg(p_{g_1,\ g_2})<d(\iota)$。这样的对已在算法中约化。由此可得

$$\mathsf{sp}(g_1,g_2)=\sum_{\substack{g\in G_{\iota-1}\\ m\in\mathsf{Mon}_n}}b_{m,g}mg$$

其中，$\mathrm{lcm}(\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(g_1),\ \mathrm{lm}_{\succ_{\mathrm{grevlex}}}(g_2))\succ_{\mathrm{grevlex}}\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(mg)$，且 $b_{m,\ g}$ 属于 $\mathbb{K}$。由此可得，$\mathsf{sp}(p_{\upsilon_1,\ j_1},\ p_{\upsilon_1,\ j_2})$ 可以表示为元素 mg 的线性组合，其中 m 属于 Mon_n，g 属于$G_{\iota-1}$，且 $\upsilon_1\succ_{\mathrm{grevlex}}\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(mg)$。

现在，我们可以利用 $\sum_{j=0}^{\ell_{\upsilon_1}}p_{\upsilon_1,\ j}$的这一新表达式来改写 g'。由此得到

$$g'=\sum_{\upsilon\in\widetilde{\Upsilon}}\sum_{j=0}^{\ell_\upsilon}\tilde{p}_{\upsilon,j},$$

~其中，Υ 的最大单项式在反向字典序下小于 υ_1。由于小于 υ_1 的单项式集合是有限的，通过重复这一过程可得，g' 必为零。既然事实并非如此，这就构成了矛盾。因此，我们有 $\deg(g')=d(\iota)$。这证明了 $\mathcal{H}_2(\iota)$。

现在，我们证明 $\mathcal{H}_3(\iota)$ 成立。设 g_1 和 g_2 属于 G_ι。若 (g_1,g_2) 属于 $G_{\iota-1}^2$，则根据 $\mathcal{H}_3(\iota-1)$，我们可推得 $\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(g_1)$ 不整除 $\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(g_2)$。假设 (g_1,g_2) 属于 $(G_\iota\setminus G_{\iota-1})^2$。由于 g_1 和 g_2 由同一个处于行阶梯形的矩阵中的不同行表示，因此 $\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(g_1)\neq\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(g_2)$。根据 $\mathcal{H}_2(\iota)$，它们的次数相同，因此单项式 $\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(g_1)$ 不整除 $\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(g_2)$。最后，假设 g_2 属于 $G_\iota\setminus G_{\iota-1}$，且 g_1 属于$G_{\iota-1}$。根据 $\mathcal{H}_1(\tilde{\iota})$ 和 $\mathcal{H}_2(\tilde{\iota})$，对于所有属于 $\{0,\ldots,\iota\}$ 的 $\tilde{\iota}$，我们有 $\deg(g_2)\ >\deg(g_1)$。那么 $\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(g_2)$

不整除 $\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(g_1)$。反设 $\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(g_1)$ 整除 $\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(g_2)$。那么，函数 SymbolicPreprocessing 会为 R_ι 选取一个约化项 mg_1，使得等式 $m\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(g_1) = \mathrm{lm}_{\succ_{\mathrm{grevlex}}}(g_2)$ 成立。由于在第 17 行，g_2 由算法 F4B 通过 mg_1 约化，因此这就产生了矛盾。于是，$\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(g_1)$ 不整除 $\mathrm{lm}_{\succ_{\mathrm{grevlex}}}(g_2)$。这证明了 $\mathcal{H}_3(\iota)$。

为了证明 $\mathcal{H}_4(\iota)$，考虑 $P(\iota+1)$ 中的一对 $p = p_{g_1,g_2}$。我们来证明 $\deg(p) > d(\iota)$。分两种情况讨论：g_1 和 g_2 是否都属于 $G_{\iota-1}$。假设 g_1 和 g_2 属于 $G_{\iota-1}$。由于此类且次数为 $d(\iota)$的所有对都已在算法 F4B 的第 9 行被移除，因此 $\deg(p) > d(\iota)$。现在假设 g_1 属于 $G_\iota \setminus G_{\iota-1}$。利用 $\mathcal{H}_3(\iota)$，可得

$$\deg\left(\mathrm{lcm}\left(\mathsf{lm}_{\succ_{\mathrm{grevlex}}}(g_1), \mathsf{lm}_{\succ_{\mathrm{grevlex}}}(g_2)\right)\right) > \max\left(\deg(\mathsf{lm}_{\succ_{\mathrm{grevlex}}}(g_1)), \deg(\mathsf{lm}_{\succ_{\mathrm{grevlex}}}(g_2))\right).$$

由 $\mathcal{H}_2(\iota)$可知 $\deg(g_1) = d(\iota)$，因此 $\deg(p) > d(\iota)$。这就证明了 $\mathcal{H}_4(\iota)$。

最后，我们证明 $\mathcal{H}_5(\iota)$生成利用引理5.5，其我们知道 V_ι 和 $\widetilde{m \in \mathsf{Mon}_{\leq d(\iota)-\deg(g),n}}$。分两种情况讨论。假设 g 属于 $G_{\iota-1}$，则有 $\deg(g) \leq d(\iota-1)$。多项式 mg 可写为 $m_1 m_2 g$，其中 $\deg(m_1) \leq d(\iota) - d(\iota-1)$，且 $m_2 g$ 属于 $V_{\iota-1}$。利用 $\mathcal{H}_5(\iota-1)$，我们知道 $m_2 g$ 属于 $V_{\iota-1}$。因此，很容易推出 $m_1 m_2 g$属于 V_ι。现在假设 g 属于 $G_\iota \setminus G_{\iota-1}$。由 $\mathcal{H}_2(\iota)$可知 $\deg(g) = d(\iota)$，因此有 $m = 1$。我们知道 g 由来自次数为 $d(\iota)$的对的多项式以及 SymbolicPreprocessing 函数组成。因此，g 属于

$$\mathrm{Span}_{\mathbb{K}}(\{mg \mid g \in G_{\iota-1}, m \in \mathsf{Mon}_{\leq d(\iota)-\deg(g),n}\}).$$

根据前一种情形，多项式 g 属于 V_ι。由此得到 $\mathcal{H}_5(\iota)$，证明得证。 □

此外，我们研究长度为n、由次数为 δ 的 n元多项式组成的序列的格罗布纳基（关于反向字典序）的性质，这些序列属于第 3.2 节定义的非空扎里斯基开集 $\mathcal{A}_{\delta,n,n}$，以及第 4.2节定义的 $\mathcal{D}_{\delta,n}$。最后，回顾一下，给定一个多项式理想 I，$G_{d,*}(I, \succ_{\mathrm{grevlex}})$（$G_d$ 在无歧义时简称为.....）表示约化的$\succ_{\mathrm{grevlex}}$-格罗布纳基中次数为 d 的多项式集合。

引理 5.7。设 $\boldsymbol{f} = (f_1, \ldots, f_n)$ 是一个属于 $\mathcal{A}_{\delta,n,n} \cap \mathcal{D}_{\delta,n} \cap \mathcal{S}_{\delta,n,n}$ 的序列，其中 $\delta \geq 2$ 且 $n \geq 2$，并令其生成的理想为 $I = \langle \boldsymbol{f} \rangle$。令 $\mathbb{D} = n(\delta-1)+1$。那么，对每个属于 $\{\delta, \ldots, \mathbb{D}\}$的 d，集合 G_d非空。

证明。设 G 表示 $\succ_{\mathrm{grevlex}}$-格罗布纳基 I。由于 $\boldsymbol{f}$ 属于 $\mathcal{S}_{\delta,\,n,\,n}$，因此可以应用引理5.5并推 deduce 出 G_δ 非空。此外，序列 $\boldsymbol{f}$ 属于 $\mathcal{D}_{\delta,\,n}$。因此，可以应用定理 4.6 并推 deduce 出 $G_{\mathbb{D}}$ 非空。

为导出矛盾，假设对于某个 $d \in \{\delta+1, \ldots, \mathbb{D}-1\}$ 集合 G_d 为空。我们证明，这将意味着 $G_{\mathbb{D}}$ 也为空。根据引理 5.6，在算法 F4B中，G_{d+1} 的每个元素都源自一个对 $p_{g_i,\,g_j}$ 该对属于 $\mathscr{T}^\star(G)$，其中 g_i 和 g_j 属于$\bigsqcup_{k=\delta}^{d} G_k$（见第 10行）。

由于 $\boldsymbol{f}$ 属于 $\mathcal{S}_{\delta,\,n,\,n}$，根据 [41, 命题 1],，相应的希尔伯特级数等于 $\left(\sum_{i=0}^{\delta-1} z^i\right)^n$。这是一个多项式，这意味着理想 I 是零维的。此外，序列 $\boldsymbol{f}$ 属于 $\mathcal{A}_{\delta,\,n,\,n}$。随后可以应用定理 3.4，从而 deduce 出这样的对 $p_{g_i,\,g_j}$ 等于 $(t,\ t_i,\ g_i,\ t_j,\ g_j)$，其中 $(t_j,\ g_j)$ 是特殊的。因此，多项式 g_j 必须属于 G_d，而根据假设该集合为空。因此可得，G_{d+1} 也为空。

通过反复运用这一推理，我们得出 $G_{\mathbb{D}}$ 必为空集；但这与我们已经证明的 $G_{\mathbb{D}}$ 非空相矛盾。证明到此结束。 □

推论 5.8. 设 $\boldsymbol{f} = (f_1, \ldots, f_s)$ 为一个多项式序列。假设 $\mathsf{hom}(\boldsymbol{f})$ 是一个正则序列。那么有以下等式：

$$\mathsf{lm}_{\succ_{\mathrm{grevlex}}}(\langle \boldsymbol{f} \rangle) = \mathsf{lm}_{\succ_{\mathrm{grevlex}}}(\langle \mathsf{hom}(\boldsymbol{f}) \rangle).$$

证明。回顾一下，集合 $\mathsf{lm}_{\succ_{\mathrm{grevlex}}}(\langle \boldsymbol{f} \rangle)$(即 $\mathsf{lm}_{\succ_{\mathrm{grevlex}}}(\langle \mathsf{hom}(\boldsymbol{f}) \rangle)$)是由以下单项式构成的集合：$\widetilde{\ }$可被最小 grevlex 格罗布纳基的首项单项式整除，G (即 G) 的 $\langle \boldsymbol{f} \rangle$ (即 $\langle \mathsf{hom}(\boldsymbol{f}) \rangle$)。设 G 为通过算法 F4B计算得到的最小 grevlex 格罗布纳基。

由于 $\mathsf{hom}(\boldsymbol{f})$ 是一个正则序列，因此可以应用引理 5.6 并使用 $\mathcal{H}_1$ 和 $\mathcal{H}_2$ 来推导出在第 约化 17行不会发生次数下降。这意味着，在算法 F4B 中执行的所有顶层约化只涉及所考察多项式的最大次数齐次分量。因此，仅将计算截断到最大次数部分，就可以精确地计算出 $\langle \mathsf{hom}(\boldsymbol{f}) \rangle$的最小 grevlex 格罗布纳基。由此可知，在以 $\boldsymbol{f}$ 为输入执行算法 F4B 期间新找到的首项单项式仅取决于 $\mathsf{hom}(\boldsymbol{f})$。

□

6. 复杂度分析

6.1. 复杂度陈述

在本小节中，我们将在一般性假设下陈述算法 F4T 的复杂度结果。如第 1节所述，我们使用若干个扎里斯基开集，并将它们取交集以表述我们的假设。其中一些集合已知是非空的，而其他集合的非空性则依赖于猜想。

- 对于所有 $i \geq n$，集合 $\mathcal{S}_{\delta,\, i,\, n}$ 根据 [40, 定理 1.5]均非空。
- 如果 [40, 猜想 1.2 和 1.6]成立，则集合 $\mathcal{D}_{\delta,\, n}$ 非空。
- 如果 [40, 猜想 4.1] 成立，则集合 $\mathcal{A}_{\delta,\, n,\, n}$ 非空。
- 对于所有 $i < n$，如果 [20, 猜想 1.1] 成立，则集合 $\mathcal{S}_{\delta,\, i,\, n}$ 非空。我们回顾一下， [20 ，猜想 1 .1]和 [40 ，猜想 1 .2] 均表示同一个陈述 .

在以下结果中，我们使用同时诺特位置的概念，其定义见 [2,定义 3]。我们引入以下记号。对于正实数 p in $(0, 1]$, ，我们定义

$$E_p(\delta) = \ln\left(\frac{1 + p(\delta - 1)}{\delta}\right) + p(\delta - 1)\ln\left(\frac{1 + p(\delta - 1)}{p(\delta - 1)}\right).$$

对于整数 $\delta \geq 2$ ，我们定义 $L_\omega(\delta) = \frac{\delta}{1-e^{-\frac{1}{(\omega-2)}}} - \frac{1}{1-e^{-\frac{1}{\delta\,(\omega-2)}}}$ ，其中 ω 是关于 $\mathbb{K}$ 的矩阵乘法常数。

注意，若 $\omega = 2$，则 $L_\omega(\delta)$ 未定义。按照约定，对于任意 $\delta \geq 2$，我们令 $L_2(\delta) = 1$ 。此外，我们用 $\boldsymbol{\ell}(\omega)$ 表示常数 $L_\omega(2)$。最后，对于任意实数 ε，我们定义常数

$$\boldsymbol{c}(\varepsilon, \delta, \omega) = E_{1/2}(\delta) + E_{\boldsymbol{\ell}(\omega)+\varepsilon}(\delta).$$

~截断 ϕ 定义见第 4.1 节。回顾一下，我们使用经典记号 $\mathcal{O}$ 和 $\mathcal{O}$表示渐近界，其定义见 [21, 定义 25.7 和 25.8]。回顾一下，对于两个函数~f， $g\colon\ \mathbb{N} \to \mathbb{R}_{\geq 0}$，函数 $f(n)$ 属于 $\mathcal{O}(g(n))$，如果存在常数 N，c 使得

$$f(n) \leq g(n)\big(\log_2(3 + g(n))\big)^c$$

对于所有 $n \geq N$。

定理 *6.1*。 设 $\boldsymbol{f} = (f_1, \ldots, f_n)$ 是环 $\mathcal{R}_n$ 中的一个非零多项式序列，使得序列 $\mathit{hom}(\boldsymbol{f}) = (\mathit{hom}(f_1) \ldots, \mathit{hom}(f_n))$ 属于 $\mathcal{A}_{\delta,n,n} \cap \mathcal{D}_{\delta,n} \cap \mathcal{S}_{\delta,n,n}$，其中 $\delta \geq 2$ 且 $n \geq 2$。此外，假设 $\phi(\mathit{hom}(\boldsymbol{f})\ n-1)$ 属于 $\mathcal{S}_{\delta,n-1,n}$。我们假设变量 $x_1, \ldots, x_n$ 相对于 $\mathit{hom}(\boldsymbol{f})$ 处于同时诺特位置。令 $\mathcal{T}$ 为以 $\boldsymbol{f}$ 为输入、采用分次反字典序 $\succ_{\mathrm{grevlex}}$ 运行算法 *F4B* 时返回的格罗布纳轨迹。

对于固定的 $\delta \geq 2$，在输入序列 $\boldsymbol{g} = (g_1, \ldots, g_n)$ （其由与 $\mathcal{T}$相容的多项式方程组成）上运行算法 F4T，可计算出 $(\,, \succ_{\mathrm{grevlex}})$ 的极小 *Gröbner* 基，使用

$$\widetilde{\mathcal{O}}\left(\delta^{\omega n+1} e^{n\boldsymbol{c}(\varepsilon,\delta,\omega)}\right)$$

在 $\mathbb{K}$ 中进行算术运算，对所有 $\epsilon > 0$ 均成立。

~我们回顾一下，定理 $\mathcal{O}$ 1.1 中记号 1.1里的隐藏因子可由 n的一个多项式上界，该多项式的次数随 ω 线性增长，且不依赖于 δ 或 ε。定理 6.1 中一个值得注意的事实是，利用轨迹 $\mathcal{T}$，可以检验其若干假设是否成立。事实上，根据轨迹 $\mathcal{T}$可以确定计算过程中各对的次数是否递减。如果并非如此，那么

$$\mathsf{lm}_{\succ_{\mathrm{grevlex}}}(\boldsymbol{f}) = \mathsf{lm}_{\succ_{\mathrm{grevlex}}}(\mathsf{hom}(\boldsymbol{f})),$$

如推论 5.8 的证明所示。因此，集合 $\mathsf{lm}_{\succ_{\mathrm{grevlex}}}(\mathsf{hom}(\boldsymbol{f}))$ 决定了 $\langle \mathsf{hom}(\boldsymbol{f}) \rangle$ 的希尔伯特级数，由此可以判断 $\mathsf{hom}(\boldsymbol{f})$ 是否属于 $\mathcal{S}_{\delta,n,n}$。同样的推理表明，条件 $\phi(\mathsf{hom}(\boldsymbol{f})\ n-1)$ 属于 $\mathcal{S}_{\delta,n-1,n}$ 也可以根据 $\mathsf{lm}_{\succ_{\mathrm{grevlex}}}(\langle \boldsymbol{f} \rangle)$，利用推论 4.5 加以验证。最后，由于 $\mathsf{lm}_{\succ_{\mathrm{grevlex}}}(\langle \mathsf{hom}(\boldsymbol{f}) \rangle)$ 完整描述了 $\langle \mathsf{hom}(\boldsymbol{f}) \rangle$ 的单项式阶梯，因此也可用于验证 $\mathsf{hom}(\boldsymbol{f})$ 是否属于 $\mathcal{A}_{\delta,n,n}$ 和 $\mathcal{D}_{\delta,n}$。

为了证明定理 1.1 可由定理 6.1推出，我们需要证明同时诺特位置这一假设具有一般性。尽管这一事实被视为众所周知的结果，但我们并未

在文献中找到正式的表述。证明见引理 2。结合正则序列具有一般性这一事实，该引理得出了所需的结果。

定理6.1 可由下文定理6.2给出的一个更精确的公式推出。即使 δ 不是固定的，该公式仍然成立。此外，它所需的假设少于定理6.1，因为它不依赖同时诺特位置假设。

考虑一个 $\boldsymbol{f}$ 多项式序列，它们属于 $\mathcal{R}_n$，且次数均为 δ。回顾一下，集合 $\mathscr{M}_{*,*}(\langle \boldsymbol{f}\rangle, \succ_{\mathrm{grevlex}})$ 和 $\mathscr{B}_{*,*}(\langle \boldsymbol{f}\rangle, \succ_{\mathrm{grevlex}})$ 已在第3.1节中定义。对于所有 j 属于 $\{1,\dots,n\}$ 的情形，以及所有整数 d，定义

$$\gamma_{d,j} = \sharp\left(\mathscr{M}_{d,j}(\langle \boldsymbol{f}\rangle, \succ_{\mathrm{grevlex}})\right).$$

此外，对于所有整数 ι 以及所有属于 $\{1,\dots,n\}$ 的 i，定义

$$\rho_{\iota,i} = \binom{i-1+\iota+\delta}{\iota+\delta} - \binom{i-2+\iota+\delta}{\iota+\delta} - \left(\sharp\left(\mathscr{B}_{\iota+\delta,i}(\langle \boldsymbol{f}\rangle, \succ_{\mathrm{grevlex}})\right) - \sharp\left(\mathscr{B}_{\iota+\delta,i-1}(\langle \boldsymbol{f}\rangle, \succ_{\mathrm{grevlex}})\right)\right).$$

现在，定义

$$N^{(1)} = \sum_{d=\delta}^{\mathbb{D}_{n-1}+1} \sum_{i=1}^{n} \binom{n+d}{d} \left(\frac{\rho_{d-\delta,i} \sum_{j=i}^{n} \gamma_{d,j}}{\min\left(\rho_{d-\delta,i}, \sum_{j=i}^{n} \gamma_{d,j}\right)^{3-\omega}} + \left(\sum_{j=i}^{n} \gamma_{d,j}\right)^{\omega-1} \right),$$

$$N^{(2)} = \sum_{d=\mathbb{D}_{n-1}+2}^{\mathbb{D}} \gamma_{d,n}{}^{\omega-2} \binom{n+d}{d} \sum_{k=0}^{2} \binom{n-2+\mathbb{D}-d+k}{\mathbb{D}-d+k},$$

并令

$$N_{F4T} = N^{(1)} + N^{(2)}.$$

整数 $\mathbb{D} = n(\delta-1)+1$ 表示 Macaulay 界；对于由正则序列生成的零维理想，该界是该理想 [33, 的任意分次格罗布纳基中元素的最大次数定理 3]。此外，令

$$\mathbb{D}_{n-1} = \left\lfloor \frac{\mathbb{D}-1}{2} \right\rfloor + 1,$$

其对应于 由 $\mathcal{S}_{\delta,\ n-1,\ n}$ 中的序列生成的理想的正则度，如 in 第 4 节。 2.

定理 6.2。 设 $\boldsymbol{f} = (f_1,\dots,f_n)$ 是环 $\mathcal{R}_n$ 中的一个非零多项式序列，使得 $\boldsymbol{hom(f)} = (hom(f_1)\dots, hom(f_n))$ 属于 $\mathcal{A}_{\delta,n,n} \cap \mathcal{D}_{\delta,n} \cap \mathcal{S}_{\delta,n,n}$，其中 $\delta \geq 2$ 且 $n \geq 2$。此外，假设 $\phi(\boldsymbol{hom(f)})\ n-1)$ 属于 $\mathcal{S}_{\delta,\ n-1,n}$。设使用 $\boldsymbol{f}$ 作为输入运行算法 *F4B* 时返回的格罗布纳轨迹为 $\mathcal{T}$。那么，对与 $\mathcal{T}$ 相容的多项式方程序列 $\boldsymbol{g} = (g_1,\dots,g_n)$ 运行算法 *F4T*，将使用 $\mathcal{O}(N_{F4T})$ 次 $\mathbb{K}$ 中的算术运算，计算出 $(\boldsymbol{g}, \succ_{\mathrm{grevlex}})$ 的极小 *Gröbner* 基，其中 N_{F4T} 如上所定义。

6.2. 定理6.2的证明

此外，我们用 I （分别用 J）表示由 $\boldsymbol{f}$ （分别由同态($\boldsymbol{f}$)）生成的理想。由于根据假设，同态($\boldsymbol{f}$) 属于 $\mathcal{S}_{\delta,\ n,\ n}$，序列同态($\boldsymbol{f}$) 是正则的。因此，我们可以应用推论5.8 得到

$$\mathsf{lm}_{\succ_{\mathrm{grevlex}}}(I) = \mathsf{lm}_{\succ_{\mathrm{grevlex}}}(J). \qquad (\clubsuit)$$

因此， 集合 $\mathsf{lm}_{\succ_{\mathrm{grevlex}}}(I)$ 继承了 $\mathsf{lm}_{\succ_{\mathrm{grevlex}}}(J)$ 的所有已确立性质，因为 I 和 J 共享相同的首项 e 单项式 理想。

再次利用 $\mathsf{hom}(\boldsymbol{f})$ 位于 $\mathcal{S}_{\delta,\ n,\ n}$ 中这一事实，可以应用引理 5.6，并由对所有 $\iota \in \mathbb{N}$ 都成立的 $\mathcal{H}_1(\iota)$ 和 $\mathcal{H}_2(\iota)$ 推出， $G(J, \succ_{\mathrm{grevlex}})$ 中的所有多项式的次数都大于 δ。此外，由于 $\mathsf{hom}(\boldsymbol{f})$ 的希尔伯特级数等于 $\left(\sum_{i=0}^{\delta-1} z^i\right)^n$ 根据 [41, 命题 1], 我们 deduce， $G(J, \succ_{\mathrm{grevlex}})$ 中的所有多项式的次数都小于 Macaulay 界 $\mathbb{D} = n(\delta-1)+1$ [33,定理 3]。因此， $G(J, \succ_{\mathrm{grevlex}})$ 中所有多项式的次数都属于 $\{\delta,\dots,\mathbb{D}\}$。

根据假设，$\mathsf{hom}(\boldsymbol{f})$ 属于 $\mathcal{A}_{\delta,\ n,\ n} \cap \mathcal{D}_{\delta,\ n} \cap \mathcal{S}_{\delta,\ n,\ n}$。因此，可以使用引理 5.7 并推得：$G_{d,\ *}(J,\ \succ_{\mathrm{grevlex}})$ 非空，当且仅当 d 属于 $\{\delta,\dots,\mathbb{D}\}$。结合 ($\clubsuit$ 可知 $G_{d,\ *}(I,\ \succ_{\mathrm{grevlex}})$ 非空，当且仅当 d 属于 $\{\delta,\dots,\mathbb{D}\}$。

利用引理 5.6，`while` 循环在第 6 行的算法 F4B 中的每次迭代都对应一个唯一的次数，因为次数不会递减。这意味着，while循环在第 6 行的算法 F4B中恰好有 $\mathbb{D}-\delta$ 次迭代。此外，使用引理 5.6中的记号，我们有

$$d(\iota) = \iota + \delta \quad \text{for all } \iota \in \{0, \ldots, \mathbb{D}-\delta\}.$$

考虑一个序列 $\mathbf{h}$，它与 $\mathcal{T}$ 相容，并生成理想 $\langle \mathbf{h} \rangle$。注意，根据 (♣) 对于所有整数 $j \in \{1, \ldots, n\}$ 和所有次数 d，都有

$$\mathscr{M}_{d,j}(J, \succ_{\text{grevlex}}) = \mathscr{M}_{d,j}(I, \succ_{\text{grevlex}}) = \mathscr{M}_{d,j}(\langle \mathbf{h} \rangle, \succ_{\text{grevlex}}). \tag{♢}$$

我们给出算法 F4T 在 $\mathbb{K}$ 上执行的算术运算次数上界，其中算法 F4T 以 $\mathbf{h}$作为输入。由于 $\mathbf{h}$ 与 $\mathcal{T}$相容，因此它继承了 $G(I, \succ_{\text{grevlex}})$此前确立的所有性质。特别地，根据 (♢)，算法 F4T 中的整数 $\iota_{\max}$ 等于 F4T 。 $\mathbb{D}-\delta$

我们用 $\mathsf{T}(\iota)$ 表示算法 F4T 在第 5 行由 ι 索引的 for循环迭代期间于 $\mathbb{K}$ 中执行的算术运算次数，其中 $\iota \in \{1, \ldots, \mathbb{D}-\delta\}$。回顾一下，由于根据引理 5.6， $d(\iota) = \iota + \delta$，此迭代期间选出的对的次数为 $\iota + \delta$，且恰好是用于计算 $\langle \mathbf{h} \rangle$ 的 grevlex 最小格罗布纳基元素的那些对，其中其首项单项式属于 $\mathscr{M}_{\iota+\delta,*}(\langle \mathbf{h} \rangle, \succ_{\text{grevlex}})$。整数 $\mathsf{T}(0)$ 表示算法 F4T 在第 5 行的 for循环之前于 $\mathbb{K}$ 中执行的算术运算次数。

最后，我们用 γ_d （分别用 $\gamma_{d,\,j}$）表示 $\mathscr{M}_{d,\,*}(I,\ \succ_{\text{grevlex}})$ （分别表示 $\mathscr{M}_{d,\,j}(I,\ \succ_{\text{grevlex}})$ ）的基数。此外，利用 (♢)，我们有 γ_d （分别有 $\gamma_{d,\,j}$）等于 $\mathscr{M}_{d,\,*}(\langle \mathbf{h} \rangle,\ \succ_{\text{grevlex}})$ （分别等于 $\mathscr{M}_{d,\,j}(\langle \mathbf{h} \rangle,\ \succ_{\text{grevlex}})$ ）的基数。

由于根据假设，$\mathsf{hom}(\boldsymbol{f})$ 属于 $\mathcal{S}_{\delta,\,n,\,n}$，这些多项式中没有一个是其他多项式的 $\mathbb{K}$-线性组合。这意味着，与 $\boldsymbol{f}$ 相关联的 Macaulay 矩阵的行阶梯形，其主元均位于由次数为 δ的单项式所标记的列中，且恰有 n 个这样的主元。因此，我们推得，算法 2 F4T 第 2 行所考察的 Macaulay 矩阵满秩。因此，利用 [43, 第 2], 章，我们有 $\gamma_\delta = n$，这意味着

$$\mathsf{T}(0) \in \mathcal{O}\left(\gamma_\delta^{\omega-1}\binom{\delta+n}{\delta}\right) \in \mathcal{O}\left(n^{\omega-1}\binom{\delta+n}{\delta}\right).$$

令 $\iota \in \{1, \ldots, \mathbb{D}-\delta\}$。现在我们对 $\mathsf{T}(\iota)$作上界估计。需要考虑两个步骤：第一个步骤见算法 11 行，第二个步骤见算法 16 行 F4T。这两个步骤在 $\mathbb{K}$ 上所需的算术运算次数分别记为 $\mathsf{T}(\iota)^{\text{pairs}}$ 和 $\mathsf{T}(\iota)^{\text{red}}$。

我们首先估计 $\mathsf{T}(\iota)^{\text{pairs}}$。由于 $\mathcal{T}$是 $\boldsymbol{f}$ 的一个格罗布纳轨迹，且 $\mathbf{h}$ 与 $\mathcal{T}$相容，因此第 11 行中要构造的 S-多项式数量等于 $\gamma_{\delta+\iota}$。构造这些 S-多项式所涉及的多项式次数为 $\delta+\iota$。因此，该步骤至多需要进行 $\gamma_{\delta+\iota}$ 次加法运算，每次将两个次数不超过 $\delta+\iota$ 的多项式相加。于是，$\mathsf{T}(\iota)^{\text{pairs}}$ 的上界如下：

$$\mathsf{T}(\iota)^{\text{pairs}} \leq \gamma_{\delta+\iota}\binom{n+\delta+\iota}{\delta+\iota}.$$

现在我们推导整数 $\mathsf{T}(\iota)^{\text{red}}$ 的一个上界。我们记

$$\mathscr{S} = \text{Mac}(S_\iota, \text{Supp}(S_\iota \cup R_\iota)) \quad \text{and} \quad \mathscr{R} = \text{Mac}(R_\iota, \text{Supp}(S_\iota \cup R_\iota))$$

约化步骤中涉及的两个矩阵。对于 $i \in \{1, \ldots, n\}$，我们用 $\mathsf{T}(\iota, i, 1)$（分别用 $\mathsf{T}(\iota, i, 2)$）表示 Algorithm Reduction 在索引为 i 的 for循环迭代期间，于第4行（分别于第 6 行）执行的 $\mathbb{K}$ 中的算术运算次数。由于我们处于顶端约简情形，且 S-多项式的次数与新计算出的多项式的次数相同， $\mathscr{R}$ 的主元位于由最高次数单项式索引的列中。根据注5.3，Algorithm Reduction 的第 9 行和第 11 行不会执行。因此

$$\mathsf{T}(\iota)^{\text{red}} = \sum_{i=1}^{n} \left(\mathsf{T}(\iota, i, 1) + \mathsf{T}(\iota, i, 2)\right).$$

令 $i \in \{1, \ldots, n\}$。我们首先估算 $\mathsf{T}(\iota,\ i,\ 2)$。令 $\mathbb{M}$ 为索引 $\mathscr{S}$ 各列的单项式序列，并令 $\mathscr{R}$。与第 5.3 节一样，我们用 $\mathbb{M}_i$ 表示 $\mathbb{M}$ 中属于 $\mathsf{Mon}_i \setminus \mathsf{Mon}_{i-1}$且次数最大的单项式子集。

在算法 约化的此阶段，矩阵 $\Psi(\mathscr{S}',\ \mathbb{M},\ \mathbb{M}_i)$ 至多有 $\binom{n+\iota+\delta}{\iota+\delta}$ 列。由于算法 约化的先前步骤已识别出 $\mathcal{R}_{i-1}$ 中所有次数为 $\iota+\delta$ 的首项单项式，因此矩阵 $\Psi(\mathscr{S}',\ \mathbb{M},\ \mathbb{M}_i)$ 的行数上界为

$$\sum_{j=i}^{n}\gamma_{\iota+\delta,j}.$$

我们可以在 $\Psi(\mathscr{S}',\mathbb{M},\mathbb{M}_i)$ 的每一行与次数为$\iota+\delta$的单项式子集之间建立双射，因此列数大于行数。根据 [43, 第 2], 章可知，$\mathsf{T}(\iota,i,2)$ 属于

$$\mathcal{O}\left(\left(\sum_{j=i}^{n}\gamma_{\iota+\delta,j}\right)^{\omega-1}\binom{n+\iota+\delta}{\iota+\delta}\right).$$

现在我们来估计 $\mathsf{T}(\iota,i,1)$。在算法 约化的这一阶段，矩阵 $\Psi(\mathscr{S}',\mathbb{M},\mathbb{M}_i)$ 有$\binom{n+\iota+\delta}{\iota+\delta}$ 列，至多有 $\sum_{j=i}^{n}\gamma_{\iota+\delta,j}$ 行。同样，矩阵 $\Psi(\mathscr{R},\mathbb{M},\mathbb{M}_i)$ 至多有 $\binom{n+\iota+\delta}{\iota+\delta}$ 列。现在我们来界定 $\Psi(\mathscr{R},\mathbb{M},\mathbb{M}_i)$ 的行数。根据定义，它不超过 $\mathbb{M}_i$ 的基数，而后者又不超过 $\mathsf{Mon}_{\delta+\iota,i}\setminus\mathsf{Mon}_{\delta+\iota,i-1}$ 的基数，即

$$\binom{i-1+\iota+\delta}{\iota+\delta}-\binom{i-2+\iota+\delta}{\iota+\delta}.$$

然而，$\Psi(\mathscr{R},\mathbb{M},\mathbb{M}_i)$ 的每一行都表示 $\langle\mathbf{h}\rangle$ 中的一个多项式，因此其首项单项式必属于 $\mathsf{lm}_{\succ_{\mathrm{grevlex}}}(\langle\mathbf{h}\rangle)$，由 (♢) 可知。因此，$\Psi(\mathscr{R},\mathbb{M},\mathbb{M}_i)$ 的行数不超过 $\rho_{\iota,i}$，其中

$$\rho_{\iota,i}=\binom{i-1+\iota+\delta}{\iota+\delta}-\binom{i-2+\iota+\delta}{\iota+\delta}-\left(\beta_{\iota,i}-\beta_{\iota,i-1}\right),$$

with

$$\beta_{\iota,i}=\sharp\left(\mathscr{B}_{\iota+\delta,i}(\langle\mathbf{h}\rangle,\succ_{\mathrm{grevlex}})\right).$$

我们应用命题 5.4，其中 a 等于 $\Psi(\mathscr{R},\mathbb{M},\mathbb{M}_i)$ 的行数，c 等于 $\Psi(\mathscr{S}',\mathbb{M},\mathbb{M}_i)$ 的行数，而 b 等于这两个矩阵的列数减去 a。由于 b 不超过 $\binom{n+\iota+\delta}{\iota+\delta}$，且 $\binom{n+\iota+\delta}{\iota+\delta}$ 大于 a 和 c，我们得到 $\mathsf{T}(\iota,i,1)$ 属于

$$\mathcal{O}\left(\frac{\binom{n+\iota+\delta}{\iota+\delta}\rho_{\iota,i}\sum_{j=i}^{n}\gamma_{\iota+\delta,j}}{\min\left(\rho_{\iota,i},\sum_{j=i}^{n}\gamma_{\iota+\delta,j}\right)^{3-\omega}}\right).$$

从现在起，$\mathsf{T}(\iota)^{\mathrm{pairs}}$ 的上界由 $\sum_{i=1}^{n}\mathsf{T}(\iota,i,2)$ 的上界支配。因此，我们有 $\mathsf{T}(\iota)\in\mathcal{O}(N_\iota)$，其中

$$N_\iota=\sum_{i=1}^{n}\left(\frac{\binom{n+\iota+\delta}{\iota+\delta}\rho_{\iota,i}\sum_{j=i}^{n}\gamma_{\iota+\delta,j}}{\min\left(\rho_{\iota,i},\sum_{j=i}^{n}\gamma_{\iota+\delta,j}\right)^{3-\omega}}+\left(\sum_{j=i}^{n}\gamma_{\iota+\delta,j}\right)^{\omega-1}\binom{n+\iota+\delta}{\iota+\delta}\right).\qquad(♠)$$

回顾 $d(\iota)=\iota+\delta$ 根据引理5.6，这就证明了对所有 $\iota\in\{0,\ldots,\mathbb{D}_{n-1}-\delta+1\}$的结果。现在，我们定义

$$N^{(1)}=\sum_{\iota=0}^{\mathbb{D}_{n-1}-\delta+1}N_\iota.$$

还需证明 $\iota in\{\mathbb{D}_{n-1}+2-\delta,\ldots,\mathbb{D}\}$ 的结果

我们刚刚得出了 $\mathsf{T}(\iota)$ 的一个上界。现在，我们将针对 $\iota \geq \mathbb{D}_{n-1}+2-\delta$ 进一步细化这个上界。为此，我们首先确立四个关键性质。

由于根据假设，序列 $\phi(\mathsf{hom}(\boldsymbol{f})\ n-1)$ 属于 $\mathcal{S}_{\delta,n-1,n}$，理想 $\langle\phi(\mathsf{hom}(\boldsymbol{f})\ n-1)\rangle$ 的正则度等于 $\mathbb{D}_{n-1}$，如第 4.2 节所示。此外，由于 $\langle\phi(\mathsf{hom}(\boldsymbol{f})\ n-1)\rangle$ 的希尔伯特级数根据 [41, 命题 1], 是一个多项式，因此该理想是零维的。因此，$\langle\phi(\mathsf{hom}(\boldsymbol{f})\ n-1)\rangle$ 的 grevlex 最小格罗布纳基中的任意元素，其次数至多为 $\mathbb{D}_{n-1}$。

根据定理 4.1，我们知道，$\langle\mathsf{hom}(\boldsymbol{f})\rangle$ 的 grevlex 最小格罗布纳基中，首项单项式次数大于或等于 $\mathbb{D}_{n-1}+1$ 的任意元素都属于 $\mathsf{Mon}_n \setminus \mathsf{Mon}_{n-1}$。结合(♢)，我们推得，对于所有 $\iota \geq \mathbb{D}_{n-1}+1-\delta$ 以及所有 $i \in \{1,\ldots,n-1\}$，

$$\gamma_{\iota+\delta,i} = 0. \tag{♡, 1}$$

根据假设，序列 同次$(\boldsymbol{f})$ 属于 $\mathcal{D}_{\delta,\ n}$。因此，利用定理 4.6 将其应用于 同次$(\boldsymbol{f})$ 并结合 (♢)，我们得到，对所有 $\iota \geq \mathbb{D}_{n-1}+1$，

$$\mathscr{M}_{d(\iota),n}(\langle\mathbf{h}\rangle, \succ_{\mathrm{grevlex}}) = \left\{ x_n^{2d(\iota)-\mathbb{D}}\, m \;\middle|\; m \in \mathscr{B}_{\mathbb{D}-d(\iota),n-1}(\langle\mathbf{h}\rangle, \succ_{\mathrm{grevlex}}) \right\}. \tag{♡, 2}$$

固定 ι 于 $\{\mathbb{D}_{n-1}+2-\delta,\ldots,\mathbb{D}-\delta\}$。回顾可知，$d(\iota) = \iota+\delta$。这意味着 $d(\iota) \geq \mathbb{D}_{n-1}+2$。我们的目标是推导出关于约化子的数量的更精确上界。

考虑算法 p 第 ι 步中选取的一对 F4T。由于 $\langle\mathbf{h}\rangle$ 与 $\mathcal{T}$ 相容，因此算法 $\tilde{p}$ 中存在相应的一对 F4B，其涉及相同的首项单项式，并以 $\boldsymbol{f}$ 作为输入。我们将 $\tilde{p} = (t,\ t_i,\ g_i,\ t_j,\ g_j)$ 记作，其中

$$t = \mathrm{lcm}\big(\mathsf{lm}_{\succ_{\mathrm{grevlex}}}(g_i), \mathsf{lm}_{\succ_{\mathrm{grevlex}}}(g_j)\big), \quad t_i = \frac{t}{\mathsf{lt}_{\succ_{\mathrm{grevlex}}}(g_i)}, \quad \text{and} \quad t_j = \frac{t}{\mathsf{lt}_{\succ_{\mathrm{grevlex}}}(g_j)}.$$

我们证明 $(t_j,\ g_j)$ 是特殊的。

首先，[12, 定理 2.2]已证明，算法 F4B 的输出 G 是 I 的反向字典序 Gröbner 基。此外，利用引理 5.6 的断言 $\mathcal{H}_3(\cdot)$，我们知道，由于 $\mathsf{hom}(\boldsymbol{f})$ 属于 $\mathcal{S}_{\delta,\ n,\ n}$，该输出是一个最小反向字典序格罗布纳基。

这种情形符合第 3.2 节的框架，因此我们可以推断所有选定对都属于 $\mathscr{T}^{(1)}(G)$。更准确地说，这些对属于 $\mathscr{T}^{\star}(G)$，因为它们是由算法 F4B 第 10 行所描述的判据选出的。最后，由于 $\mathsf{hom}(\boldsymbol{f})$ 属于 $\mathcal{A}_{\delta,\ n,\ n}$ 且理想 I 是零维的，我们可以应用定理 3.4 得出 $(t_j,\ g_j)$ 是特殊的。

由于 $\langle\mathbf{h}\rangle$ 与 $\mathcal{T}$ 相容，对 p 与 $\tilde{p}$ 具有完全相同的首项单项式。由此可知，对 p 是利用一个首项单项式属于 $\mathscr{M}_{d(\iota)-1,\ n}(I,\ \succ_{\mathrm{grevlex}})$ 的多项式构造的。由于 $d(\iota-1) = d(\iota)-1$，因此，对 p 是利用一个首项单项式属于 $\mathscr{M}_{d(\iota-1),\ n}(I,\ \succ_{\mathrm{grevlex}})$ 的元素构造的。

此外，利用 (♡, 2)，这些元素在 x_n 中的次数等于 $2d(\iota)-\mathbb{D}-2$。因此，用于构造这些对的多项式的首项单项式在 x_n 中的次数至少为 $2d(\iota)-\mathbb{D}-2$。

我们来总结一下这一步中各对的性质：

- 它们的总次数为 $d(\iota)$；
- 每一对中的一个元素的次数为 $d(\iota)-1$；
- 该元素的首项单项式在 x_n 中的次数等于 $2d(\iota)-\mathbb{D}-2$；
- 这一步生成的新多项式在 x_n 中的次数等于 $2d(\iota)-\mathbb{D}$，根据 (♡, 2)。

回顾一下，我们处于顶端约化情形。由此可知，轨迹 $\mathcal{T}$ 满足：此步骤中使用的约化子次数也为 $d(\iota)$。因此，对于任意约化项的首项单项式 μ，我们有

$$2d(\iota)-\mathbb{D}-2 \ \leq\ \deg_{x_n}(\mu)\ \leq\ 2d(\iota)-\mathbb{D}.$$

此外，由于 $d(\iota) \geq \mathbb{D}_{n-1}+2$，我们有 $2d(\iota)-\mathbb{D}-2 > 0$。由此可得，对于所有整数 $i \in \{1,\ldots,n-1\}$，$\rho_{\iota,i}$ 的约化子数量为零。剩下的任务是给出对应于情形 $i=n$ 的约化子数量的上界。此类约化子的数量不超过次数为 $d(\iota)$ 且在 x_n 中的次数介于 $2d(\iota)-\mathbb{D}-2$ 和 $2d(\iota)-\mathbb{D}$ 之间的单项式数量。因此得到

$$\rho_{\iota,n} = \sum_{k=0}^{2} \binom{n-2+\mathbb{D}-d(\iota)+k}{\mathbb{D}-d(\iota)+k}, \quad \text{and} \quad \rho_{\iota,i} = 0 \ \text{ for all } \ i \in \{1,\ldots,n-1\}. \tag{♡, 3}$$

利用 (♡,2)，我们推得 $\gamma_{d(\iota),n}$ 不超过 $\mathscr{B}_{\mathbb{D}-d(\iota),n-1}(\langle \mathbf{h}\rangle, \succ_{\mathrm{grevlex}})$ 的基数，而后者又不超过 $\binom{n-2+\mathbb{D}-d(\iota)}{\mathbb{D}-d\ \iota}$ () 。因此，我们得到

$$\gamma_{d(\iota),n} \leq \binom{n-2+\mathbb{D}-d(\iota)}{\mathbb{D}-d(\iota)} < \rho_{\iota,n}. \tag{♡,4}$$

让我们深入探讨这一步骤更精细的算术复杂度表达式。首先，我们使用(♠) (♡,1) 以及关于约化子的数量的新上界(♡,3) 。因此，我们得到 $\mathsf{T}(\iota)^{\mathrm{red}} \in \mathcal{O}(N_{\iota,\mathrm{red}})$，其中

$$\begin{aligned} N_{\iota,\mathrm{red}} &\leq \frac{\binom{n+\iota+\delta}{\iota+\delta}\,\rho_{\iota,n}\,\gamma_{\iota+\delta,n}}{\min(\rho_{\iota,i},\gamma_{\iota+\delta,n})^{3-\omega}} + \gamma_{\iota+\delta,n}^{\omega-1}\binom{n+\iota+\delta}{\iota+\delta} \\ &\leq \binom{n+\iota+\delta}{\iota+\delta}\left(\rho_{\iota,n}\,\gamma_{\iota+\delta,n}^{\omega-2} + \gamma_{\iota+\delta,n}^{\omega-1}\right) && \text{(by (♡,4))} \\ &\leq 2\binom{n+\iota+\delta}{\iota+\delta}\rho_{\iota,n}\,\gamma_{\iota+\delta,n}^{\omega-2}. && \text{(by (♡,4))} \end{aligned}$$

我们已经看到，$\mathsf{T}(\iota)^{\mathrm{pairs}} \in \mathcal{O}(N_{\iota,\mathrm{pairs}})$，其中

$$\begin{aligned} N_{\iota,\mathrm{pairs}} &\leq \gamma_{\delta+\iota}\binom{n+\delta+\iota}{\delta+\iota} \\ &\leq \gamma_{\delta+\iota,n}\binom{n+\delta+\iota}{\delta+\iota} && \text{(by (♡,4))} \\ &\leq \binom{n+\iota+\delta}{\iota+\delta}\rho_{\iota,n}\,\gamma_{\iota+\delta,n}^{\omega-2}. && \text{(by (♡,1))} \end{aligned}$$

因此可得 $\mathsf{T}(\iota) \in \mathcal{O}\left(\widetilde{N_\iota}\right)$，其中

$$\widetilde{N_\iota} = \binom{n+\iota+\delta}{\iota+\delta}\rho_{\iota,n}\,\gamma_{\iota+\delta,n}^{\omega-2}.$$

证明至此结束。此外，我们定义 $N^{(2)} = \sum_{\iota=\mathbb{D}_{n-1}-\delta+2}^{\mathbb{D}-\delta} \widetilde{N_\iota}$。

6.3. 定理6.1的证明

现在我们旨在理解定理6.2中所确立的复杂度界的渐近行为，当变量 n 趋于无穷时。回顾一下，对于序列 $\boldsymbol{f}$ 中由 $\mathcal{R}_n$组成的，我们对所有 j属于 $\{1,\ldots,n\}$ 且所有整数 d，定义如下

$$\gamma_{d,j} = \sharp\left(\mathscr{M}_{d,j}(\langle \boldsymbol{f}\rangle, \succ_{\mathrm{grevlex}})\right).$$

此外，若 $\boldsymbol{f}$生成一个零维理想，对于所有整数 ι以及所有 i属于 $\{1,\ldots,n\}$，我们定义

$$\rho_{\iota,i} = \binom{i-1+\iota+\delta}{\iota+\delta} - \binom{i-2+\iota+\delta}{\iota+\delta} - \left(\sharp\left(\mathscr{B}_{\iota+\delta,i}(\langle \boldsymbol{f}\rangle, \succ_{\mathrm{grevlex}})\right) - \sharp\left(\mathscr{B}_{\iota+\delta,i-1}(\langle \boldsymbol{f}\rangle, \succ_{\mathrm{grevlex}})\right)\right).$$

对于一个序解 列 $\boldsymbol{f}$，其 $\mathcal{R}_n$次数为 δ且满足定理 6.2的假设，我们考虑分为 N_{F4T} 的两个项，并采用第 6.2 节中的记号

$$N_{F4T} = N^{(1)} + N^{(2)}$$

其中

$$N^{(1)} = \sum_{d=\delta}^{\mathbb{D}_{n-1}+1}\sum_{i=1}^{n}\binom{n+d}{d}\left(\frac{\rho_{d-\delta,i}\sum_{j=i}^{n}\gamma_{d,j}}{\min\left(\rho_{d-\delta,i},\sum_{j=i}^{n}\gamma_{d,j}\right)^{3-\omega}} + \left(\sum_{j=i}^{n}\gamma_{d,j}\right)^{\omega-1}\right)$$

and

$$N^{(2)} = \sum_{d=\mathbb{D}_{n-1}+2}^{\mathbb{D}}\gamma_{d,n}{}^{\omega-2}\binom{n+d}{d}\sum_{k=0}^{2}\binom{n-2+\mathbb{D}-d+k}{\mathbb{D}-d+k}$$

采用定理6.2 .

回忆一下，对于正实数 p in $(0,1]$, , 我们定义

$$E_p(\delta)=\ln\left(\frac{1+p(\delta-1)}{\delta}\right)+p(\delta-1)\ln\left(\frac{1+p(\delta-1)}{p(\delta-1)}\right).$$

此外，我们令 $L_\omega(2)=(1+e^{-1/(2(\omega-2))})^{-1}$，并通过令$L_2(2)=1$，利用连续性扩展此定义。为了证明定理6.1，我们先确立以下命题。

命题 6.3。沿用前述记号，并固定 $\delta\geq 2$ 的值，我们有：*1.* $N^{(1)}\in\widetilde{\mathcal{O}}\left(\delta^{\omega n+1}e^{2E_{1/2}(\delta)n}\right)$。

此外，若变量 $x_1,\ldots,x_n$ 关于 齐次($\boldsymbol{f}$) 处于同时诺特位置，我们有
ave that
2. $N^{(2)}\in\widetilde{\mathcal{O}}\left(\delta^{\omega n+3-\omega}e^{n\left(E_{1/2}(\delta)+E_{L_\omega(2)+\epsilon}(\delta)\right)}\right)$ *for all* $\epsilon>0$.

为完成命题6.3的证明，我们需要以下两个引理。这里给出贝祖界的一个特例及其推论。

引理 6.4。设 $\boldsymbol{f}=(f_1,\ldots,f_n)$ 是由 $\mathcal{R}_n$ 中的齐次多项式构成的正则序列，使得次数 $f_i=\delta_i$ 对所有 i 都成立，其中 $\{1,\ldots,n\}$。那么有

$$\sharp\left(\mathscr{B}(\langle\boldsymbol{f}\rangle,\succ_{\mathrm{grevlex}})\right)=\prod_{i=1}^{n}\delta_i\quad and\quad\sharp\left(G(\langle\boldsymbol{f}\rangle,\succ_{\mathrm{grevlex}})\right)\leq n\prod_{i=1}^{n}\delta_i.$$

证明。由于 $\boldsymbol{f}$ 是正则的，因此根据 [41, 命题 1]，其希尔伯特级数等于 $\prod_{i=1}^{n}\frac{1-z^{\delta_i}}{1-z}$。理想 $\langle x_1^{\delta_1},\ldots,x_n^{\delta_n}\rangle$的希尔伯特级数也相同。由此可得

$$\sharp\left(\mathscr{B}(\langle\boldsymbol{f}\rangle,\succ_{\mathrm{grevlex}})\right)=\sharp\left(\mathscr{B}(\langle x_1^{\delta_1},\ldots,x_n^{\delta_n}\rangle,\succ_{\mathrm{grevlex}})\right)=\prod_{i=1}^{n}\delta_i.$$

利用 [14, 命题 2.1], , 可得

$$\sharp\left(G(\langle\boldsymbol{f}\rangle,\succ_{\mathrm{grevlex}})\right)\leq n\sharp\left(\mathscr{B}(\langle\boldsymbol{f}\rangle,\succ_{\mathrm{grevlex}})\right)$$

至此证明完成。 □

利用通过伽马函数表示的广义二项式系数，并结合斯特林公式，可得到以下渐近结果。

引理 6.5。设 $\delta\geq 2$ 为一个固定整数，且令 $p\in(0,1]$。则有：

$$\binom{n+p(\delta-1)n}{p(\delta-1)n}\underset{n\to+\infty}{\sim}e^{E_p(\delta)\,n}\,\delta^n\sqrt{\frac{1+p(\delta-1)}{2\pi n\,p(\delta-1)}},$$

证明。我们首先将该二项式分解

$$\binom{n+p(\delta-1)n}{p(\delta-1)n}=\frac{\Gamma(n+p(\delta-1)n+1)}{\Gamma(n+1)\,\Gamma(p(\delta-1)n+1)}.$$

然后我们使用斯特林公式如下

$$\begin{aligned}\binom{n+p(\delta-1)n}{p(\delta-1)n}&\underset{n\to+\infty}{\sim}\left(\sqrt{\frac{1+p(\delta-1)}{2\pi\,n\,p(\delta-1)}}\right)\left(\frac{(n+p(\delta-1)n)^{n+p(\delta-1)n}}{n^n\,(p(\delta-1)n)^{p(\delta-1)n}}\right)\\&\underset{n\to+\infty}{\sim}\left(\sqrt{\frac{1+p(\delta-1)}{2\pi\,n\,p(\delta-1)}}\right)(1+p(\delta-1))^n\left(\frac{1+p(\delta-1)}{p(\delta-1)}\right)^{p(\delta-1)n}\\&\underset{n\to+\infty}{\sim}\left(\sqrt{\frac{1+p(\delta-1)}{2\pi\,n\,p(\delta-1)}}\right)\delta^n\left(\frac{1+p(\delta-1)}{\delta}\right)^n\left(\frac{1+p(\delta-1)}{p(\delta-1)}\right)^{p(\delta-1)n}\\&\underset{n\to+\infty}{\sim}\left(\sqrt{\frac{1+p(\delta-1)}{2\pi\,n\,p(\delta-1)}}\right)\delta^n\,e^{E_p(\delta)\,n}\end{aligned}$$

□

命题6.3的第 1项证明。我们首先对 $N^{(1)}$进行上界估计。

$$\begin{aligned}
&\sum_{d=\delta}^{\mathbb{D}_{n-1}+1}\sum_{i=1}^{n}\binom{n+d}{d}\left(\frac{\rho_{d-\delta,i}\sum_{j=i}^{n}\gamma_{d,j}}{\min\left(\rho_{d-\delta,i},\sum_{j=i}^{n}\gamma_{d,j}\right)^{3-\omega}}+\left(\sum_{j=i}^{n}\gamma_{d,j}\right)^{\omega-1}\right)\\
\leq&\sum_{d=\delta}^{\mathbb{D}_{n-1}+1}\sum_{i=1}^{n}\binom{n+\mathbb{D}_{n-1}+1}{\mathbb{D}_{n-1}+1}\left(\frac{\rho_{d-\delta,i}\sum_{j=i}^{n}\gamma_{d,j}}{\min\left(\rho_{d-\delta,i},\sum_{j=i}^{n}\gamma_{d,j}\right)^{3-\omega}}+\left(\sum_{j=i}^{n}\gamma_{d,j}\right)^{\omega-1}\right)\\
\leq&\binom{n+\mathbb{D}_{n-1}+1}{\mathbb{D}_{n-1}+1}\sum_{d=\delta}^{\mathbb{D}_{n-1}+1}\sum_{i=1}^{n}\left(\frac{\rho_{d-\delta,i}\sum_{j=i}^{n}\gamma_{d,j}}{\min\left(\rho_{d-\delta,i},\sum_{j=i}^{n}\gamma_{d,j}\right)^{3-\omega}}+\left(\sum_{j=i}^{n}\gamma_{d,j}\right)^{\omega-1}\right)\\
\leq&\binom{n+\mathbb{D}_{n-1}+1}{\mathbb{D}_{n-1}+1}\sum_{d=\delta}^{\mathbb{D}_{n-1}+1}\sum_{i=1}^{n}\left(\rho_{d-\delta,i}\left(\sum_{j=i}^{n}\gamma_{d,j}\right)^{\omega-2}+\rho_{d-\delta,i}^{\omega-2}\left(\sum_{j=i}^{n}\gamma_{d,j}\right)+\left(\sum_{j=i}^{n}\gamma_{d,j}\right)^{\omega-1}\right)\\
\leq&n^{\omega-1}\binom{n+\mathbb{D}_{n-1}+1}{\mathbb{D}_{n-1}+1}\sum_{d=\delta}^{\mathbb{D}_{n-1}+1}\sum_{i=1}^{n}\left(\rho_{d-\delta,i}\,\delta^{n(\omega-2)}+\rho_{d-\delta,i}^{\omega-2}\,\delta^{n}+\delta^{n(\omega-1)}\right)\qquad\text{(by Lemma 6.4)}
\end{aligned}$$

由于根据定义有 $\rho_{d-\delta,\,i}\leq\binom{n+\mathbb{D}_{n-1}+1}{\mathbb{D}_{n-1}+1}$，因此我们得到

$$\begin{aligned}
&\sum_{d=\delta}^{\mathbb{D}_{n-1}+1}\sum_{i=1}^{n}\binom{n+d}{d}\left(\frac{\rho_{d-\delta,i}\sum_{j=i}^{n}\gamma_{d,j}}{\min\left(\rho_{d-\delta,i},\sum_{j=i}^{n}\gamma_{d,j}\right)^{3-\omega}}+\left(\sum_{j=i}^{n}\gamma_{d,j}\right)^{\omega-1}\right)\\
\leq&n^{\omega-1}\binom{n+\mathbb{D}_{n-1}+1}{\mathbb{D}_{n-1}+1}\sum_{d=\delta}^{\mathbb{D}_{n-1}+1}\sum_{i=1}^{n}\left(\binom{n+\mathbb{D}_{n-1}+1}{\mathbb{D}_{n-1}+1}\delta^{n(\omega-2)}+\binom{n+\mathbb{D}_{n-1}+1}{\mathbb{D}_{n-1}+1}^{\omega-2}\delta^{n}+\delta^{n(\omega-1)}\right).\\
\leq&\delta n^{\omega+1}\binom{n+\mathbb{D}_{n-1}+1}{\mathbb{D}_{n-1}+1}\left(\binom{n+\mathbb{D}_{n-1}+1}{\mathbb{D}_{n-1}+1}\delta^{n(\omega-2)}+\binom{n+\mathbb{D}_{n-1}+1}{\mathbb{D}_{n-1}+1}^{\omega-2}\delta^{n}+\delta^{n(\omega-1)}\right).\qquad(1)
\end{aligned}$$

我们有

$$\begin{aligned}
\binom{n+\mathbb{D}_{n-1}+1}{\mathbb{D}_{n-1}+1}&\leq\binom{n+\frac{n(\delta-1)}{2}+2}{\frac{n(\delta-1)}{2}+2}\leq\left(1+\frac{2n}{n(\delta-1)+4}\right)\left(1+\frac{2n}{n(\delta-1)+2}\right)\binom{n+\frac{n(\delta-1)}{2}}{\frac{n(\delta-1)}{2}}\\
&\leq 9\binom{n+\frac{n(\delta-1)}{2}}{\frac{n(\delta-1)}{2}}.
\end{aligned}$$

应用引理6.5 于上述上界，并取 $p=\frac{1}{2}$，我们得到

$$\binom{n+\mathbb{D}_{n-1}+1}{\mathbb{D}_{n-1}+1}\in\widetilde{\mathcal{O}}\left(e^{E_{1/2}(\delta)\,n}\,\delta^{n}\right).\qquad(2)$$

结合(1) 和(2)，我们有

$$\begin{aligned}
N^{(1)}&\in\widetilde{\mathcal{O}}\left(\delta^{\omega n+1}\left(e^{2E_{1/2}(\delta)n}+e^{(\omega-1)E_{1/2}(\delta)n}+e^{E_{1/2}(\delta)n}\right)\right)\\
&\subset\widetilde{\mathcal{O}}\left(\delta^{\omega n+1}e^{2E_{1/2}(\delta)n}\right).
\end{aligned}$$

□

在深入证明命题6.3的第2项之前，我们先引入一些上界。为此，我们使用 [2, 定理 12]。设 i 属于 $\{1,\ldots,n\}$，且 d 为一个整数。我们首先定义 $b_d^{(i)}$ 如下

$$\sum_{d=0}^{+\infty}b_d^{(i)}z^d=z^{\delta}\prod_{j=1}^{i-1}\frac{1-z^{\delta}}{1-z}.$$

以下引理在一般性假设下，为 grevlex 最小格罗布纳基中子集的基数建立了一些上界。对于此引理，我们采用定理 6.2中引入的以下记号

$$\gamma_d=\sharp\left(\mathscr{M}_{d,*}(\langle\boldsymbol{f}\rangle,\succ_{\text{grevlex}})\right)\quad\text{and}\quad\gamma_{d,i}=\sharp\left(\mathscr{M}_{d,i}(\langle\boldsymbol{f}\rangle,\succ_{\text{grevlex}})\right).$$

引理 6.6。 考虑多项式序列 $\boldsymbol{f}=(f_1,\dots,f_n)$，使得变量 $x_1,\dots,x_n$ 相对于多项式序列 (齐次化$(f_1)\dots,$ 齐次化 (f_n)) 处于同时诺特位置。那么，对于所有 $i\in\{1,\dots,n\}$ 和所有 $d\in\mathbb{N}$，有

$$\sum_{j=i}^{n}\gamma_{d,j}\leq\sum_{j=i}^{n}b_d^{(j)}.$$

证明。 我们通过确立四个关键断言来证明此引理。

首先，由于变量 x_1、……、x_n 相对于多项式序列 $(\mathsf{hom}(f_1)$……、$\mathsf{hom}(f_n))$处于同时诺特位置，根据 [2, 命题 6] 可知 $(\mathsf{hom}(f_1)$……、$\mathsf{hom}(f_n))$ 是正则序列。因此，我们应用推论 5.8 得到

$$\mathsf{lm}_{\succ_{\mathrm{grevlex}}}(\langle\boldsymbol{f}\rangle)=\mathsf{lm}_{\succ_{\mathrm{grevlex}}}(\langle\mathsf{hom}(\boldsymbol{f})\rangle).\tag{$\star,1$}$$

在证明的其余部分，对于所有 $j\in\{1,\dots,n\}$，我们设 $I_j=\langle\mathsf{hom}(f_1)$……、$\mathsf{hom}(f_j)\rangle$。

令 $i\in\{1,\dots,n\}$。由于变量 x_1、……、x_n 相对于 o
该序列 多项式 $(\mathsf{hom}(f_1)\dots,\mathsf{hom}(f_n))$ 的集合，我们可以应用 [2, 命题 11]。于是，我们得到 in

$$\bigcup_{j=1}^{i-1}\mathscr{M}_{d,*}(I_j,\succ_{\mathrm{grevlex}})\subseteq\mathsf{Mon}_{d,i-1}\,.$$

另一方面，根据定义，

$$\bigsqcup_{j=i}^{n}\mathscr{M}_{d,j}(I_n,\succ_{\mathrm{grevlex}})\subseteq(\mathsf{Mon}_d\setminus\mathsf{Mon}_{d,i-1})\,.$$

由此可得

$$\bigsqcup_{j=i}^{n}\mathscr{M}_{d,j}(I_n,\succ_{\mathrm{grevlex}})\subseteq\mathscr{M}_{d,*}(I_n,\succ_{\mathrm{grevlex}})\setminus\left(\bigcup_{j=1}^{i-1}\mathscr{M}_{d,*}(I_j,\succ_{\mathrm{grevlex}})\right).\tag{$\star,2$}$$

为了证明下一个性质，我们使用以下备注。

备注 6.7. 设 E_1、…、E_n 是集合。那么，对于所有 $i\in\{1,\dots,n\}$，我们有

$$E_n\setminus\left(\bigcup_{j=1}^{i-1}E_j\right)\subseteq\bigsqcup_{j=i}^{n}\left(E_j\setminus\bigcup_{k=1}^{j-1}E_k\right).$$

令 $E_i=\mathscr{M}_{d,\ *}(I_i,\ \succ_{\mathrm{grevlex}})$ 并应用备注 6.7，我们得到

$$\mathscr{M}_{d,*}(I_n,\succ_{\mathrm{grevlex}})\setminus\left(\bigcup_{j=1}^{i-1}\mathscr{M}_{d,*}(I_j,\succ_{\mathrm{grevlex}})\right)\subseteq\bigsqcup_{j=i}^{n}\mathscr{M}_{d,*}(I_j,\succ_{\mathrm{grevlex}})\setminus\left(\bigcup_{k=1}^{j-1}\mathscr{M}_{d,*}(I_k,\succ_{\mathrm{grevlex}})\right).\tag{$\star,3$}$$

再次利用变量 x_1、……、x_n 关于多项式序列 $(\mathsf{hom}(f_1)$……、$\mathsf{hom}(f_n))$ 处于同时诺特位置，根据 [2, 定理 12] 可得不等式

$$\sharp\left(\mathscr{M}_{d,*}(I_j,\succ_{\mathrm{grevlex}})\setminus\mathscr{M}_{d,*}(I_{j-1},\succ_{\mathrm{grevlex}})\right)\leq b_d^{(j)}\tag{$\star,4$}$$

对所有 $j\in\{1,\dots,n\}$ 都成立。

现在我们可以得出结论：

$$\begin{aligned}
\sum_{j=i}^{n}\gamma_{d,j} &= \sharp\left(\bigsqcup_{j=i}^{n}\mathscr{M}_{d,j}(I_n,\succ_{\mathrm{grevlex}})\right) && \text{(by } (\star,1)\text{)}\\
&\le \sharp\left(\mathscr{M}_{d,*}(I_n,\succ_{\mathrm{grevlex}})\setminus\left(\bigcup_{j=1}^{i-1}\mathscr{M}_{d,*}(I_j,\succ_{\mathrm{grevlex}})\right)\right) && \text{(by } (\star,2)\text{)}\\
&\le \sum_{j=i}^{n}\sharp\left(\mathscr{M}_{d,*}(I_j,\succ_{\mathrm{grevlex}})\setminus\left(\bigcup_{k=1}^{j-1}\mathscr{M}_{d,*}(I_k,\succ_{\mathrm{grevlex}})\right)\right) && \text{(by } (\star,3)\text{)}\\
&\le \sum_{j=i}^{n}\sharp\left(\mathscr{M}_{d,*}\left(I_j,\succ_{\mathrm{grevlex}}\right)\setminus\mathscr{M}_{d,*}\left(I_{j-1},\succ_{\mathrm{grevlex}}\right)\right)\\
&\le \sum_{j=i}^{n}b_d^{(j)}. && \text{(by } (\star,4)\text{)}
\end{aligned}$$

□

命题 *6.3*的第 *2* 项的证明。首先有

$$\begin{aligned}
N^{(2)} &= \sum_{d=\mathbb{D}_{n-1}+2}^{\mathbb{D}}\gamma_{d,n}^{\omega-2}\binom{n+d}{d}\sum_{k=0}^{2}\binom{n-2+\mathbb{D}-d+k}{\mathbb{D}-d+k}\\
&\le \sum_{d=\mathbb{D}_{n-1}+2}^{\mathbb{D}}\left(b_d^{(n)}\right)^{\omega-2}\binom{n+d}{d}\sum_{k=0}^{2}\binom{n-2+\mathbb{D}-d+k}{\mathbb{D}-d+k} && \text{(by Lemma 6.6)}\\
&\le 3\sum_{d=\mathbb{D}_{n-1}+2}^{\mathbb{D}}\left(b_d^{(n)}\right)^{\omega-2}\binom{n+d}{d}\binom{n-2+\mathbb{D}-d+2}{\mathbb{D}-d+2}.
\end{aligned}$$

现在，假设 $\omega>2$。$\omega=2$ 的情形将在证明末尾处理，因为它比情形 $\omega>2$简单。我们仿照 [2, 第 3 节 2], 中的推理，同时将其调整到我们的情境中。为建立我们的结果，我们回顾在那里引入的内容。

对于所有 $r>0$，都有 $b_d^{(n)}\le\frac{B_n}{(r)\ r^d}$，其中 $B_n(r)=r^\delta\prod_{j=1}^{n-1}\frac{1-r^\delta}{1-r}$。对于固定的 d 和 n，存在$r(n,\ d)>0$，使得 $\frac{B_n}{(r)\ r^d}$最小。现在我们可以写出

$$N^{(2)}\le 3\sum_{d=\mathbb{D}_{n-1}+2}^{\mathbb{D}}\left(\frac{B_n(r(n,d))}{r(n,d)^d}\right)^{\omega-2}\binom{n+d}{d}\binom{n-2+\mathbb{D}-d+2}{\mathbb{D}-d+2}. \tag{1}$$

此外，根据 [2, 第 3 节2], ，我们知道 $r(n,\ d)$ 满足以下方程：

$$\frac{d-\delta}{n-1}=\frac{\delta}{1-r^{-\delta}}-\frac{1}{1-r^{-1}} \tag{2}$$

且 $r(n,\ d)$ 关于 d 可微且递增。

现在，我们通过计算各项关于 d的对数导数，来确定在 (1) 中占主导地位的次数 $d(n)$。设 ψ 为 Γ 函数的对数导数（参见 [1, 第 6]章），当

$$\begin{aligned}
(\omega-2)\log(r(n,d)) &= \psi(d+n+1)-\psi(d+1)-\psi(n+\mathbb{D}-d+1)+\psi(\mathbb{D}-d+3)\\
&= \sum_{i=1}^{n}\frac{1}{d+i}-\sum_{i=2}^{n-1}\frac{1}{\mathbb{D}-d+i+1}.
\end{aligned} \tag{3}$$

我们推得，(3) 定义了唯一的函数 $d(n)$，使得

- $d(n)$ 满足(3)；
- $(d(n)\ r(n,d(n)))$ 满足(2)。

由于 $\mathbb{D}-d+1\le d$ 对所有 $d\ge \mathbb{D}_{n-1}+2$ 均成立，因此我们有

$$(\omega-2)\log(r(n,d(n))) = \sum_{i=1}^{n}\frac{1}{d(n)+i} - \sum_{i=2}^{n-1}\frac{1}{\mathbb{D}-d(n)+i+1} \qquad \text{(by (3))}$$
$$\le \frac{1}{\delta}+\frac{1}{\delta+n} \quad . \qquad (4)$$

上界 $\frac{1}{\delta}+\frac{1}{\delta+n}$ 记作 $t(n)$。

由 (4) 可推得 $r(n,\ d(n)) \le e^{\frac{t}{(n)\,\omega-2}}$，这意味着 $r(n,\ d(n))^{-1} \ge e^{-\frac{t(n)}{\omega-2}}$。

我们考虑函数 $f:\ x\mapsto \frac{\delta}{1-x^{\delta}} - \frac{1}{1-x^{\circ}}$ 函数 f 在 $x\ge 0$ 上有定义、连续且单调递减，并且 $f(0)=\delta-1$。结合 (2)，可推得

$$\frac{d(n)-\delta}{n-1} \le f\left(e^{-\frac{t(n)}{\omega-2}}\right). \qquad (5)$$

我们回顾一下此证明的结构。我们已经得到了关于 (1) 的上界 $N^{(2)}$，并确定了对应于该上界中最高次项的次数 $d(n)$。然而，我们无法给出 $d(n)$的显式表达式。因此，在接下来的推理中，我们使用 (5) 对次数 $d(n)$ 作上界估计，然后将其代入 (1)。为此，我们确定 $p\in[0,1]$的可能取值，这些取值独立于 δ，且存在一个整数 n_0 使得对所有 $n\ge n_0$，不等式

$$f\left(e^{-\frac{t(n)}{\omega-2}}\right) \le p(\delta-1) \qquad (6)$$

成立。

我们定义 $x(n) = e^{-\frac{t}{(n)\,\omega-2}}$。函数 $x(n)$ 单调递增，因此 $f(x(n))$ 单调递减。因此，我们需要找到一个与 p 无关的 n_0，使得 $f(x(n_0)) \le p(\delta-1)$。当 n 趋于无穷时，$x(n)$ 趋于 $x_\infty(\delta,\ \omega) = e^{-\frac{1}{\omega-2}}$。由此可得，$f(x(n))$ 的极限为 $L_\omega(\delta) = f(x_\infty(\delta,\ \omega))$。因此，$p$ 必须满足

$$\sup_{\delta\ge 2}\frac{L_\omega(\delta)}{\delta-1} < p.$$

该上确界在 $\delta=2$ 处取得，因此 $L_\omega(2)<p$。于是我们知道，条件 (6) 等价于$L_\omega(2)<p$，其中

$$L_\omega(2) = \frac{1}{1+e^{-\frac{1}{2(\omega-2)}}}.$$

最后，结合 (5)和 (6)，对于所有 $p>L_\omega(2)$，存在 n_0，使得对于所有 $n\ge n_0$，以下不等式成立：

$$d(n) \le p(\delta-1)(n-1)+\delta$$
$$\le \left(p+\frac{1}{n-1}\right)(\delta-1)(n-1)+1.$$

这意味着，对于所有 $p>L_\omega(2)$，都存在 n_0，使得对于所有 $n\ge n_0$，我们有

$$d(n) \le p(\delta-1)(n-1)+1$$
$$\le p(\delta-1)n+1.$$

设 $n\ge n_0$，我们使用 $d(n)$，它是使 (1) 中的和式项达到最大的次数。这就得到以下不等式

$$N^{(2)} \le 3n\delta\left(\frac{B_n(r(n,d(n)))}{r(n,d(n))^{d(n)}}\right)^{\omega-2}\binom{n+d(n)}{d(n)}\binom{n-2+\mathbb{D}-d(n)+2}{\mathbb{D}-d(n)+2}. \qquad (7)$$

现在，w 我们建立两个不等式，并将其代入 (7)。由于 $d(n)\ge \mathbb{D}_{n-1}+2$ 我们有

$$\binom{n-2+\mathbb{D}-d(n)+2}{\mathbb{D}-d(n)+2} \le \binom{n-2+\mathbb{D}-\mathbb{D}_{n-1}}{\mathbb{D}-\mathbb{D}_{n-1}} \le \binom{n-2+\mathbb{D}_{n-1}+2}{\mathbb{D}_{n-1}+2} \le \binom{n+\frac{n(\delta-1)}{2}+3}{\frac{n(\delta-1)}{2}+3}$$
$$\le \left(1+\frac{2n}{n(\delta-1)+6}\right)\left(1+\frac{2n}{n(\delta-1)+4}\right)\left(1+\frac{2n}{n(\delta-1)+2}\right)\binom{n+\frac{n(\delta-1)}{2}}{\frac{n(\delta-1)}{2}}$$
$$\le 27\binom{n+\frac{n(\delta-1)}{2}}{\frac{n(\delta-1)}{2}}. \qquad (8)$$

由于对所有 $r>0$， $r(n,\ d(n))$ 都能使 $\binom{B_n}{r^{d(n)}}$ 取最小值，因此我们可以令 $r=1$，从而得到其上界。由此可得

$$\left(\frac{B_n(r(n,d(n)))}{r(n,d(n))^{d(n)}}\right)\leq\delta^{n-1}. \tag{9}$$

令 $p=L_\omega(2)+\epsilon$ 满足 $\epsilon>0$。对于 $\omega=2$的情况，只需令 $L_\omega(2)=1$。我们有 $p\geqslant\frac{1}{2}$。在 (7) 中使用(8) 和(9)，可得

$$\begin{aligned}
N^{(2)} &\leq 81n\delta^{(\omega-2)(n-1)+1}\binom{n+d(n)}{d(n)}\binom{n+\frac{n(\delta-1)}{2}}{\frac{n(\delta-1)}{2}}\\
&\leq 81n\delta^{(\omega-2)(n-1)+1}\binom{n+p(\delta-1)n+1}{p(\delta-1)n+1}\binom{n+\frac{n(\delta-1)}{2}}{\frac{n(\delta-1)}{2}} && \text{(because } n\geq n_0\text{)}\\
&\leq 243n\delta^{(\omega-2)(n-1)+1}\binom{n+p(\delta-1)n}{p(\delta-1)n}\binom{n+\frac{n(\delta-1)}{2}}{\frac{n(\delta-1)}{2}}. && \text{(because } p\geq\tfrac{1}{2}\text{)}
\end{aligned}$$

回顾一下， δ 是固定的。现在，我们对两个二项式应用引理 6.5 ，得到

$$N^{(2)}\in\widetilde{\mathcal{O}}\Big(\delta^{\omega n+3-\omega}\,e^{n\left(E_{1/2}(\delta)+E_{L_\omega(2)+\epsilon}(\delta)\right)}\Big) \qquad \square$$

为了完成定理 6.1的证明，我们建立以下引理。

引理 6.8。 设 $\delta\geq 2$ 为一个整数，且 p_1 和 p_2 属于 $(0,1]$ ，满足 $p_1<p_2$。*Th* *en*

$$E_{p_1}(\delta)<E_{p_2}(\delta)$$

证明。 固定一个整数 $\delta\geq 2$。我们将函数 $E_p(\delta)$ 视为变量 $p\in(0,1]$的函数。

该函数在 $(0,1]$上定义良好且可微。直接计算可知，它关于 p 的导数为

$$\begin{aligned}
\frac{\partial}{\partial p}E_p(\delta) &= \frac{\delta-1}{\delta}\times\frac{\delta}{1+p(\delta-1)}+(\delta-1)\ln\left(\frac{1+p(\delta-1)}{p(\delta-1)}\right)-\frac{\delta-1}{1+p(\delta-1)}\\
&= (\delta-1)\ln\left(\frac{1+p(\delta-1)}{p(\delta-1)}\right).
\end{aligned}$$

由于 $\delta\geq 2$ 和 $p\in(0,1]$, ，我们有

$$\frac{1+p(\delta-1)}{p(\delta-1)}>1,$$

因此对数为正。由此可得， $\frac{\partial}{\partial p}E_p(\delta)>0$ 在 $(0,1]$上。 —

因此，函数 $E_p(\delta)$ 关于 p 在 $(0,1]$上严格递增。 $\square$

定理 6.1 的证明。根据假设，序列 $\mathsf{hom}(f)$ 属于 $\mathcal{A}_{\delta,n,n}\cap\mathcal{D}_{\delta,n}\cap\mathcal{S}_{\delta,n,n}$，其中 $\delta\geq 2$且 $n\geq 2$。此外， $\phi(\mathsf{hom}(f))$ $n-1$) 属于 $\mathcal{S}_{\delta,n-1,n}$。因此，我们可以应用定理 6.2 并推断：对与格罗布纳轨迹 $\mathcal{T}$相容的多项式序列运行算法 F4T，需要在 $\mathbb{K}$中进行 $\mathcal{O}(N_{F4T})$ 次运算。

回顾一下 $N_{F4T}=N_{(1)}+N_{(2)}$。由于变量 $x_1,\ldots,x_n$相对于 $\mathsf{hom}(f)$处于同时诺特位置，我们可以应用命题 6.3 并得到

$$N_{F4T}\in\widetilde{\mathcal{O}}\left(\delta^{\omega n+1}\left(e^{n\left(E_{1/2}(\delta)+E_{L_\omega(2)+\epsilon}(\delta)\right)}+e^{2nE_{1/2}(\delta)}\right)\right)$$

对所有 $\epsilon>0$。由于 $L_\omega(2)\geqslant\frac{1}{2}$，我们可以应用引理 6.8 推得

$$N_{F4T}\in\widetilde{\mathcal{O}}\left(\delta^{\omega n+1}e^{n\left(E_{1/2}(\delta)+E_{L_\omega(2)+\epsilon}(\delta)\right)}\right)\quad\text{for all }\epsilon>0. \qquad \square$$

6.4. 公式比较

我们首先将我们的复杂度估计与 Lazard 算法的复杂度估计进行比较。Lazard 算法在 [33],中提出，通常应用于满足某些正则性假设的 F4 算法族（例如参见[15, 16, 17, 18]）。

我们的第二项比较是与文献 [2] 中针对 F5算法 某一变体所确立的、更为精确的复杂度进行比较。F5算法 的一个主要优势在于，得益于其签名系统，在正则性假设下，它可以避免所有归约为零。然而，这一机制也带来了一个重要限制：它阻碍了该算法充分利用高效的线性代数技术来对 Macaulay 矩阵 [11] 执行行阶梯变换。具体而言，签名系统限制了可能进行的行变换，从而限制了优化的稠密或稀疏线性代数方法的使用。

由于算法 F4T 同样旨在消除归约为零的情况（但所采用的框架更为严格），因此，对这两种算法进行比较仍然是自然且有意义的。

计算序列 $\boldsymbol{f} = (f_1, \ldots, f_n)$ 在 $\mathcal{R}_n$ 中计算 grevlex Gröbner 基的背景与第 6节其余部分相同。我们的比较基于对复杂度公式进行评估。

We 回想一下， N_{F4T}可以表示为以下各项之和： $N_{(1)} + N_{(2)}$，如第6.2节所示。注意 t

$$N^{(2)} = \sum_{d=\mathbb{D}_{n-1}+2}^{\mathbb{D}} {\gamma_{d,n}}^{\omega-2} \binom{n+d}{d} \sum_{k=0}^{2} \binom{n-2+\mathbb{D}-d+k}{\mathbb{D}-d+k},$$

其中 $\gamma_{d,n} = \sharp(G_{d,n}(\langle \boldsymbol{f} \rangle, \succ_{\text{grevlex}}))$。由于我们在定理6.2 中假设$\mathsf{hom}(\boldsymbol{f})$属于$\mathcal{S}_{\delta,n,n}$，序列$\mathsf{hom}(\boldsymbol{f})$ 是正则的，并且根据推论5.8 可得

$$\sharp(G_{d,n}(\langle \boldsymbol{f} \rangle, \succ_{\text{grevlex}})) = \sharp(G_{d,n}(\langle \mathsf{hom}(\boldsymbol{f}) \rangle, \succ_{\text{grevlex}})).$$

此外，由于我们在定理6.2 中假设$\mathsf{hom}(\boldsymbol{f})$属于$\mathcal{D}_{\delta,n}$且 $\phi(\mathsf{hom}(\boldsymbol{f})\ n-1)$属于$\mathcal{S}_{\delta,n-1,n}$，我们可以对4.6 应用定理 $\mathsf{hom}(\boldsymbol{f})$ ，从而推出

$$\gamma_{d,n} = \sharp(G_{d,n}(\langle \mathsf{hom}(\boldsymbol{f}) \rangle, \succ_{\text{grevlex}})) = \beta_{\mathbb{D}-d},$$

其中 $\left[\frac{n}{(1-z^{\delta})^{n-1}}\right]_+ = \sum_{d=0}^{\mathbb{D}_{n-1}-1} \beta_d z^d$（

$1-z)$。

我们引入一个新的公式 $\widetilde{N}_{F4T} = \widetilde{N}_{(1)} + N_{(2)}$，使得 $N_{(1)} \leq \widetilde{N}^{(1)}$在某些一般性假设下成立。为此，我们采用 $b_d^{(i)}$ 引理6.6之前刚刚引入的记号。此外，对所有 i属于$\{0, \ldots, n\}$的，我们引入以下记号：

$$\left[\frac{(1-z^{\delta})^n}{(1-z)^i}\right]_+ = \sum_{d=0}^{+\infty} \beta_{d,i}\, z^d.$$

我们还使用 第 4.1 节引入的截断 ϕ。现在我们在以下命题中表示 $\widetilde{N}^{(1)}$ n.

命题6.9。 假设对于所有 $i \in \{1, \ldots, n\}$，序列 ϕ(齐次($\boldsymbol{f}$) i) 都属于 $\mathcal{S}_{\delta,\ i,\ n}$，且变量 x_1、.....、x_n 相对于 齐次($\boldsymbol{f}$)处于同时诺特位置。那么我们有$N^{(1)} \leq \widetilde{N}^{(1)}$，其中

$$\widetilde{N}^{(1)} = \sum_{d=\delta}^{\mathbb{D}_{n-1}+1} \sum_{i=1}^{n} \binom{n+d}{d} \left(\frac{\widetilde{\rho}_{d-\delta,i} \sum_{j=1}^{n} b_d^{(j)}}{\min\left(\rho_{d-\delta,i}, \sum_{j=1}^{n} b_d^{(j)}\right)^{3-\omega}} + \left(\sum_{j=1}^{n} b_d^{(j)}\right)^{\omega-1} \right)$$

其中

$$\widetilde{\rho}_{d-\delta,i} = \binom{i-1+d}{d} - \binom{i-2+d}{d} - (\beta_{d,i} - \beta_{d,i-1}).$$

证明。 我们回顾一下

$$N^{(1)} = \sum_{d=\delta}^{\mathbb{D}_{n-1}+1} \sum_{i=1}^{n} \binom{n+d}{d} \left(\frac{\rho_{d-\delta,i} \sum_{j=i}^{n} \gamma_{d,j}}{\min\left(\rho_{d-\delta,i}, \sum_{j=i}^{n} \gamma_{d,j}\right)^{3-\omega}} + \left(\sum_{j=i}^{n} \gamma_{d,j}\right)^{\omega-1} \right).$$

由于变量 $x_1,\dots,x_n$ 相对于 齐次化($\boldsymbol{f}$)处于同时诺特位置，因此我们可以应用引理 6.6 来推导出

$$N^{(1)} \leq \sum_{d=\delta}^{\mathbb{D}_{n-1}+1} \sum_{i=1}^{n} \binom{n+d}{d} \left(\frac{\rho_{d-\delta,i} \sum_{j=1}^{n} b_d^{(j)}}{\min\left(\rho_{d-\delta,i}, \sum_{j=1}^{n} b_d^{(j)}\right)^{3-\omega}} + \left(\sum_{j=1}^{n} b_d^{(j)}\right)^{\omega-1} \right).$$

设 d 属于 $\{\delta,\dots,\mathbb{D}_{n-1}+1\}$，并设 i 属于 $\{1,\dots,n\}$。根据第$\rho_{d-\delta}$节i 6.2 节中给出的定义，可得

$$\rho_{d-\delta,i} = \binom{i-1+d}{d} - \binom{i-2+d}{d} - \left(\sharp\left(\mathscr{B}_{d,i}(\langle \mathsf{hom}(\boldsymbol{f})\rangle, \succ_{\mathrm{grevlex}})\right) - \sharp\left(\mathscr{B}_{d,i-1}(\langle \mathsf{hom}(\boldsymbol{f})\rangle, \succ_{\mathrm{grevlex}})\right)\right).$$

应用推论4.5，可得

$$\sharp\left(\mathscr{B}_{d,i}(\langle \mathsf{hom}(\boldsymbol{f})\rangle, \succ_{\mathrm{grevlex}})\right) = \sharp\left(\mathscr{B}_{d,i}(\langle \phi(\mathsf{hom}(\boldsymbol{f}), i)\rangle, \succ_{\mathrm{grevlex}})\right).$$

因为，根据假设，序列 ϕ(hom($\boldsymbol{f}$) i) 属于 $\mathcal{S}_{\delta,\ i,\ n}$，由 [41, 命题 1] th 可推得 at

$$\sharp\left(\mathscr{B}_{d,i}(\langle \phi(\mathsf{hom}(\boldsymbol{f}), i)\rangle, \succ_{\mathrm{grevlex}})\right) = \beta_{d,i}.$$

对 $\sharp$($\mathscr{B}_{d,\ i-1}$(⟨hom($\boldsymbol{f}$)⟩, $\succ_{\mathrm{grevlex}}$)) 应用相同的推理，即可完成证明。 □

现在我们得到一个新的公式 $\widetilde{N}_{F4T} = \widetilde{N}_{(1)} + N_{(2)}$，它更容易计算，并且是 N_{F4T} 的一个上界。

我们从 Lazard 算法的复杂度比较开始。考虑多项式序列 $\boldsymbol{f}$ =(f_1、.....、 f_n)，使得 hom($\boldsymbol{f}$) 属于第4.2节中引入的扎里斯基开集 $\mathcal{S}_{\delta、\ n、\ n}$。hom($\boldsymbol{f}$) 属于 $\mathcal{S}_{\delta、\ n、\ n}$ 这一事实导出以下推论。

首先，理想 ⟨hom($\boldsymbol{f}$)⟩ 是零维的，因为其希尔伯特级数是一个多项式 [41, 命题 1]。因此，根据 [33, 定理 3], ， ⟨hom($\boldsymbol{f}$)⟩ 的最小反向字典序格罗布纳基中元素的最大次数为 Macaulay 界

$$\mathbb{D} = n(\delta-1)+1.$$

利用推论 5.8，同样的结果也适用于 ⟨$\boldsymbol{f}$⟩。

此外，利用引理 $\mathcal{H}_5(\cdot)$ 中的断言 5.6， $\mathbb{K}$维向量空间

$$\langle S\rangle_{\mathbb{K}} \quad \text{where} \quad S = \{m f_i \mid i \in \{1,\dots,s\},\ m \in \mathsf{Mon}_{\leq \mathbb{D}-\delta,n}\}$$

包含 ⟨$\boldsymbol{f}$⟩ 的一个反向字典序格罗布纳基。因此，Lazard 算法包括计算矩阵的行阶梯形

$$\mathrm{Mac}(S, \mathsf{Mon}_{\leq \mathbb{D},n}).$$

根据 [43, 第 2], 章，其算术复杂度为

$$\mathcal{O}(N_L), \qquad \text{with} \qquad N_L = n\binom{n+\mathbb{D}}{\mathbb{D}}^{\omega}.$$

~图 2 比较了 N_L 与 N_{F4T} 在 $\omega=3$ 及不同 δ取值下的比值的对数。它展示了我们对算法F4T 的分析带来的 n 指数级提升。请注意，随着 δ 增大，这一优势似乎略有增加。例如，当 $\omega=3$ 且 $\delta=30$时，$\ln\left(\frac{N_L}{\widetilde{N}_{F4T}}\right)$ 关于 n 的函数的斜率约为2.550。

图 3 给出了相同的比较，但固定 δ 为10 ，并取 ω的不同值。图中显示，当 ω 减小时，这种指数级优势会减弱，但即使假设 $\omega=2$，优势仍然存在。例如，当 $\omega=2$ 且 $\delta=10$时，$\ln\left(\frac{N_L}{\widetilde{N}_{F4T}}\right)$ 关于 n 的函数的斜率约为1.335。

~现在我们将 N_{F4T}与 N_{F5}进行比较，后者是 [2]中得到的复杂度结果。回顾一下，该分析假设 hom($\boldsymbol{f}$) 属于 $\mathcal{S}_{\delta,n,n}$，并且变量 $x_1,\dots,x_n$ 相对于序列 hom($\boldsymbol{f}$) [2, 定义 3]处于同时诺特位置。然而，算法 F4T 的复杂度结果需要更强的假设。除前述假设外，还要求序列 hom($\boldsymbol{f}$) 属于 $\mathcal{A}_{\delta,n,n} \cap \mathcal{D}_{\delta,n}$，其中 $\delta \geq 2$且 $n \geq 2$。我们还假设，对于所有 $i \in \{1,\dots,n\}$，序列 ϕ(hom($\boldsymbol{f}$) i) 属于 $\mathcal{S}_{\delta,i,n}$。特别地， ϕ (hom($\boldsymbol{f}$) $n-1$) 属于 $\mathcal{S}_{\delta,n-1,n}$。

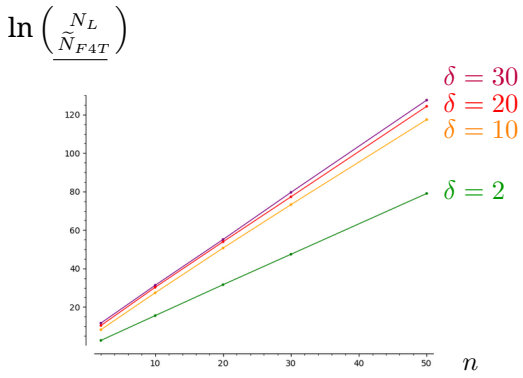

图 2： $\omega = 3$

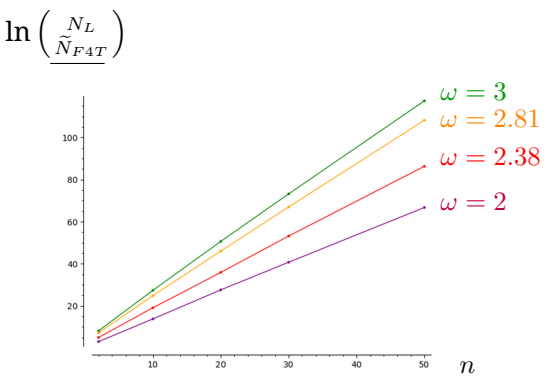

图 3： $\delta = 10$

一个事实是，变量 $x_1, \ldots, x_n$ 相对于序列 $(\mathsf{hom}(f_1) \ldots, \mathsf{hom}(f_n))$ 处于同时诺特位置，这意味着序列 $(\mathsf{hom}(f_1) \ldots, \mathsf{hom}(f_n))$ 是正则的，依据 [2,命题 6]。如 [2,第 3 节2],所述，F5算法的复杂度为

$$N_{F5} = \sum_{i=1}^{n} \sum_{d=\delta}^{\mathbb{D}} b_d^{(i)} \binom{i-1+d}{d} \binom{n+d}{d},$$

使用符号 $b_d^{(i)}$ 引理之前刚刚引入的 6.6。

~图 4和图 5对 N_{F4T}和 N_{F5}进行了与图2和 3对 N_{F4T}和 N_L所做的相同比较。

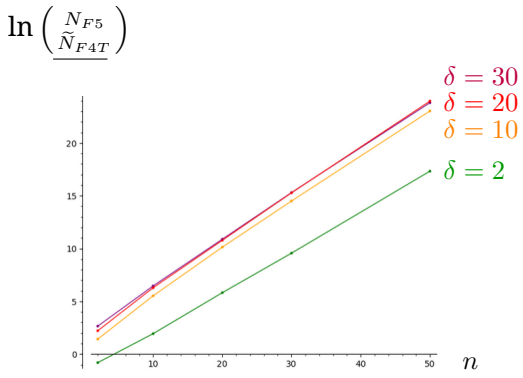

图 4： $\omega = 3$

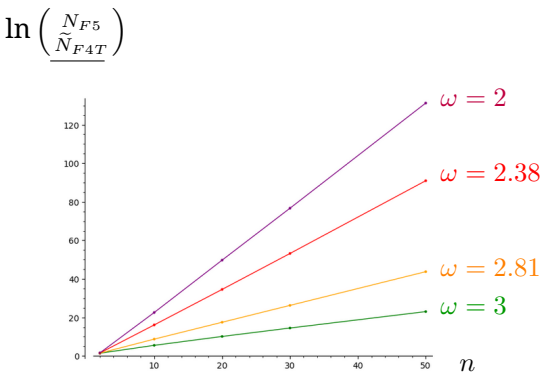

图 5： $\delta = 10$

~将 ω设为 3，图 4展示了由 n带来的 N_{F4T}在不同取值下所提供的指数级增益δ。图 5表明，当将 δ 固定时，这种指数级增益会随着 的减小而 增大 ω 。例如，当 $\omega = 3$ 且 $\delta = 30$ 时，$\ln\left(\frac{N_L}{\widetilde{N}_{F4T}}\right)$ 关于 n 的斜率值约为 0.476。

图 6 概述了上述复杂度陈述，不过这次是表示为理想的次数的幂。表中每个条目所报告的值由 $a = \log_{\delta(N)} n$给出，具体取决于 δ， n 和 ω。

我们观察到，在所有情况下， ω 越小，运算次数的上界就越低。~此外，对于固定的 n、 δ和 ω， N_{F4T} 对应的 a 值总是小于 N_L对应的值。~ N_{F4T}与 N_{F5}之间的比较也同样如此，但 $n = 2$ 和 $\delta = 2$时除外。

对于图 6中的所有列，我们观察到，当 n 增大时， a 也随之增大；对于几乎所有固定的 δ 和 ω值都是如此。然而，当 n 和 ω固定时，随着 δ 增大， a 会减小。不过，它有一个~下界。证明如下。所有复杂度公式 N_{F4T}、 N_L和 N_{F5}都大于 $\binom{n+\mathbb{D}}{\mathbb{D}}$，而后者本身又大于 δ^n。由于

$$\frac{\log_\delta(\delta^n)}{n} = 1,$$

图 6 中报告的每个值都必然大于 1。最后，对于固定的 n 和 δ，随着 ω的减小，该值也会减小。为了更清楚地说明图 6中的数据所显示的提升，我们固定一行。例如，在

	$\widetilde{N}_{F4T}$				N_L				N_{F5}
	$\omega=3$	$\omega=2.81$	$\omega=2.38$	$\omega=2$	$\omega=3$	$\omega=2.81$	$\omega=2.38$	$\omega=2$	
$\delta=2$									
$n=2$	3.58	3.47	3.25	3.08	5.48	5.16	4.45	3.82	3.00
$n=10$	3.62	3.48	3.16	2.90	5.86	5.51	4.71	4.01	3.90
$n=20$	3.63	3.47	3.11	2.80	5.91	5.55	4.73	4.01	4.05
$n=30$	3.65	3.48	3.10	2.77	5.93	5.56	4.74	4.00	4.11
$n=50$	3.67	3.49	3.10	2.76	5.95	5.58	4.74	4.00	4.17
$\delta=10$									
$n=2$	1.85	1.84	1.82	1.81	3.63	3.41	2.91	2.47	2.16
$n=10$	2.89	2.75	2.43	2.15	4.08	3.83	3.26	2.75	3.13
$n=20$	3.05	2.89	2.52	2.19	4.15	3.89	3.30	2.79	3.27
$n=30$	3.11	2.94	2.55	2.21	4.17	3.91	3.32	2.80	3.32
$n=50$	3.17	2.99	2.58	2.23	4.19	3.93	3.33	2.81	3.37
$\delta=20$									
$n=2$	1.74	1.73	1.73	1.72	3.47	3.26	2.78	2.35	2.11
$n=10$	2.84	2.70	2.37	2.09	3.85	3.61	3.07	2.59	3.05
$n=20$	3.00	2.84	2.46	2.13	3.90	3.66	3.11	2.62	3.18
$n=30$	3.06	2.89	2.50	2.15	3.92	3.68	3.12	2.63	3.23
$n=50$	3.11	2.93	2.53	2.17	3.94	3.69	3.13	2.63	3.27
$\delta=30$									
$n=2$	1.70	1.70	1.69	1.69	3.41	3.20	2.73	2.31	2.09
$n=10$	2.83	2.68	2.35	2.07	3.75	3.52	2.99	2.52	3.02
$n=20$	2.99	2.82	2.44	2.11	3.80	3.56	3.02	2.55	3.15
$n=30$	3.04	2.87	2.48	2.13	3.82	3.58	3.04	2.56	3.19
$n=50$	3.09	2.91	2.51	2.15	3.84	3.59	3.05	2.56	3.23
$\delta=50$									
$n=2$	1.66	1.66	1.66	1.66	3.35	3.15	2.68	2.26	2.08
$n=10$	2.81	2.67	2.34	2.05	3.66	3.43	2.91	2.46	2.99
$n=20$	2.97	2.80	2.43	2.09	3.70	3.47	2.94	2.48	3.11
$n=30$	3.03	2.85	2.46	2.11	3.72	3.48	2.95	2.49	3.16
$n=50$	3.07	2.89	2.48	2.12	3.73	3.50	2.96	2.49	3.20

图 6：关于理想次数的复杂度

对应于 $\delta=2$ 和 $n=50$的行中，当 $\omega=3$时， $\widetilde{N}_{F4T}$ 相较于 N_{F5} 的提升为 $\delta^{(4.17-3.67)n}=\delta^{0.50n}$；而当 $\omega=2.38$时，提升为 $\delta^{1.07n}$。

6.5. 一般格罗布纳基的基数

总而言之，输出大小是衡量可达到的复杂度性能的重要指标。假设此前提出的若干猜想成立，我们推导出一般情形下输出大小的一个新上界。令 G 表示由序列 $\boldsymbol{f}$ 生成的理想 I 的约化字典序逆序格罗布纳基，其中 $\mathsf{hom}(\boldsymbol{f})$ 属于 $\mathcal{S}_{\delta,\ n,\ n}$。 G 的大小为

$$\sum_{g\in G} \sharp\left(\mathrm{Supp}(g)\right).$$

由于 G 是约化的，以下性质成立。对于每个多项式 $g\in G$，$\mathrm{Supp}(g)$ 中与 $\mathsf{lm}_{\succ_{\mathrm{grevlex}}}(g)$ 不同的每个单项式都属于 $\mathsf{Mon}_n\setminus \mathsf{lm}_{\succ_{\mathrm{grevlex}}}(I)$。此外，由于 $\mathsf{hom}(\boldsymbol{f})$ 属于 $\mathcal{S}_{\delta,\ n,\ n}$，推论 5.8蕴含

$$\mathsf{Mon}_n\setminus \mathsf{lm}_{\succ_{\mathrm{grevlex}}}(I)=\mathsf{Mon}_n\setminus \mathsf{lm}_{\succ_{\mathrm{grevlex}}}(\langle \mathsf{hom}(\boldsymbol{f})\rangle).$$

利用 [41, 命题 1]，，我们推得 $\langle \mathsf{hom}(\boldsymbol{f})\rangle$ 的希尔伯特级数等于 $\left(\sum_{d=0}^{\delta-1} z^d\right)^n$。由于这也是由$(x_1^\delta$、…、$x_n^\delta)$生成的理想的希尔伯特级数，因此可得

$$\sharp\left(\mathsf{Mon}_n\setminus \mathsf{lm}_{\succ_{\mathrm{grevlex}}}(I)\right)\leq \delta^n.$$

	$n=2$	$n=5$	$n=10$	$n=15$	$n=20$	$n=30$	$n=50$
$\delta=2$	0.79	0.87	0.87	0.88	0.89	0.91	0.94
$\delta=5$	0.55	0.76	0.85	0.89	0.91	0.94	0.96
$\delta=10$	0.52	0.76	0.86	0.90	0.92	0.95	0.96
$\delta=15$	0.51	0.76	0.87	0.90	0.93	0.95	0.96
$\delta=20$	0.50	0.76	0.87	0.91	0.93	0.95	0.96
$\delta=30$	0.50	0.77	0.87	0.91	0.93	0.95	0.97
$\delta=50$	0.50	0.77	0.87	0.91	0.93	0.95	0.97

图 7： G 相对于理想次数的基数

因此，对于任意 $g \in G$，我们有

$$\sharp\left(\mathrm{Supp}(g)\right) \leq \delta^n + 1.$$

我们刚刚证明，输出的大小有上界 $\sharp(G)$ $(\delta^n + 1)$。现在我们着重为 G 的基数给出上界。

我们的目标是应用定理 3.2，这要求 $\mathsf{lm}_{\succ_{\mathrm{grevlex}}}(I)$ 稳定，且 I 为零维。我们回顾一下，I 是零维的，因为它的希尔伯特级数是一个多项式。此外，根据备注 3.9，如果 $\mathsf{hom}(\boldsymbol{f})$ 属于 $\mathcal{A}_{\delta,\ n,\ n}$，那么 $\mathsf{lm}_{\succ_{\mathrm{grevlex}}}(\mathsf{hom}(\boldsymbol{f}))$ 就是稳定的。根据推论 5.8，$\mathsf{lm}_{\succ_{\mathrm{grevlex}}}(I)$ 也满足这一性质。此外，[40, 猜想 4.1] 指出，$\mathcal{A}_{\delta,\ n,\ n}$ 是一个非空的扎里斯基开集。

因此，我们补充以下假设：$\delta \geq 0$，$n \geq 1$，并且 $\mathsf{lm}_{\succ_{\mathrm{grevlex}}}(I)$ 稳定。利用定理 3.2，我们推得：

$$\sharp\left(G\right) = \sum_{i=0}^{n-1} \sharp\left(\mathscr{B}_i(I,\succ)\right) = \sum_{i=0}^{n-1}\sum_{d=0}^{+\infty} \sharp\left(\mathscr{B}_{d,i}(I,\succ)\right) = 1 + \sum_{i=1}^{n-1}\sum_{d=0}^{+\infty} \sharp\left(\mathscr{B}_{d,i}(I,\succ)\right). \qquad (\star)$$

在此阶段，我们考虑一个整数 d 和 i 属于 $\{1,\cdots,n-1\}$，并求得 $\sharp(\mathscr{B}_{d,i}(I,\succ))$ 的一个表达式。利用推论 4.5，我们已经知道

$$\sharp\left(\mathscr{B}_{d,i}(I,\succ)\right) = \sharp\left(\mathscr{B}_{d,i}(\langle\phi(\mathsf{hom}(\boldsymbol{f}),i)\rangle,\succ)\right).$$

假设对于所有 i 属于 $\{1,\ldots,n\}$，序列 $\phi(\mathsf{hom}(\boldsymbol{f})\ i)$ 都属于 $\mathcal{S}_{\delta,\ i,\ n}$，则对于所有 i 属于 $\{1,\ldots,n\}$

$$\sum_{d=0}^{+\infty} \sharp\left(\mathscr{B}_{d,i}(\langle\phi(\mathsf{hom}(\boldsymbol{f}),i)\rangle,\succ)\right) z^d = \sum_{d=0}^{+\infty} \sharp\left(\mathscr{B}_{d,i}(I,\succ)\right) z^d = \left[\frac{(1-z^\delta)^n}{(1-z)^i}\right]_+.$$

将最后这个公式代入$(\star)$后，我们便能计算 $\sharp(G)$，而无需计算 G 本身。回顾一下，对于所有 i 属于 $\{1,\ldots,n-1\}$，$\mathcal{S}_{\delta,\ i,\ n}$ 是非空扎里斯基开集这一事实依赖于 [20, 猜想 1.1]。由此得到以下结果。

定理 6.10。设 $\boldsymbol{f}$ 是一个多项式序列，使得对于所有 i 属于 $\{1,\ldots,n\}$，序列 $\phi(\mathsf{hom}(\boldsymbol{f})\ i)$ 都属于 $\mathcal{S}_{\delta,\ i,\ n}$。假设 $\mathsf{lm}_{\succ_{\mathrm{grevlex}}}(I)$ 是稳定的，并设 G 是 $\langle f\rangle$ 的一个极小反向字典序 *Gröbner* 基。那么我们有

$$\sharp\left(G\right) = 1 + \sum_{i=1}^{n-1}\sum_{d=0}^{+\infty} \beta_{d,i} \quad \textit{with} \quad \left[\frac{(1-z^\delta)^n}{(1-z)^i}\right]_+ = \sum_{d=0}^{+\infty} \beta_{d,i} z^d \quad \textit{for all } i \textit{ in } \{1,\ldots,n-1\}.$$

图 7 展示了数值数据，说明格罗布纳基的基数如何随理想的次数呈幂次增长。表中列索引为 n 且行索引为 δ 的单元格所报告的值等于 $b = \log_\delta(\sharp(G))\ n$。

附录 A.

引理 1. 设 $\boldsymbol{f} = (f_1,\ldots,f_s)$ 是由次数为 δ 的齐次多项式构成的序列，其中这些多项式属于 $\mathcal{R}_n$，并设 $e \in \mathbb{N}$。设 $G = G(I, \succ_{\mathrm{grevlex}})$ 是理想 $I = \langle\boldsymbol{f}\rangle$ 的约化 $\succ_{\mathrm{grevlex}}$-格罗布纳基。我们用 E_e 表示矩阵的行最简阶梯形

$$\mathrm{Mac}(\mathsf{P}_{e,n}(\boldsymbol{f}), \mathsf{Mon}_{e,n}).$$

那么，以下断言成立。

1. 矩阵 E_e 包含所有满足 $\deg(g) = e$ 的 G 中的多项式 g，并将它们作为行。

其证明　引理 *1* 的第 *1* 部分*1.* 设 g 属于 G，且 $\deg(g) = e$。由于 G 是约化的格罗布纳基 of 齐次理想 根据 [8, 第 8 章第 3 节定理 2]，g 是齐次的。

根据引理 2.3，多项式 g 属于由 Macaulay 矩阵 Mac($P_{e,n}$(*f*), $Mon_{e,n}$)的各行生成的 $\mathbb{K}$-向量空间。因此，多项式 g 也属于由该矩阵的行最简阶梯形 E_e的各行生成的 $\mathbb{K}$-向量空间。根据引理 2.3 和注 4.2，E_e 的各行的主元列由所有可能的首项单项式（相对于 $\succ_{\text{grevlex}}$）索引，其次数为 e。因此，E_e 中存在一行表示多项式 f，使得

$$\mathsf{lm}_{\succ_{\text{grevlex}}}(f) = \mathsf{lm}_{\succ_{\text{grevlex}}}(g).$$

由于 f 和 g 都是次数为 e的齐次多项式，因此它们的差 $f - g$ 也是次数为 e 的齐次多项式，或者为零。

由于 E_e 是行最简阶梯形，我们有 $\mathsf{lc}_{\succ_{\text{grevlex}}}(f) = 1$。由于 G 是约化的 $\succ_{\text{grevlex}}$-格罗布纳基，根据约化格罗布纳基的定义，我们也有 $\mathsf{lc}_{\succ_{\text{grevlex}}}(g) = 1$。因此，我们有 $\mathsf{lt}_{\succ_{\text{grevlex}}}(f) = \mathsf{lt}_{\succ_{\text{grevlex}}}(g)$。这意味着 $f - g$的首项单项式不是 $\mathsf{lm}_{\succ_{\text{grevlex}}}(f)$。假设 $f - g$ 不为零，并写作 $m = \mathsf{lm}_{\succ_{\text{grevlex}}}(f - g)$。

假设 m 属于 $\mathsf{Supp}(f) \setminus \mathsf{lm}_{\succ_{\text{grevlex}}}(f)$。那么，由于 E_e 是行最简阶梯形，单项式 m 不对应 E_e的主元列。但由于 $f - g$ 属于 I 且次数为 e，其首项单项式必对应 E_e的主元列。这就产生了矛盾。

假设 m 属于 $\mathsf{Supp}(g) \setminus \mathsf{lm}_{\succ_{\text{grevlex}}}(g)$。根据格罗布纳基的定义，$m$ 不能被 G 中元素的任何首项单项式整除，因此也不能被 I 中元素的任何首项单项式整除。特别地，它不能作为 E_e 的主元列的索引。另一方面，由于 $f - g$ 属于 I 且为次数为 e 的齐次多项式，这与m 必须是 E_e中的主元索引这一事实矛盾。

我们得出 $f - g = 0$，因此 g 作为一行出现在 E_e 中。 □

引理 2。设 h_1、……、h_n 是 $\mathcal{R}_n$ 中满足 $1 \notin \langle h_1$、……、$h_n\rangle$ 的齐次多项式。当且仅当对于所有整数 $i \in \{1, \ldots, n\}$，序列 $\phi((h_1$、……、$h_i)\ i)$ 是正则的，变量x_1、……、x_n 相对于 h_1、……、h_n 处于同时诺特位置。

证明。由 [2, 命题 6] 和 [2, 定义 3], 可知，只需证明对于所有 $i \in \{1, \ldots, n\}$，序列 $(h_1, \ldots, h_i, x_{i+1}, \ldots, x_n)$ 是正则的。令 $i \in \{1, \ldots, n\}$。根据假设，我们知道

$$\begin{aligned} &\phi((h_1, \ldots, h_i), i) \text{ is regular} \\ \iff &(x_{i+1}, \ldots, x_n, h_1, \ldots, h_i) \text{ is regular} \\ \iff &(h_1, \ldots, h_i, x_{i+1}, \ldots, x_n) \text{ is regular,} \end{aligned}$$

由此得证。 □

参考文献

[1] Abramowitz, M., Stegun, I.A., 1992. 数学函数手册：含公式、图表和数学表格。Dover Publication Inc.，纽约，1972年版重印。[2] Bardet, M., Faugère, J.C., Salvy, B., 2015. 关于 F_5 格罗布纳基算法的复杂度。《符号计算杂志》70，49–70。doi：10.1016/j.jsc.2014.09.025。[3] Basu, S., Pollack, R., Roy, M.F., 2006. 实代数几何算法。第10卷，计算与数学算法第2版，柏林：施普林格。doi：10.1007/3-540-33099-2。[4]Berthomieu, J., Eder, C., Safey El Din, M., 2021. msolve：用于求解多项式系统的程序库。2021年国际符号与代数计算研讨会，51–58。doi：10.1145/3452143.3465545。[5] Bosma, W., Cannon, J., Playoust, C., 1997. Magma 代数系统。I. 用户语言。《符号计算杂志》24，235–265。doi：10.1006/jsco.1996.0125。计算代数与数论（伦敦，1993年）。

[6] Buchberger, B., 1965. 一种求出零维多项式理想的剩余类环基元素的算法。博士论文。因斯布鲁克大学。[7] Caminata, A., Gorla, E., 2023. 求解次数、最后下降次数及相关不变量。《符号计算杂志》114，322–335。doi:10.1016/j.jsc.2022.05.001。[8] Cox, D., Little, J., O'Shea, D., 1992.《理想、簇与算法》。数学本科教材，施普林格出版社，纽约。[9] Dubé, T.W., 1990. 多项式理想与格罗布纳基的结构。《SIAM计算杂志》19，750–773。doi:10.1137/0219053。[10] Dumas, J.G., Giorgi, P., Pernet, C., 2004. FFPACK：有限域线性代数软件包，载于：ISSAC 2004。ACM，纽约，第119–126页。doi:10.1145/1005285.1005304。[11] Eder, C., Faugère, J.C., 2017. 计算格罗布纳基的基于签名算法综述。《符号计算杂志》80，719–784。doi:10.1016/j.jsc.2016.07.031。[12] Faugère, J.C., 1999. 一种计算格罗布纳基的新型高效算法（F4）。《纯粹与应用代数杂志》139，61–88。doi:10.1016/S0022-4049(99)00005-5。[13] Faugère, J.C., 2002. 一种无需约化为零即可计算格罗布纳基的新型高效算法（F5）。2002年国际符号与代数计算研讨会27，75–83。[14] Faugère, J.C., Gianni, P., Lazard, D., Mora, T., 1993. 通过序变换高效计算零维格罗布纳基。《符号计算杂志》16，329–344。doi:10.1006/jsco.1993. 1051。[15] Faugère, J.C., Safey El Din, M., Spaenlehauer, P.J., 2010. 利用格罗布纳基计算线性矩阵的秩亏损轨迹及其在密码学中的应用。ISSAC 2010，257–264。doi:10.1145/ 1837934.1837984。[16] Faugère, J.C., Safey El Din, M., Spaenlehauer, P.J., 2011. 由双次数为（1，1）的多项式生成的双齐次理想的格罗布纳基：算法与复杂度。《符号计算杂志》46，406–437。doi:10.1016/j.jsc.2010.10.014。[17] Faugère, J.C., Safey El Din, M., Spaenlehauer, P.J., 2012. 临界点与格罗布纳基：无混合情形。ISSAC 2012，162–169。doi:10.1145/2442829.2442855。[18] Faugère, J.C., Safey El Din, M., Spaenlehauer, P.J., 2013. 关于广义 MinRank 问题的复杂度。《符号计算杂志》55，30–58。doi:10.1016/j.jsc.2013.03.004。[19] Faugère, J.C., Safey El Din, M., Verron, T., 2016. 关于计算带权齐次系统格罗布纳基的复杂度。《符号计算杂志》76，107–141。doi:10.1016/j.jsc.2015. 12.001。[20] Fröberg, R., Hollman, J., 1994. 一般形式生成的理想的希尔伯特级数。《符号计算杂志》17，149–157。doi:10.1006/jsco.1994.1008。[21] von zur Gathen, J., Gerhard, J., 2003.《现代计算机代数》。剑桥大学出版社。[22] Gebauer, R., Möller, H.M., 1988. 关于 Buchberger 算法的一种实现。《符号计算杂志》6，275–286。doi:10.1016/S0747-7171(88)80048-8。[23] Giovini, A., Mora, T., Niesi, G., Robbiano, L., Traverso, C., 1991. "请来一块糖块"，或 Buchberger 算法中的选择策略。ISSAC 1991，49–54。[24] Giusti, M., 1984. 多项式理想理论中的若干有效性问题，载于：《计算机科学讲义》。施普林格，柏林。计算机科学讲义第174卷，第159–171页。doi:10.1007/BFb0032839。[25] Gopalakrishnan, S., 2025. 关于计算互素行列式理想的格罗布纳基的算术复杂度。《代数杂志》668，233–264。doi:10.1016/j.jalgebra.2025.01.014。

[26] Gopalakrishnan, S., Neiger, V., Safey El Din, M., 2024. 极大行列式理想和临界点计算的优化格罗布纳基算法，载于：2024年国际符号与代数计算研讨会论文集，ACM，第400–409页。[27] Gorla, E., Mueller, D., Petit, C., 2022. HFE系统计算格罗布纳基成本的更强上界。《符号计算杂志》109，386–398。doi:10.1016/j.jsc.2020.07.011。[28] Hashemi, A., Lazard, D., 2011. 零维格罗布纳基和多项式系统求解的更精确复杂度界。《国际代数与计算杂志》21，703–713。doi:10.1142/S0218196711006364。[29] Hashemi, A., Seiler, W.M., 2017. 格罗布纳基的依赖维数上界。CoRR abs/1705.02776。arXiv:1705.02776。[30] Herzog, J., Hibi, T., 2011. 单项式理想。数学研究生教材第260卷。施普林格出版社，伦敦有限公司，伦敦。doi:10.1007/978-0-85729-106-6。[31] Hoffman, K., Kunze, R., 1971. 线性代数。第2版，普伦蒂斯·霍尔。[32] Huynh, D.T., 1986. 格罗布纳基与交换 Thue 系统的超指数下界。《信息与控制》68，196–206。doi:https://doi.org/10.1016/S0019-9958(86)80035-3。[33] Lazard, D., 1983. 格罗布纳基、高斯消元与代数方程组求解，载于：计算机代数（伦敦，1983年）。施普林格，柏林。计算机科学讲义第162卷，第146–156页。doi:10.1007/3-540-12868-9_99.[34] Le, H.P., Safey El Din, M., 2022. 通过Hermite矩阵求解实数域上的参数多项式方程组。《符号计算杂志》112，25–61。doi:10.1016/j.jsc.2021.12.002。[35] Macaulay, F.S., 1903. 消元公式。《伦敦数学会会报》35，3–27。doi:10.1112/plms/s1-35.1.3。[36] Maplesoft, 2019. Maple。https://www.maplesoft.com。计算机代数系统。[37] Matsumura, H., 1989. 交换环论。剑桥高等数学研究丛书第8卷。第2版，剑桥大学出版社，剑桥。由 M. Reid 从日文翻译。[38] Mayr, E.W., Meyer, A.R., 1982. 交换半群字问题和多项式理想的复杂度。《数学进展》46，305–329。doi:10.1016/0001-8708(82)90048-2。[39] Möller, H.M., Mora, F., 1984. 格罗布纳基次数的上界和下界，载于：ISSAC/EUROSAM 1984论文集。施普林格，柏林。计算机科学讲义，第172–183页。[40] Moreno-Socías, G., 2003. 一般完全交的反字典序格罗布纳基。《纯粹与应用代数杂志》180，263–283。doi:10.1016/S0022-4049(02)00297-9。[41] Pardue, K., 2010. 一般多项式序列。《代数杂志》324，579–590。doi:10.1016/j.jalgebra.2010.04.018。[42] Pardue, K., Richert, B., 2009. 半正则序列的 Syzygies。《伊利诺伊数学杂志》53，349–364。[43] Storjohann, A., 2000. 矩阵标准形算法。博士论文。瑞士联邦理工学院（苏黎世联邦理工学院）。网址：http://dx.doi.org/10.3929/ethz-a-004141007。[44] Traverso, C., 1989. 格罗布纳迹算法，载于：ISSAC 1988论文集。施普林格，柏林。计算机科学讲义第358卷，第125–138页。doi:10.1007/3-540-51084-2_12。