arXiv:2302.05813v2 [cs.SC] 7 Dec 2023

Lazard 风格柱面代数分解与等式约束

James H. Davenport
巴斯大学 英国
m
asjhd@bath.ac.uk

Akshar Nair
巴斯大学 英国
aks
har.nair@gmail.com

Gregory Sankaran
大学 o f Bath
英国
g.k.sankaran@bath.ac.uk

Ali K. Uncu
RICAM、奥地利科学院与巴斯大学
奥地利与英国
akuncu@ricam.oeaw.ac.at

摘要

McCallum 风格柱面代数分解（柱状代数分解）是对 Collins 原始版本的一项重大改进，此后也取得了许多进展，尤其是在处理完全或部分等式约束方面。但它存在零化问题。最近得到理论论证的 Lazard 风格柱面代数分解不存在这一问题。然而，将等式约束方面的研究成果移植到 Lazard 风格中，确实会重新引入零化问题。本文基于第二作者的博士论文以及 Brown–McCallum 对 Lazard 方法的改进，阐释了这一问题及其解决方案。

采用单个等式约束时，我们在 Lazard 风格的柱状代数分解中也能获得与 McCallum 风格相同的改进。此外，我们的方法不会像 McCallum 的方法那样因零化而失效。不出所料，在发生零化的情况下，它无法达到与未发生零化时相同程度的改进。我们还考虑了多个等式约束的情况。

CCS 概念

• **计算方法 → 符号与代数运算**。

关键词

柱面代数分解、Lazard 投影与提升、等式约束

ACM 参考格式：
James Davenport、Akshar Nair、Gregory Sankaran 和 Ali K. Uncu。2023年。Lazard 风格柱状代数分解与等式约束。载于 *2023*年国际符号与代数计算研讨会（*ISSAC 2023*），*2023*年*7*月*24*日至*27*日，挪威特罗姆瑟。ACM，纽约，NY，美国，9 页。 https://doi.org/10.1145/ 3597066.3597090

我们感谢英国研究与创新署工程与物理科学研究委员会一直以来的支持。第二作者的论文研究得到 EPSRC 项目资助 EP/N509589/1 的支持。第一作者和最后一位作者获得了 EPSRC 项目资助 EP/T015713/1 的部分支持。最后一位作者还感谢奥地利科学基金 FWF 项目资助 P34501-N 提供的部分支持。我们感谢 Chris Brown 对 [4]所作的解释。

允许免费为个人或课堂使用而制作本作品全部或部分内容的数字副本或纸质副本，但不得为营利或商业利益而制作或分发副本，且副本首页必须附有本声明和完整引文。本作品中第三方组件的版权必须得到尊重。其他用途请联系所有者/作者。*ISSAC 2023*，*2023*年*7*月*24*日至*27*日，挪威特罗姆瑟 ©2023年版权归所有者/作者所有。ACM ISBN 979-8-4007-0039-2/23/07。
https://doi.org/10.1145/3597066.3597090

1 引言

柱面代数分解 (柱状代数分解，CAD)由 Collins 于 1975 [6]提出。此后出现了许多改进 [6]，其中 [14] 引入了投影-提升范式。McCallum [14],提出了一项重大改进，但其缺点是，当某个多项式被消去为零时，该方法便无法应用。此后，这一领域取得了许多进展，通常涉及等式约束，即半代数集位于一个真子簇中的情形。 [18] 为 Lazard 在 [13],提出的想法提供了理论依据：采用不同形式的投影与提升来避免消去为零的问题。本文旨在将这些改进引入 [14] Lazard 框架。具体而言，我们以 Brown–McCallum [4] 版本的 Lazard方法为基础。

先前的论文 [20, 21]基于 [18]。第二作者的论文 [19] 主要基于 [18], , 并针对 [4]作了一些更新。本文将 [4] 贯穿全文。

2 背景与记号

2.1 通过投影-提升进行柱状代数分解

计算柱面代数分解有多种方法，例如通过三角分解 [5], , 但本文是在 Collins 引入的投影-提升范式 [6]的背景下展开的：见图 1。设 $S \subset \mathbb{Z}[x_1, \ldots, x_n]$ 为感兴趣的多项式集合， $\phi(S)$ 为我们希望分解满足的性质。一般而言， $\phi(S)$ 将是“每个单元对 S 中的多项式均符号不变”这一性质的某种变体，因为正是这一性质使量词消去成为可能，而这也是 Collins 最初的动机。

$$
\begin{array}{llll}
\mathbb{R}^n & S & D_n & \phi_X(S) \\
 & \downarrow P_X & \uparrow L_X & \\
\mathbb{R}^{n-1} & P_X(S) & D_{n-1} & \phi_X(P_X(S)) \\
 & \downarrow P_X & \uparrow L_X & \\
\vdots & \vdots & \vdots & \vdots \\
\mathbb{R}^2 & P_X^{n-2}(S) & D_2 & \phi_X(P_X^{n-2}(S)) \\
 & \downarrow P_X & \uparrow L_X & \\
\mathbb{R}^1 & P_X^{n-1}(S) \quad \rightarrow \text{隔离根} \rightarrow & D_1 & \phi_X(P_X^{n-1}(S))
\end{array}
$$

其中， X 表示投影/提升的具体变体，而 D_i 是 $\mathbb{R}^i$ 的中间分解。

图 1：投影/提升范式

最初的柱面代数分解 Collins 算法 [6] 采用了代价高昂（与其后继算法相比）的投影算子 P_C，且 ϕ_C确实是符号不变性。提升操作 L_C很简单：在每个单元 $C \in D_i$ 上方都有一个柱体$C \times \mathbb{R} \subset \mathbb{R}^{i+1}$，它被 $p_k = 0$ 中多项式的实分支切分为 $p_k \in P^{n-i-1}(S)$，而 P_C 确保这些分支在 C上可描绘，即它们互不相交，并且在整个 C上方都是简单曲面。 D_{i+1} 中的相关单元分别是每个分支（称为“截面”），以及相邻分支之间的“扇区”，包括“所有截面”扇区和“所有截面 $< x_{i+1} < \infty$”扇区。

2.2 帘

当某些多项式恒等于零，也就是说，在 $\mathbb{R}^k = x_1, \ldots\ldots, x_k$ 的某个子集上消失时，Collins 算法的大多数改进都可能遇到困难。 [20] 首次引入了“幕”这一术语，用来指称多项式恒等于零时对应的代数簇：

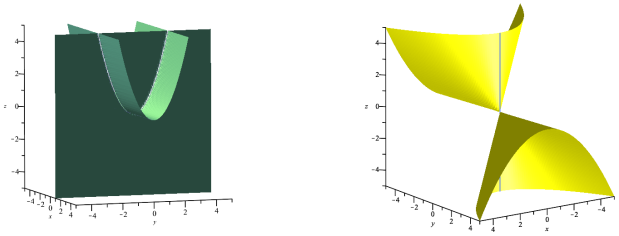
定义 1 ([19, 定义 43]). 若代数簇 $C \subseteq \mathbb{R}^n$ 满足：只要 $(x, x_n) \in C$，则对所有 $y \in \mathbb{R}$，都有 $(x, y) \in C$，则称其为幕。C 若是 $\mathbb{R}^n \to \mathbb{R}^{n-1}$ 的纤维之并，则称其为幕。

定义 2（[19, 定义 44]）。设 $f \in \mathbb{R}[x_1, \ldots, x_n]$ 且 $S \subseteq \mathbb{R}^{n-1}$。如果对于所有（$\alpha_1, \ldots, \alpha_{n-1}$）$\in S$，$y \in \mathbb{R}$ 都有 f（$\alpha_1, \ldots, \alpha_{n-1}, y$）$= 0$，则称 V_f（或 f）在 S处有一个幕。我们称 S为该幕的基底。如果基底 S是单点集，则称该幕为点帷幕。

定义 3（参见 [19, 定义 45]）。设多项式 $f \in \mathbb{R}[x_1, \ldots, x_n]$ 可因式分解为 $f = gh$，其中 $g \in \mathbb{R}[x_1, \ldots, x_{n-1}]$ 且 g（$\alpha_1, \ldots, \alpha_{n-1}$）$= 0$。那么，$f$的簇称为包含一个显式帷幕，其基底为 g的零点集。若一个帘不（按集合意义）包含显式帷幕，则称其为隐式帷幕；若一个帘包含显式帷幕，但其本身不是显式帷幕（因为 h 本身有幕），则称其为混合帷幕。

例1（幕的类型）。

- 显式帷幕：$f(x, y, z) = xy^2 - y^2 - xz + z = (x-1)(y^2-z)$，帷幕位于 $(1, 0)$。在图2a中可以看到该帷幕，它是由 $x = 1$ 给出的平面。
- 隐式幕：$f(x, y, z) = x^2 + yz$，帷幕位于 $(0, y, 0)$。图2b中的蓝线表示该帷幕。



(a) 带有显式帷幕的曲面帷幕　(b) 带有隐式幕的曲面幕

图2：不同类型的帘

2.3 McCallum 对 Collins 方法的改进

定义 4（[14, 第 46]）。设 A是 $\mathbb{Z}[x_1, \ldots, x_n]$中的一组多项式，cont($A$) 表示 A 中各元素关于 x_n的内容，B是 A的一个无平方因子基[1]。设 coeff(B) 表示 B 中各成员的所有系数的集合（将其视为关于 x_n的多项式），disc(B) 表示 B 中各元素的判别式集合（关于 x_n），而 res(B) 表示 B中元素对关于 x_n 的所有结式的集合。*McCallum* 投影算子 P_M 定义为

$$P_M(A) := \text{cont}(A) \cup \text{coeff}(B) \cup \text{disc}(B) \cup \text{res}(B). \quad (1)$$

根据这个定义，McCallum [14] 对 Collins 最初的方法 [6]作了改进。投影 P_M明显小于 P_C，相应的性质 ϕ_M是阶不变性，即如果一个多项式在单元 $C \in D_i$上为零，那么它在该单元上为零的阶数恒定。相应的提升算子 L_M与 L_C完全相同，唯一的区别是：如果一个多项式 q 在零维单元上为零，就用相应的刻画多项式 [15, 定义 1]替代。然而，如果相关多项式在正维 $\mathbb{R}^k$ 单元上恒等于零，L_M可能会失败（给出错误消息，但不会产生错误结果）。

2.4 Brown 对 McCallum 方法的改进

Brown [3] 对 [14]提出了一项有用的改进。

定义 5. 我们使用与定义4相同的记号，并用 lc 表示首项系数。*Brown* 的投影定义如下

$$P_B(A) := \text{cont}(A) \cup \text{lc}(B) \cup \text{disc}(B) \cup \text{res}(B). \quad (2)$$

相应的提升 L_B 相较于 L_M 有若干（必要的）改进，但具体细节在此大多无关紧要：相关的改进是，在我们正在构造的柱状代数分解上方，加入那些会使某个投影因子归零的点（如果它在正维集合上归零，那么该系统就不是良定向的）。对于任意非平凡的多项式集合 A，P_B（A）$\subsetneq P_M$（A），区别在于 B的非首项系数。这不会影响 O 阶渐近，因为其主要由 res(B) 项决定，但在实践中非常有效。 [3, 表 1,2] 考虑了一个含六个变量的例子 A，其中 $|P_B^4$（A）$| = 18$，而 $|P_M^4$（A）$| = 129$。$|P_B^5$（A）$| = 141$，而 P_M^5（A）无法计算，但很可能 $|P_M^5$（A）$| > 8000$。

2.5 字典序最小赋值与 Lazard 提升

Lazard [13]引入了一种柱状代数分解的新方法，以避开零化问题，后来由 [18]使其得到严格论证。本节包含相关定义，均采用 [19, 22] 中的用法。

定义 6。令 $v, w \in \mathbb{Z}^n$。我们称 $v = (v_1, \ldots\ldots, v_n) \geq_{lex} (w_1, \ldots\ldots, w_n) = w$，当且仅当 $v = w$，或者存在一个 $i \leq n$，使得 $v_i > w_i$，并且对于范围 $1 \leq k < i$内的所有 k，都有 $v_k = w_k$。

定义 7（[18, 定义 2。4]）。令 $n \geq 1$，并假设 $f \in \mathbb{R}[x_1, \ldots, x_n]$ 非零且为 $\alpha = (\alpha_1, \ldots\ldots, \alpha_n) \in \mathbb{R}^n$。在 α处的字典序最小赋值 $v_\alpha(f)$是满足以下条件的元素 $v = (v_1, \ldots\ldots, v_n) \in \mathbb{N}^n$ 中关于 $\geq_{lex}$最小者：f围绕 α 展开后含有项

$$c(x_1 - \alpha_1)^{v_1} \cdots (x_n - \alpha_n)^{v_n},$$

其中 $c \neq 0$。

[1] [14] 采用最精细的无平方因子基，但这是出于效率方面的考虑。

注意，$v_\alpha(f) = (0, \ldots, 0)$ 当且仅当 $f(\alpha) \neq 0$。需要注意的是，我们使用的术语与之前的术语略有不同。例如，在 [18]中，字典序最小赋值被称为 Lazard 赋值。我们这样做是为了确保表述准确。

f在 $\alpha \in \mathbb{R}^n$ 处的字典序最小赋值，计算方法是先选定变量 $x_1 \prec x_2 \prec \cdots \prec x_n$的一个序，然后按给定的变量顺序依次代入 α_i。（投影的顺序是先从 x_n开始，赋值计算的顺序是先从 x_1开始。）在每一步依次代入$f(\alpha_1, \ldots, \alpha_{i-1}, x_i, \ldots, x_n)$时，我们确定满足以下条件的最大正整数$v_i$

$$(x_i - \alpha_i)^{v_i} \mid f(\alpha_1, \ldots, \alpha_{i-1}, x_i, \ldots, x_n).$$

v_i是 f在 α处的字典序最小赋值中对应于 α_i的分量。我们继续进行赋值计算，首先将 $f(\alpha_1, \ldots, \alpha_{i-1}, x_i, \ldots, x_n)$替换为 $f(\alpha_1, \ldots, \alpha_{i-1}, x_i, \ldots, x_n) \times (x - \alpha_i)^{-v_i}$，然后在这个新函数中代入 α_i。

例 2. 若 $n = 1$ *and* $f(x_1) = x_1^3 - 2x_1^2 + x_1 = x_1(x_1 - 1)2$，则对所有 $x \neq 0, 1$，有 $v_0(f) = 1$、$v_1(f) = 2$ 和 $v_x(f) = 0$。类似地，若$n = 2$ (采用标准序 $x_1 \prec x_2$) 且 $f(x_1, x_2) = x_1(x_2 - 1)2$，则 $v(0,0)(f) = (1, 0)$、$v(2,1)(f) = (0, 2)$、$v(0,1)(f) = (1, 2)$，其他情况下为 $(0, 0)$。

如下例所示，字典序最小赋值在很大程度上取决于变量的序。

例 3. 设 $f(x, y, z, w) = x^2 + y^2 z - 2yz^2 + zw$, $\alpha_1 = (0, 1, 0, 1)$，且 $\alpha_2 = (0, 0, 1, 0)$。对于序 $x \prec y \prec z \prec w$，有 $v_{\alpha_1}(f) = (0, 0, 1, 0)$，且 $v_{\alpha_2}(f) = (0, 0, 0, 1)$。对于序 $x \prec z \prec y \prec w$，有 $v_{\alpha_1}(f) = (0, 1, 0, 0)$，且 $v_{\alpha_2}(f) = (0, 0, 0, 1)$。

请注意，在 α_2 的情形下，变量排序不会改变赋值，这与 α_1 的情形不同。比较点的赋值时，变量排序至关重要，必须固定。

命题 1（[18, 命题 3。1]）。 v_α是一个赋值：也就是说，如果 f 和 g 是 $\mathbb{R}[x_1, \ldots, x_n]$ 和 $\alpha \in \mathbb{R}^n$ 中的非零元素，那么

$$v_\alpha(fg) = v_\alpha(f) + v_\alpha(g) \text{ and } v_\alpha(f + g) \geq_{lex} \min\{v_\alpha(f), v_\alpha(g)\}.$$

定义 8（根据 [18, 定义 2。6]）。令 $n \geq 2$，并假设 $f \in \mathbb{R}[x_1, \ldots, x_n]$ 非零且 $\beta \in \mathbb{R}^{n-1}$。$f$ 在/高于 β、$v_\nu\beta(f) = (v_1, \ldots, v_{n-1})$ 的字典序最小半赋值，定义为由 f 在 β 处的赋值结果构成的 $n-1$ 个非负整数向量，并将其视为 $K[x_1, \ldots, x_{n-1}]$ 中的一个元素，其中 $K = \mathbb{R}[x_n]$。因此 $f = f_\beta (x_1 - \beta_1)^{v_1} \cdots (x_{n-1} - \beta_{n-1})^{v_{n-1}}$，我们称 f_β 为 f 的 *Lazard* 余式。

f的字典序最小半赋值称为 f在 β上方的 *Lazard* 评价，记作 $v\beta(f) \ni \mathbb{N}^{n-1}$，其中 [18]。Lazard 余式 $f_\beta \in \mathbb{R}[x_n]$ 称为 f在 β处、[18]中的 *Lazard* 评价。

请注意，[18] 用 v表示两个函数。当 v作为在某处的赋值使用时，它被视为一个从 $\mathbb{R}^n \times \mathbb{R}[x_1, \ldots, x_n] \to \mathbb{N}^n$出发的函数。当 v 作为定义在某处之上或之处的~~赋值使用~~时，它被视为一个从 $\mathbb{R}^{n-1} \times \mathbb{R}[x_1, \ldots, x_n] \to \mathbb{N}^{n-1}$出发的函数。我们认为有必要将这两个函数区分开来。旧记法在阅读 $v_\alpha(f)$时也可能造成混淆。读者需要判断是 $\alpha \in \mathbb{R}^n$ 还是 $\alpha \in \mathbb{R}^{n-1}$，或者判断 $v_\alpha(f) \in \mathbb{N}^n$ 还是$v_\alpha(f) \in \mathbb{N}^{n-1}$。

f 在 $\beta \in \mathbb{R}^{n-1}$ 上的字典序最小半赋值，不应与在 $\alpha \in \mathbb{R}^n$处的字典序最小赋值混淆；后者定义于定义7中。请注意，如果 $b = (\beta, b_n) \in \mathbb{R}^n$，那么对于某个整数 v_n，有 $v_b(f) = (v\beta(f), v_n)$：换言之，$v\beta(f)$由 f在 β之上任意一点处的赋值的前 $n-1$ 个坐标组成。

字典序最小半赋值和 Lazard 余式也依赖于变量的排序，以下例子对此进行了说明。

例 4. 设 $f(x, y, z, w) = x^2 + y^2 z - 2yz^2 + zw$且 $\beta = (0, 1, 0)$，变量排序为 $x \prec y \prec z \prec w$，则 $v'\beta(f) = (0, 0, 1)$ 且 $f_\beta = w + 1$。若将变量排序改为 $x \prec y \prec w \prec z$，则 $v'\beta(f) = (0, 0, 0)$ 且 $f_\beta = z - 2z^2$。

2.6 Lazard 投影与 Lazard 提升

Lazard 的想法是将图 1 中的内容具体化为字典序最小不变性。通过“Lazard 提升”绕过了等式约束的零化问题：当多项式在单元上零化时，其字典序最小赋值在（样本点处的）相应变量上非零，并且在整个单元上都非零。由于该赋值属于相应多项式集的字典序最小不变柱面代数分解，因此它在该单元上也是常量。提升时，如果该赋值为相应的元组，我们就用相应的商替换多项式（这类似于 Collins 的符号不变 CAD 提升）。

要使这一方法奏效，我们需要一个合适的投影算子。其定义如下。

定义 9（[18, 定义 2。1]）。设 A 是 $\mathbb{Z}[x_1, \ldots, x_k]$ 中不可约多项式的集合。*Lazard* 投影 $P_L(A)$ 是 $\mathbb{Z}[x_1, \ldots, x_{k-1}]$ 中以下多项式集合的并集。

（1）A 中各元素的所有首项系数。（2）A 中各元素的所有末项系数。（3）A 中各元素的所有判别式。（4）A 中任意两个不同元素的所有结式。

$$P_L(A) := \mathrm{lc}(A) \cup \mathrm{tc}(A) \cup \mathrm{disc}(A) \cup \mathrm{res}(A). \tag{3}$$

虽然 [18], 中没有明确提及，但多项式的任何内容（关于 x_k）也会传递到 $P_L(A)$ 中。我们还注意到，$P_L \subsetneq P_M$ 作为中间系数，不会出现在 P_L 中。

正如可描绘性是 L_C（以及 L_M）的关键，我们在此情形下也需要一个相应的定义。

定义 10（[18, 定义 2。10]）。设 f 是 $\mathbb{Z}[x_1, \ldots, x_n]$ 中的非零元素，且 S 是 $\mathbb{R}^{n-1}$ 的子集。若 f 在 S 上 *Lazard* 可描绘，则称

(1) 对每个点 $\alpha \in S$，f 在 α 上的字典序最小赋值都相同；
(2) 存在有限个连续函数 $\theta_1 \prec \cdots \prec \theta_k$，从 S 映射到 $\mathbb{R}$，且满足 $k \geq 0$，使得对于所有 $\alpha \in S$，$f_\alpha(x_n)$ 的实根集合为 $\{\theta_1(\alpha) \ldots, \theta_k(\alpha)\}$（当 $k = 0$ 时为空）；*(3)* 若 $k > 0$，则存在正整数 $m_1, \ldots m_k$，使得对于所有 $\alpha \in S$ 和所有 i，m_i 是 $\theta_i(\alpha)$ 作为 $f_\alpha(x_n)$ 的根的重数。

如果字典序最小赋值为零，这与普通可 delineability 相同；否则，这是字典序最小剩余 f_α 的可划分性。

[2] [18,备注 2.2]注意，我们也可以针对无平方因子基来定义这一概念。

2.7 Brown–McCallum 改进

Brown–McCallum CAD 正确性证明中关于截面可划分性的一项关键结果如下。

定理 2.1 [4, 3]。$f \in \mathbb{R}[x_1, \ldots, x_n]$（定理）。假设 $(, \ldots,)$ 在 中具有正次数，且 $disc()$ 和 $lc_{x_n}(f)$ 非零（作为 $\mathbb{R}[x_1, \ldots, x_{n-1}]$ 的元素）。设 S 是 $\mathbb{R}^{n-1}$ 的一个连通解析子流形，其中 $disc_{x_n}(f)$ 和 $lc_{x_n}(f)$ 字典序最小不变，并且 f 在其中任一点都不恒等于零。那么 f 在 S 上解析可描绘，因此 f 在 S 上的每个 *Lazard* 截面和扇区中都是字典序最小不变。

这比 [18,定理 5.1] 对 Lazard CAD 的要求更宽松；在 Lazard CAD 中，可划分性还要求末项系数和结式均不为零。反过来，我们增加了限制“其上不存在任何使 f 恒等于零的点”，这实质上是引入了幕的概念。

对于任意非平凡的多项式集合 A P_B（A） $\subseteq P_L$（A），两者的区别在于末项系数：它们出现在 P_L 中，却不出现在 P_B 中。我们能否将它们去掉？同样，这不会影响渐近复杂度，但在实践中或许有用。末项系数有两个作用：

(1) 识别幕；
(2) 确保幕内按字典序最小不变区域构成堆叠。

如果幕的底部是孤立点，那么理由2 就无关紧要，而假设1 则提供了识别幕的另一种方法。

在 [18, 第 64], 页中提到，如果 lc(p) 处处不为零，那么就不需要 tc(p)。 [4] 中的论证指出，如果 lc(p) 仅在有限多个点处为零，那么就不需要 tc(p)。不过，这一论证和投影过程更为复杂。

假设 1（Brown–McCallum [4]）。有一种实用且高效的测试T，给定 $f \in \mathbb{Z}[x_1, \ldots, x_m]$ 后，它会返回 $\mathbb{R}^{m-1}$ 中的一个有限点集 N，或 $\perp$。如果返回的是 N，那么 N 包含所有使 $f(\alpha_1, \alpha_2, \ldots, \alpha_{m-1}, x_m)$ 恒等于零的点$(\alpha_1, \alpha_2, \ldots \alpha_{m-1})$。

满足该假设的一种方法是针对 $f = \sum a_i(x_1, \ldots, x_{m-1})x_m^i$ 的系数 a_i，计算 $\mathbb{R}^{m-1}$ 的柱状代数分解。这并不像看起来那么昂贵，因为它只涉及 a_i，与原问题中的其他所有多项式无关。与 [23], 中一样，作者实际上会从 a_i 的格罗布纳基开始；如果它是零维的（在 $\mathbb{C}^{m-1}$ 中），那么 N 肯定是有限的。

改进的 Lazard 投影在 [4], 中引入，记为 P_{BM}；它除了接收一个由 m 变量构成的多项式集外，还接收 $\mathbb{R}^m$ 中的一个点集 γ_m，并返回一个由 $m-1$ 变量构成的多项式集以及 $\mathbb{R}^{m-1}$中的一个点集 γ_{m-1}。

定义 11（[4, 定义 4]）。设 A 是 $\mathbb{Z}[x_1, \ldots, x_k]$中的不可约多项式[2]的集合， Γ 是 $\mathbb{R}^k$ 中的有限集，其中包含使 A中的元素发生零化的点。改进的 *Lazard* 投影 P_{BM}（A）的多项式部分，是这些 $\mathbb{Z}[x_1, \ldots, x_{k-1}]$中的多项式集的并集。

(1) A中各元素的所有首项系数。(2) A 中那些经T 返回 $\perp$的元素的末项系数。(3) A中各元素的所有判别式。

(4) A中任意两个不同元素的所有结式。

“点”部分是先前确定的点与T确定的点的投影。

$$P_{BM}(A, \Gamma)_{poly} := \mathrm{lc}(A) \cup \bigcup_{\mathbf{T}(f)=\perp} \mathrm{tc}(f) \cup \mathrm{disc}(A) \cup \mathrm{res}(A), \quad (4)$$

$$P_{BM}(A, \Gamma)_{points} := \{(\gamma_1, \ldots, \gamma_{k-1}) | (\gamma_1, \ldots, \gamma_k) \in \Gamma\} \cup \bigcup_{\mathbf{T}(f)\neq\perp} \{\mathbf{T}(f) | f \in A\}. \quad (5)$$

尽管在 *[4],* 中没有明确说明，多项式的任何内容（相对于 x_k）也会延续到 P_{BM}（A, Γ）中。

L_{BM} 由……修改而来 L_L（Lazard 提升），类比于……所作的修改 L_B将……加入 L_M：在每个阶段，我们都向柱状代数分解中加入D_k中的点 Γ_k。这是可行的，因为根据（5）的第一部分，这些点的投影已经是 D_{k-1}中的点胞腔。

3 一个单独的等式约束

定义 12（[12, 定义 2]）。等式约束（*EC*）是一个由无量词公式 Φ 逻辑蕴含的多项式方程。如果它是该公式的一个原子公式，则称其为显式；否则称其为隐式。如果从公式中可以明显看出该约束是一个等式，即公式 Φ *is* $(f = 0) \wedge \Phi'$，则称该约束在语法上是显式的。

Φ 可能有多个等式约束，但在本节中，我们选定其中一个作为所选等式约束。

3.1 McCallum 的柱状代数分解

在 [16], McCallum 中，受 [7], 启发，他将 [14] 的方法改造为：把 $\mathbb{R}^{n-1}$ 的序不变柱面代数分解提升为一个符号不变柱面代数分解，但分解的对象不是 $\mathbb{R}^n$，而是一个关于 x_n 中正次数本原 [3] 多项式 $f \in \mathbb{Z}[x_1, \ldots, x_n]$ 的簇 V_f。这种方法继承了 [14], 的空化问题，但当多项式问题的形式为 $f = 0 \wedge \Phi$ 时很有用，即存在一个等式约束（另见 [12]）。从 $\mathbb{R}^n$ 到 $\mathbb{R}^{n-1}$ 的投影算子要小得多：若 E 是 f 的一个不可约基，那么

$$P_M^E(A) = P_M(E) \cup \{\mathrm{res}_{x_n}(f, g) : f \in E, g \in A \setminus E\}. \quad (6)$$

将此与原来的 $P_M(A)$（见（1））比较可知，我们无需计算 $\mathrm{disc}(A \setminus E)$ 或 $\mathrm{res}(A \setminus E)$，这降低了渐近复杂度——关于多项式数量的双重指数从 n 降至 $n-1$ [12]。

3.2 字典序最小情形

一个显而易见的问题是，我们能否对 Brown– McCallum 投影[4]做同样的处理。令 E为等式约束的不可约因子集合。与（6）中一样，我们可以定义一个新的投影算子，将 $\mathbb{R}^n$映射到 $\mathbb{R}^{n-1}$。

定义 13. 设 E 是所选等式约束 f 的一个不可约基。定义修正后的 *Brown–McCallum* 投影

[3]如果 f相对于 x_n不是本原的，那么当内容为零时，我们对 x_n没有任何约束。有关内容的更多信息，请参见 [8]。[4]本节基于 [19, 第 4], 章，该章使用的是 Lazard 投影。

P^E_{BM} *by*

$$P^E_{BM}(A,\Gamma)_{poly} := P_{BM}(E,\Gamma)_{poly} \cup \{\mathrm{res}(f,g) : f \in E, g \in A \setminus E\}. \tag{7}$$

$$P^E_{BM}(A,\Gamma)_{points} := P_{BM}(E,\Gamma)_{points}. \tag{8}$$

注意，除了不单独从 $A \setminus E$ 计算任何投影多项式外，我们也只关注来自 E 的点帘的底足，而非来自整个 A 的底足。

下述定理是 [16, 定理 2。2], 的字典序最小等价形式，证明见 [19]。

定理 3 1 [19, 18] $n \geq 2$ f $g \in$。$\mathbb{R}[x_1,\ldots,x_n]$ x_n S（定理）。设 且，在主变量 中次数为正。设 为 $\mathbb{R}^{n-1}$ 的一个连通子集。假设 f 在 S 上是 *Lazard* 可描绘的，$\mathrm{res}_{x_n}(f,g)$ 在 S 上字典序最小不变，且 V_f 在 S 上没有幕。那么， g 在 f 的每个 *Lazard* 截面上、位于 S 上方时，都是符号不变的。

定理 3.2（参见 [19, 定理 25]）。设 $A = \{f_1, \ldots, f_m\}$ 是关于 n 个变量 $x_1, ..., x_n$ 的两两互素的不可约多项式集合，且它们关于 x_n 的次数为正，其中 $n \geq 2$。设 Γ 是 $\mathbb{R}^n$ 中的一个有限点集。令 S 为通过 *Brown–McCallum* 算法得到的 $\mathbb{R}^{n-1}$ 的子集，因此 $P^E_{BM}(A,\Gamma)_{poly}$ 的每个元素在 S 上都是字典序最小不变的。那么， A 的每个元素在其他每个元素的 *Lazard* 截面和扇区上都是字典序最小不变的。

证明。设 $f = f_1 \ldots f_m$。那么 f 的首项系数非零，因此在 S 中是字典序最小不变的。我们知道，$\mathrm{disc}_{x_n}(f)$ 可展开如下：

$$\mathrm{disc}_{x_n}(f_1 \ldots f_m) = \Big(\prod_{i=1}^{m} \mathrm{disc}_{x_n}(f_i)\Big)\Big(\prod_{1\leq i<j\leq m} \mathrm{res}_{x_n}(f_i,f_j)\Big). \tag{9}$$

如果（9）右侧的所有内容在 S 中都是字典序最小不变的，那么 $\mathrm{disc}_{x_n}(f)$ 就是字典序最小不变的。因此，根据定理 2.1， f 在 S 上是 Lazard 可描绘的。由于对所有 $\mathrm{res}_{x_n}(f_i,f_j)$ 而言， $1 \leq i < j \leq m$ 在 S 中都是字典序最小不变的，任意两个 f_i 和 $f_j (i \neq j)$ 的 Lazard 截面要么互不相交，要么相同。因此， A 的每个元素在其他每个元素的 Lazard 截面上都是字典序最小不变的。□

定理 3.3 ([19, 定理 26])。设 A 是关于 n 个变量 $x_1, ..., x_n$ 的一组两两互素的不可约多项式，这些多项式在 x_n 中具有正次数，其中 $n \geq 2$。设 E 是 A 的一个子集，且 Γ 是 $\mathbb{R}^n$ 中由有限个点构成的集合。设 S 是 $\mathbb{R}^{n-1}$ 的一个连通子集。假设 $P^E_{BM}(A,\Gamma)_{poly}$ 的每个元素在 S 中都是字典序最小不变的。那么， E 的每个元素在 S 上都是 *Lazard* 可描绘的，并且以下情况恰有一种成立。

(1) 由 E 中各元素的乘积定义的超曲面 V_E 在 S 上有一幅幕。
(2) E 中各元素在 S 上的 *Lazard* 截面两两不相交。 E 中的每个元素在每个这样的 *Lazard* 截面上都是字典序最小不变的。 $A \setminus E$ 中的每个元素在每个这样的 *Lazard* 截面上都是符号不变的。

因此，在 E的帘之外，来自 $\mathbb{R}^{n-1}$ 针对 $P^E_{BM}(A,\Gamma)$ 的字典序最小不变分解的提升单元，构成了 V_E 关于 A的符号不变分解。

证明。 如果不存在点 S 使得 E 被零化，那么定理 2.1 表明，E 中的每个元素都是 Lazard 可描绘的

因为 $P_{BM}(E,\Gamma)_{poly} \subseteq P^E_{BM}(A,\Gamma)_{poly}$。否则， V_E 在 S 上有一个幕，而 E 中不含幕的元素的 Lazard 截面两两不相交。现在令 $f \in E$（使得 f在 S上方没有幕），令 σ为 f在 S上方的一个截面，并令 $g \in A$。如果 $g \in E$，那么根据定理 2.1， g在 f的每个截面和扇区中都是字典序最小不变的。如果 $g \notin E$，那么， $R = \mathrm{res}(f,g) \in P^E_{BM}(A,\Gamma)_{poly}$，并且根据假设， R 在 S 中是字典序最小不变的。于是根据定理 3.1， g在 σ中符号不变。□

下一节将讨论 E 的帘上会发生什么。

4 帘与单个等式约束

McCallum 将 [16] 中的阶不变性提升为符号不变性，并将 [17], 中的阶不变性提升为符号不变性，但前提是输入多项式没有任何帘。由于帘本来就是基础算法面临的问题，由等式约束的帘所引起的其他问题便未被察觉。

4.1 帘的分类

对于单个等式约束，有些帘可以简单处理。因此，我们进一步对帘进行分类。

定义 14. 设 $f \in \mathbb{R}[x_1,\ldots,x_n]$和 $\alpha \in \mathbb{R}^{n-1}$。我们称 f在 α处有点帷幕，如果对于所有 $y \in \mathbb{R}$，都有 $f(\alpha, y) = 0$，并且存在 α的一个欧几里得开邻域 $U \subset \mathbb{R}$，使得不存在 $\beta \in U\backslash\{\alpha\}$ 满足对于所有 $y \in \mathbb{R}$，都有 $f(\beta, y) = 0$。

例5. 我们给出一个例子来说明这种差异。

- 点帷幕： $f(x,y,z) = x^2 + zy^2 - z$在$(0,1)$和$(0,-1)$处有点帘。
- 非点帘：考虑 $f\ x\ y\ z = -x^3y^3z - xy^4z + xy^3z^2 + x^4 + 2x^3z + x^2y - x^2z + 2xyz - 2xz^2$ (, ,)。对于所有 $y \in \mathbb{R}$，它在$(0,y)$上有一个非点帘。

注意，在 $\mathbb{R}^3$中，所有非点帘都是显式帷幕。例 5 中关于非点帘的例子，其形式为 $x\cdot$(五次多项式)，因此是显式帷幕（参见定义 3）。例 1 中的帘分别是显式非点帘和隐式点幕。这些帘绘制在图2中。

现在来说明，当我们试图利用等式约束所定义的超曲面时，帘为何会带来问题。

例 6. 令 $f = x^2 + y^2 - 1$ （我们假设它是一个等式约束）、$g_1 = z - x - 1$和 $g_2 = z - y - 1$。那么 $\mathrm{res}_z(f,g_1) = x^2 + y^2 - 1 = \mathrm{res}_z(f,g_2)$，但这并未提供有关 $\mathrm{res}(g_1,g_2)$的信息。在这种情况下，当等式约束存在非点帘时，就无法利用 P^E_{BM}检测该帘上其他约束的交集。在本例中， f在 z中的次数不是正次数，因此无论如何都不会考虑它。

例7。 设 $f = x - yz$（我们假设它是一个等式约束）、$g_1 = z - x$ $= z - y$和 g_2 （我们假设它们不是等式约束）。那么 $\mathrm{res}(f,g_1)$ g_1， g_2 $= x^2 - 1 - x$ 以及 $\mathrm{res}(f,) = y^2 - x$ 以及 $\mathrm{res}(\mathrm{res}(f,),\mathrm{res}(f,))()$。这为我们提供了关于 g_1和 g_2相互作用的信息。在这种情况下，当等式约束具有点帷幕时， P^E_{BM}会检测该帷幕上其他约束的交集。

对帘进行分类同样重要。给定一个使 $f \in \mathbb{R}[x_1, \ldots, x_n]$ 归零的点 $\beta \in \mathbb{R}^{n-1}$，可以通过查看字典序最小半赋值，对脚部含有 β 的帘进行分类。如果 $\nu_\beta(f) \neq 0$，则检查 1-胞腔邻居。如果其中任何一个单元在该点的半赋值也非零，那么该帘就是非点帘。

4.2 点帘

点帘不会给提升过程带来问题。

命题 2（[19, 命题 6]）。设 f，$g \in \mathbb{R}[x_1, \ldots, x_n]$ 和 $\alpha \in \mathbb{R}^{n-1}$，并假设簇 V_f 由 f 定义，且在 α 处包含一个帘。如果 结式$(f, g)(\alpha) = 0$，那么 V_g 在 α 处包含一个帘，或在 V_f 上与其相交于有限多个点 α。

修正投影算子 P^E_{BM} 仅投影关于等式约束以及等式约束与非等式约束之间结式的信息。在 $\mathbb{R}^{n-1}$中，测试 T 在 P^E_{BM} 会检测具有点足的帘；如果它认为存在非点帘，则会返回 $\perp$。由 P_{BM} 在较低层级检测到的任何帘，无论是点帘还是非点帘，提升后都会成为 $\mathbb{R}^{n-1}$中具有非点足的帘。下述定理表明，P^E_{BM} 实际上会为 $\mathbb{R}^{n-1}$中具有点足的帘生成符号不变的柱状代数分解。

定理 4.1（[19, 定理 20]）。设 $f, g \in \mathbb{R}[x_1, \ldots, x_n]$，$E$ 是 f 我们等式约束的不可约基，并假设 $\alpha \in \mathbb{R}^{n-1}$ 是 P^E_{BM}（$\{f, g\}$ Γ）$points$ 的一个单元。那么 g 在 $f_\alpha g_\alpha$ 的截面和扇区上符号不变。

证明。根据假设，V_f 在 α 处有一个点帷幕。这意味着存在 $\mathbb{R}^{n-1}$ 中包含 0^{n-1} $\beta \in B$ α $\nu_\alpha f \neq 0^{n-1}$ 的一个邻域 B，使得对于 $\setminus\{\}$，$\nu(f)$，且 $\nu(\,)$。由于我们使用投影算子 $P_{BM}(E)$，其中 E 是 f 的不可约因子集合，因此多项式 f 相对于投影算子 $P_{BM}(E)$ 生成的柱状代数分解是字典序最小不变的。由于多项式 f 相对于该柱状代数分解是字典序最小不变的，且 V_f 在 α 处有一个幕，因此该柱状代数分解由形如 $\alpha \times (a, b)$ 的单元或点胞腔 $\alpha \times \{c\}$ 组成，其中 $a, b, c \in \mathbb{R}$。

我们知道 $\mathrm{res}(f, g)(\alpha) = 0$。根据命题 2，$V_g$ 在 α 处有一个点帷幕，或仅在有限多个点处与 V_f 相交。如果 V_g 在 α 处有一个帷幕，那么 g 在 α 上方的所有单元中都是符号不变（为零）的。假设 V_f 仅在有限多个点处与 V_g 相交，并令 $Z = \{\beta_1, \ldots, \beta_k\}$（按递增顺序排列）为 $f_\alpha g_\alpha$ 的根。那么，α 上方的单元将呈现为 $\alpha \times (a, b)$ 或点胞腔 $\alpha \times \{c\}$ 的形式，其中 a、b、$c \in Z$。注意，对于每个 i，β_i 必定是 f_α 或 g_α 的根。由于 $g = 0$ 仅在有限多个点处与 $f = 0$ 相交，且 g_α 的所有根都位于 Z 中，因此 g 在 $\alpha \times (\beta_i, \beta_{i+1})$ 中非零。g 在点胞腔 (α, β_i) 上为零，其中 β_i 是 g 的根；在其他位置则非零。□

定理 4.1 是 Lazard 风格柱面代数分解与等式约束理论融合过程中首个并不直接明了的地方。

4.3 非点幕

即使存在非点幕，根据定理 3.3 和 4.1 我们知道，在第一（投影）层使用 P^E_{BM}，并在后续层使用P_{BM}，可以在非点幕之外生成符号不变柱面代数分解。因此，挑战完全局限于非点幕（如果存在）。例 6 表明，我们需要考虑等式约束以外的多项式的结式，因为 P^E_{BM} 相比P_{BM}丢失了过多信息。因此，我们的策略如下。

(1) 在第一层使用 P^E_{BM} 进行投影，在后续各层使用 P_{BM}，并提升至 $\mathbb{R}^{n-1}$，从而得到分解 D_1、……、D_{n-1}，以及 D_n；其中其他约束在非幕单元和点幕单元上保持符号不变，在这些单元上 $f = 0$。(2) 如果不存在非点幕，则过程完成。否则，设 (α_1 α_{n-1} $C_i \in (i)$、… D_{n-1} …、(i)) 为构成非点幕的单元的样本点。我们知道，所选的等式约束在这些单元上为零。(3) 使用 P_{BM} 将所有其他约束投影至 $\mathbb{R}^1$。令 P_i 为投影在层级 $\mathbb{R}^i$ 上的多项式部分。(4) 在 $\mathbb{R}^1$ 中，考虑其样本点为 $\alpha(i)$ 1 的单元，并根据 P_1 对其进一步分解，将 D_1 细化为 D_1，同时引入必要的样本点。(5) 在 $\mathbb{R}^2$ 中，考虑其样本点为 $(\alpha(i)\,1,\ \alpha(i)\,2)$ 的那些单元

它们在 $\mathbb{R}^1$ 上的基底已在前一阶段完成分割，但也可能需要根据 P_2中的多项式，沿 x_2 方向进一步分割。此时需要计算适当的新样本点。(6) 继续执行到 $\mathbb{R}^{n-1}$，然后将这些单元提升到 $\mathbb{R}^n$。(7) 我们在每个 D_i 中细分了若干单元，从而得到 $\widehat{D}_i$。若要得到完全柱状的分解，可能需要将这些细分扩展到每个 $\widehat{D}_i$的整体。

步骤（7）纯粹是数据结构操作：除了为新分割的单元计算样本点之外，无需进行新的多项式计算。

分解等式约束的一张幕，与分解集合 $S \times \mathbb{R}$（其中 $S \subset \mathbb{R}^{n-1}$）是相同的。在幕中处理时，等式约束并未提供任何关于其余多项式约束如何相互作用的信息。以下定理验证了我们分别分解幕的方法。

定理 4.2（[19, 定理 21]）。设 $A = \{f,\ g_1,\ \ldots g_m\}$ 是一个多项式约束集，其中 f 是等式约束。设 D 是通过应用步骤 (1)–(7)得到的柱状代数分解。则 g_1，……，g_m 在 D 的单元上符号不变，其中 $f = 0$。

证明。设 S 是 $\mathbb{R}^{n-1}$ 的一个连通子集，使得 f 在 S 上是 Lazard 可描绘的，并且集合 $\{\mathrm{res}_{x_n}(f, g_j) | 1 \leq j \leq m\}$ 在 S 上是字典序最小不变的。若 V_f 在 S 上不包含非点帘，则由定理 3.3 和 4.1 可得结论。反设不然。由于 V_f 在 S 上包含非点帘，上述步骤将 S 分解为互不相交的连通子集，其中 f 是 Lazard 可描绘的，且 $P_{BM}(\{g_1, \ldots, g_m\}$ $\Gamma)$ 是 [4]上的字典序最小不变的。因此，根据定理 3.1，g_1，……，g_m 在 V_f 的帘的单元上字典序最小不变，因而也符号不变。 □

5 多重等式约束

我们现在将前面的思想推广到包含多个等式约束的情形，这需要修改投影的多个层级。

5.1 高维幂

定义 15（参见[19,定义 43]）。若簇 $C \subseteq \mathbb{R}^n$被称为 m-幕，如果对于任意 $(x_1, \ldots\ldots, x_n) \in C$，则 $(x_1, \ldots\ldots, x_{n-m}, y_{n-m+1}\ y_n\ \ y_{n-m+1}\ y_n\ \ , \ldots\ldots,) \in C$对所有 $(, \ldots\ldots,) \in \mathbb{R}^m$均成立。

换言之， C 是一个 m-幕，当且仅当它是$\mathbb{R}^n \to \mathbb{R}^{n-m}$的纤维的并。

定义 16（参见[19,定义 44]）。设 $S \subseteq \mathbb{R}^{n-m}$且 $f \in \mathbb{R}[x_1, \ldots, x_n]$。我们称 V_f（或 f）在 S处有一个 m-幕，如果对于所有 $(\alpha_1, \ldots, \alpha_{n-m}) \in S$以及所有 $(y_{n-m+1}, \ldots, y_n) \in \mathbb{R}^m$，都有 $f(\alpha_1, \ldots, \alpha_{n-m}, y_{n-m+1}, \ldots, y_n) = 0$。我们称 S为帷幕底集。

5.2 修正投影

对于多个等式约束，我们受 [17] 启发，进一步修改了投影算子。现在假设给定一个如下形式的无量词公式

$$(f_1 = 0) \wedge \ldots \wedge (f_k = 0) \wedge \Phi,$$

其中 Φ 包含多项式约束 g_j。

在此公式中，等式约束由多项式 f_1、……、f_k 给出。由于该塔斯基公式的解集必须满足这些等式约束，因此我们将注意力集中于等式约束的交集。

定义 17. 设 A 是 $\mathbb{R}[x_1, \ldots, x_n]$ 中一个有限的不可约多项式集，满足 $n \geq 2$，且设 E 是 A 的子集。多个等式约束的修正 *Brown–McCallum* 投影算子 $\hat{}P^E_{BM}(A)$ 是 $\mathbb{R}[x_1, \ldots, x_{n-1}]$ 的子集，由以下多项式组成。

(1) A 中各元素的所有首项系数。 (2) A 中由测试 **T** 要求的各元素的末项系数。 (3) A 中各元素的所有判别式。 (4) 所有结式 $\mathrm{res}_{x_n}(f, g)$，其中 $f \in E$、 $g \in A$ 且 $f \neq g$。

这与定义 13 的区别恰好在于： [17] 与 [16] 的区别在于增加了项目（3）。与之前一样，我们将选择等式约束，并令 E 为它们的不可约因子集合。

我们通过递归使用此算子来利用多个等式约束。所选等式约束与其余等式约束之间的结式，是投影多项式的等式约束。因此，我们一次处理一个等式约束；所以如果有 k 个等式约束，我们将在前 k 次投影中使用 $\hat{}P^E_{BM}(A)$：有关多个等式约束的更多内容，请参见 [12] 。下面的定理证明了递归使用 $\hat{}P^E_{BM}(A)$ 的合理性。

定理 5.1（参见 [19,定理 22]）。假设 f 和 $g \in \mathbb{R}[x_1, \ldots, x_n]$ 在 x_n 中都具有正次数。令 $S \subset \mathbb{R}^{n-1}$ 为一个连通子集，使得 f 在 S 上没有幕。若 判别式x_n（g）、首项系数x_n（g）以及 结式x_n（f、g）在 S 上都为字典序最小不变，则 g 在 S 上的 f 的每个截面和扇区上都是字典序最小不变的。

证明。由定理 3.1 可知， g 在 f的各个截面上符号不变。由于 $\mathrm{disc}_{x_n}(g)$ 和 $\mathrm{lc}_{x_n}(g)$ 在 S上字典序最小不变， g由定理 S2.1可知，在 S上 Lazard 可描绘。因此， g 在 f的各个截面和扇区上字典序最小不变。□

5.3 无幕时的正确性

定理 5.2（参见 [19,定理 27]）。设 A是 x_1中一组不可约多项式，它们在 x_n 中次数为正，其中 $n \geq 2$。设 E是 A的一个子集，且 Γ是 $\mathbb{R}^n$中的一个有限点集。设 S是 $\mathbb{R}^{n-1}$的一个连通子集。假设 $\hat{}P^E_{BM}(A, \Gamma)$的每个元素在 S中均字典序最小不变。那么 E的每个元素在 S上均 *Lazard* 可描绘，且以下情况恰有一种成立。

(1) 由 E 中各元素的乘积定义的超曲面有一个底足为 S 的幕。(2) E 中各元素的 *Lazard* 截面在 S 上两两不相交。 A 中的每个元素在这些 *Lazard* 截面上都是字典序最小不变的。

证明。如果属于情况 1，那么 E 中至少有一个元素在整个幕上为零，因此情况 2 没有意义。故这两种情况互不相交。

因此，假设 S不是 E中任何元素的幕底足。那么，由于 $\hat{}P^E_{BM}(A, \Gamma) \supset P_{BM}(E)$， 中各元素的 Lazard 截面在 S上两两不相交。根据定理 5.1， 中的元素在这些 Lazard 截面上都是字典序最小不变的。□

因此，如果从未遇到幕，那么我们在 S 上得到一个字典序最小不变的柱状堆栈。假设（在计算结式以传播等式约束之后） $x_n, \ldots, x_{n-k+1}$中每个变量层级都有一个等式约束，那么，先应用 k 次 $\hat{}P^E_{BM}$，接着应用 $n-k-1$次 P_{BM}，最后进行 $n-1$ 次 Lazard 提升，在没有幕的情况下，就能得到一个关于 A 的字典序最小不变柱状代数分解，变量为 $V_{f_1,\ldots f_k}$。

5.4 幕

但是，如果我们在提升过程中遇到等式约束的幕（无论是原始方程约束，还是等式约束的结式），该怎么办？在这里，我们必须借鉴 §4.3 中的方法，即将整个 $A \setminus E$投影到幕上。不过，可能存在多个幕，它们可能位于不同的提升层级，而且这些幕可能属于导出等式约束。

因此我们建议，如果在提升阶段检测到幕，就采用 §4.3 的方法，但对 A到 $\mathbb{R}^1$进行完整的投影，使用 P_{BM}，然后执行步骤（4）–（6），细化那些包含幕的堆叠上的分解。

6 示例

更多示例见 [22, §7.2] 和 [10]。此处讨论的例子是 [22, §7.2]，中的第一个例子，摘自 [11, §2.2.3]。问题最初的表述如下：

$$\exists u\, \exists v\ -uv + x = 0 \wedge -uv^2 + y = 0 \wedge -u^2 + z = 0. \tag{10}$$

由 [22] $u \prec v \prec y \prec z \prec x$ 中所述启发式方法选出的序为 。由于我们有多个等式约束，因此可以按照 [9, 12, 23] 中的建议使用 Gröbner 基。这将柱面代数分解问题转化为

$$\{vx - y, uv - x, \mathbf{ux - vz}\}, \tag{11}$$

其中，粗体显示的方程被视为等式约束。其投影如下：

$$\{-v^2z + uy, \mathbf{u^2 - z}\}; \{\mathbf{uv^2 - y}\}; \{v\}; \{u\}. \tag{12}$$

选定 $uz - vz$ 作为初始等式约束后，各幂为 $u = 0 \wedge v = 0$ 和 $u = 0 \wedge z = 0$，但实际上它们被分解为 15 个单元（每个分解为 9 个单元，但其中有三个重复），如 [22, 表 7.1]所示。如 §5.4 中所述，我们必须在这些幂上提升 $A \setminus E$，即 $\{vx - y,\ uv - x\}$。

$$\{vx - y, uv - x\}; \emptyset, ; \{y, uv^2 - y\}; \{v\}; \{u\} \tag{13}$$

合并后的结果是一个包含 591 个单元的柱状代数分解。

如果我们仅采用“单个等式约束”方法，Lazard 投影（如 [22, 第 238] 页所示）为

$$\{-v^2z + uy, u^2 - z\}; \{y, uv^2 - y\}; \{v\}; \{u\} \tag{14}$$

由于多了一个 y 多项式，因此总共有 951 个单元。

这 y 是一个末项系数，Brown–McCallum 投影不需要它，因此在这种情况下，其行为与多个等式约束相同（这是意料之中的，因为首次投影之后，只有当多项式总数超过两个时，才能体现出节省）。

7 复杂度分析

定义 18. 设 $\{f_i\}$ 为一个有限多项式集。$\{f_i\}$ 的组合最大次数是集合中的最大元素

$$\bigcup_j \left\{ \deg_{x_j} \prod_i f_i \right\}.$$

定义 19（[14, 第 6 节。1]）。若一组多项式可以划分为 m 个集合，且每个集合的组合最大次数都小于或等于 d，则该组多项式具有 (m, d)性质。

在 [19, 第 8] 章（基于 [14]）进行的复杂度分析结果汇总于表 1。如果输入集具有 (m, d)性质，那么投影之后的投影多项式集具有 $(M, 2d^2)$性质，其中 M如表 1所示。

表 1：柱状代数分解中多项式的增长

理论依据		原始	单个等式约束	多重等式约束
McCallum	[14]	$\left\lfloor \frac{(m+1)^2}{2} \right\rfloor$	$\left\lfloor \frac{5m+4}{4} \right\rfloor$	$\left\lfloor \frac{11m}{4} \right\rfloor$
Lazard	[18]	$\left\lfloor \frac{(m+1)^2}{2} \right\rfloor$	$\left\lfloor \frac{5m+3}{4} \right\rfloor$	$\left\lfloor \frac{9m-1}{4} \right\rfloor$
Brown-McCallum	[4]	$\frac{m(m+1)}{2}$	$\left\lfloor \frac{5m+2}{4} \right\rfloor$	$\left\lfloor \frac{9m-2}{4} \right\rfloor$

值得注意的是，随着表格向下，渐近复杂度几乎没有改善：唯一发生变化的首项是“多重等式约束”列中的首项，从 11 降至 9。实际应用中的差异则更为显著：[4, p 145] 表明，他们的方法（“改进的 Lazard 方法”）所需的单元仅为基本 Lazard 方法的 27%。

这表明，如果只有一个等式约束，那么“单一等式约束”方法更优。然而，如果有多个等式约束，“多重等式约束”方法则更优：对于具有两个（或更多）等式约束的投影，原始方法的多项式数量上界为 $O(m^4)$，“单一等式约束”方法的上界为 $O(m^2)$，“多重等式约束”方法的上界为 $O(m)$。

8 结论

我们分析了单个和多个等式约束。表1 明，如果只有一个等式约束，“单个”方法明显更优，但代价是只能生成一个符号不变分解，而这足以满足所有已知应用的需求。

8.1 单个等式约束

定理 3.3 告诉我们，可以将 [16] 的单个等式工作（可能因零化而失败）转移到 Brown– McCallum 投影中，适用于 [16] 有效的情形。复杂度增益 [12] 相同：多项式数量的双重指数降低 1。定理 4.1 将此结论扩展到点帷幕，并带来相同的复杂度改进。

定理4.2 表明，即使存在非点帘，我们也可以使用等式约束，但在帘上获得的效率提升较为有限，且难以用简单的形式表述。

8.2 多个等式约束

定理 5.2 告诉我们，可以将 [17] 的单个等式工作（遇到零化时会失败）转移到 Brown–McCallum 投影中，适用于 [17] 有效的情形。复杂度增益[12] 相同：多项式数量的双重指数降低 k，即我们可以应用$\hat{}P^E_{BM}$的连续层数。

存在帘时，我们的方法可能比单纯使用 [4], 更高效，但这很难量化。参见 §6。

8.3 未来工作

还有几个开放问题。

(1) 我们讨论过“具有等式约束的连续层数”。这在 [17] 中也是隐式的。但在没有帘的情况下，似乎可以在 PBM 和 $\hat{}P^E_{BM}$ 之间灵活搭配，在每个存在等式约束的层使用 $\hat{}P^E_{BM}$。不过，要将其形式化，需要一个合适的归纳假设。(2) §4.2 更简洁地处理了单个等式约束情形下的点帘。当这个帘出现在从 $\mathbb{R}^{n-1}$ 到 $\mathbb{R}^n$ 的提升过程中时，我们可能也能对多个等式约束采用同样的方法。但如果点帘出现在别处呢？目前我们建议将其视为非点帘——还能做得更好吗？(3) [12] 建议在 [17] 的情形下，使用 Gröbner 基而非结式来传播等式约束。这已在 §6 中得到验证。(4) [1, （另见 [2]] ）引入了“真值表不变 CAD”的概念，在这种方法中，等式约束可能只支配公式的一部分，例如 $((f_1 = 0) \wedge \Phi_1) \vee ((f_2 = 0) \wedge \Phi_2)$。这套理论建立在 [16], 之上，因此应该也适用。

此外，[19, §9.1] 探讨了字典序最小是否是我们应该考虑的唯一另一种赋值（除了 [6]中的符号和 [14]中的序之外）。文中指出：“上半连续性这一性质保证，如果两个多项式在某个集合上赋值不变，那么它们的乘积在同一集合上也赋值不变，反之亦然；这有助于我们利用等式约束。”那么，我们还可以考虑哪些其他上半连续赋值?

参考文献

[1] R.J. Bradford、J.H. Davenport、M. England、S. McCallum 和 D.J. Wilson。2013。用于布尔组合的柱面代数分解。载于 ISSAC *2013* 125 132 10 1145 2465506 2465516 会议论文集。– 。[2] https://doi.org/ 。/ 。R.J. Bradford、J.H. Davenport、M. England、S. McCallum 和 D.J. Wilson。2016。真值表不变柱面代数分解。《符号计算杂志》76（2016 1 35 10 1016 2015 11 002），– 。https://doi.org/ 。/j.jsc.。[3] C.W. Brown。2001。柱面代数分解的改进投影。《符号计算杂志》32 2001 447 465 10 1006 2001 0481（），– 。[4] https://doi.org/ 。/jsco.。C.W. Brown 和 S. McCallum。。柱面代数分解的 Lazard 方法改进。载于《科学计算中的计算机代数 CASC 2020》（施普林格计算机科学讲义，第 12291 卷），F. Boulier、M. England、T.M. Sadykov 和 E.V. Vorozhtsov（编）。129–149。https://doi.org/ 10 1007 978 3 030 60026 6_8 。/ - - - - C. Chen、M. Moreno Maza、[5] B. Xia 和 L. Yang。2009。通过三角分解计算柱面代数分解。载于 ISSAC *2009,* 95 102 10 1145 1576702 1576718 会议论文集，J. May（编）。–[6] 。https://doi.org/ 。/ 。G.E. Collins。。通过柱面代数分解消去实闭域上的量词。载于第二届 GI 自动机理论与形式语言大会论文集（施普林格计算机科学讲义，第 33 卷）。134–183。https://doi.org/ 10 1007 3 540 07407 4_17 。/ - - - G.E. Collins。。通过柱面代数分解进行量词消去——二十年的进展。载于《量词消去与柱面代数分解》，B.F. Caviness 和 J.R. Johnson（编）。Springer Verlag，维也纳，8–23。https://doi.org/ 10 1007 978 3 7091 9459 1_2 。/ - - - - J.H. Davenport 和 M. England。。多项式系统是否需要双重指数时间？载于《国际数学软件大会 ICMS 2016》（施普林格计算机科学讲义，第 9725 卷），G-M. Greuel、T. Koch、P. Paule 和 A. Sommese（编）。157–164。https://doi.org/10.1007/978-3-7091- 9459-1 2[9] J.H. Davenport 和 M. England。2017。带等式约束的 CAD 对 SC-Square 的潜力与挑战。载于 MACIS 2017 会议论文集：计算机与信息科学的数学方面。280–285。https://doi.org/10.1007/978-3-319-72453-9 22[10] J.H. Davenport、Z.P. Tonks 和 A.K. Uncu。2023年。一种用于量词消去的多算法方法。https://arxiv.org/abs/2302.06814。[11] A. Dolzmann、A. Seidl 和 Th. Sturm。2004。用于 CAD 的高效投影序。载于 ISSAC 2004 会议论文集，J. Gutierrez（编）。111–118。https://doi.org/10.1007/978- 3-319-72453-9 22

[12] M. England、R.J. Bradford 和 J.H. Davenport。2020。带等式约束的柱面代数分解。载于《符号计算与可满足性检查：符号计算杂志特刊》，J.H. Dav-enport、M. England、A. Griggio、T. Sturm 和 C. Tinelli（编）。第 100 卷。38–71。https://doi.org/ 10 1016 2019 07 019 。/j.jsc. . . D. Lazard。. 柱面代数分解的改进投影[13] 算子。载于《代数几何及其应用：Shreeram S. Abhyankar 60 岁生日会议论文集》，C.L. Bajaj（编）。1994。467 476 10 1007 978 1 4612 2628 4_29 –。https://doi.org/。/ - - - - S. McCallum。[14] 。. 柱面代数分解的改进投影运算。技术报告 578。威斯康星大学麦迪逊分校计算机科学系。1985。https://minds.wisconsin.edu/bitstream/handle/1793/58594/TR578.pdf?sequence=1[15] S. McCallum。1998。柱面代数分解的改进投影运算。载于《量词消去与柱面代数分解》，B.F. Caviness 和 J.R. Johnson（编）。施普林格出版社，维也纳，242–268。https: //doi.org/ 10 1007 978 3 7091 9459 1_12 。/ - - - - S. McCallum。[16] 。. 带等式约束的基于 CAD 的量词消去中的投影。载于 ISSAC ’99 论文集，S. Dooley（编）。1999。145–149。https: //doi.org/ 10 1145 309831 309892 。/。S. McCallum。[17] 。. 基于 CAD 的量词消去中等式约束的传播。载于 ISSAC 2001 论文集，B. Mourrain（编）。2001。223–230。https://doi.org/ 10 1145 384101 384132 。/。S. McCallum、A. Parusiński 和 L. Paunescu。[18] 2019。CAD 构造中 Lazard 方法的有效性证明。《符号计算杂志》92（2019），52–69。https: //doi.org/ 10 1016 2017 12 002 。/j.jsc. . . A.S. Nair。. 柱面代数分解中的帷幕。博士论文。[19] 巴斯大学。2021。https://researchportal.bath.ac.uk/en/studentTheses/curtains-in-cylindrical-algebraic-decomposition [20] A.S. Nair、J.H. Davenport 和 G.K. Sankaran。2020。CAD 中的帷幕：为什么它们是问题，又该如何解决？载于《数学软件——ICMS 2020》（《施普林格计算机科学讲义》，第 12097 卷），A.M. Bigatti、J. Carette、J.H. Davenport、M. Joswig 和 T. de Wolff（编）。17–26。https: //doi.org/ 10 1007 978 3 030 52200 1_2 。/ - - - - A. Nair、J. Davenport、G. Sankaran 和[21] S. McCallum。2019。利用等式约束的 Lazard CAD。《ACM 计算机代数通讯》53（2019），138–141。https://doi.org/ 10 1145 3377006 3377020 。/。Z. Tonks。. 实数域量词消去中的多算法技术。[22] 博士论文。2021。巴斯大学。https://researchportal.bath.ac.uk/en/ studentTheses/poly-algorithmic-techniques-in-real-quantifier-elimination [23] D.J. Wilson、R.J. Bradford 和 J.H. Davenport。2012。利用 Gröbner 基加速柱面代数分解。载于 CICM 2012 论文集，J. Jeuring 等（编）。279–293。https://doi.org/10.1007/978-3-642-31374-5_19