arXiv:2602.06817v1 [cs.SC] 6 Feb 2026

使用通用有理单变量表示求解参数多项式系统

Florent Corniquel[1]

索邦大学，巴黎西岱大学，法国国家科学研究中心（IMJ-PRG），INRIA
florent.corniquel@inria.fr

摘要。本文提出一种针对一般情况下为零维的参数多项式系统的通用参数化。具体而言，我们研究有理单变量表示的特化性质，并推导其各元素在次数和高度方面的界。此外，我们还提出两种算法，以有效计算这种参数化。

关键词：计算机代数，多项式系统，参数系统，零维

1 引言

1.1 经典零维情形

考虑 K一个特征零的域，以及生成零维理想 $\mathcal{I}$的 f_1、……、$f_n \in K[X_1, \ldots, X_n]$多项式。利用乔形式，可以找到仿射簇 $V(\mathcal{I})$ 的参数化。定义所谓的乔形式为 $h(U_0, \ldots, U_n) := \prod_{x \in V(\mathcal{I})} (U_0 - x_1 U_1 - \cdots - x_n U_n)^{\mu(x)}$其中 U_0、……、U_n是相互独立的变量，而 $\mu(x)$ 表示 x的重数。随后，我们选取系数 a_1、……、$a_n \in K$，使线性形式 $t = a_1 X_1 + \cdots + a_n X_n$在 $V(\mathcal{I})$ 上是单射。在这种情况下，我们称 t 分离了$V(\mathcal{I})$。于是，初始系统 $f_1 = \cdots = f_n = 0$ 等价于下列系统：

$$\begin{cases} h(U_0, a_1, \ldots, a_n) = 0 \\ X_i = \frac{\frac{\partial h}{\partial U_i}(U_0, a_1, \ldots, a_n)}{\frac{\partial h}{\partial U_0}(U_0, a_1, \ldots, a_n)}, \ 1 \leqslant i \leqslant n \end{cases} .$$

我们用 $h_0 := h(U_0, a_1, \ldots, a_n)$、$h_1 := \frac{\partial h}{\partial U_0}(U_0, a_1, \ldots, a_n)$ 和 $h_{X_i} := \frac{\partial h}{\partial U_i}(U_0, a_1, \ldots, a_n)$ 表示 $i \in [\![1, n]\!]$。这里，$[\![1, n]\!]$ 是介于 1 和 n 之间的整数集合。族 $\mathcal{F} := \{h_0, h_1, h_{X_1}, \ldots, h_{X_n}\} \subseteq K[U_0]$ 称为 $V(\mathcal{I})$ 的有理单变量表示（ RUR ）。

人们尝试了不同的方法来计算这些多项式。Rene- gar 在 [25] 中将 h 表示为 Van der Waerden 的 u-结式的一个因子。这种方法的主要问题在于，当代数簇 $V(\mathcal{I})$ 含有维数大于零的分支，或

存在无穷远点时，-结式可能恒等于零。然而，可以利用 Canny 广义特征多项式（[3]）解决这一问题。

最成功的实现基于对商环 $\mathcal{A} := K[X_1, \ldots, X_n]/\mathcal{I}$ 的了解，更具体地说，是通过 $\mathcal{A}$ 的一组基 $\mathcal{B} = \{p_1, \ldots, p_D\}$，以及 $\mathcal{A}$ 中各变量对应的乘法矩阵 M_{X_1}、.....、M_{X_n}。这些可由初始系统的 Gr¨obner 基计算得到，所需运算次数为 $O(nD^3)$，运算所在的域为 K（例如参见 [10]）。Rouillier 在 [26] 中进一步完善了这一方法，他指出，可利用相对于 $\mathcal{B}$ 的乘法矩阵的迹来计算 $\mathcal{F}$ 的元素。线性形式 $t = a_1X_1 + \cdots + a_nX_n$ 分离 $V(\mathcal{I})$ 这一事实至关重要；所提出的算法采用拉斯维加斯方法：先“随机”选取线性形式，之后再验证其是否为单射。

验证形式 t 是否分离 $V(\mathcal{I})$ 是该问题的重要环节，而在大多数情况下，这一验证的代价与多项式的计算一样高。由于无需预先知道 t 是否分离 $V(\mathcal{I})$，就能计算多项式 h_0、h_1、h_{X_1}、.....、h_{X_n}，因此通常将族 $\mathcal{F}$ 称为有理单变量表示候选（RUR 候选）；当 t 是分离形式时，才称其为 RUR。这一区分是合理的，因为无论如何都能计算 $\mathcal{F}$ 的元素。

在 [8], 中，作者提出了一种新的拉斯维加斯算法：给定一个零维理想 $\mathcal{I}$，仅根据商代数 $K[X_1, \ldots, X_n]/\mathcal{I}$中变量对应的乘法矩阵$M_{X_1}$、.....、$M_{X_n}$，即可在 $\tilde{O}(D^2\delta + nD^2(D - \delta + 1))$次运算内，同时解决计算 $V(\mathcal{I})$的有理单变量表示以及验证给定线性形式 t 在其中具有分离性的问题。这里，δ 是 t 的最小多项式的次数，而 D 是商代数的维数。

1.2 参数系统

对于参数系统，我们考虑 f_1、.....、$f_n \in K[W, X]$。我们称 $W := [W_1, \ldots, W_s]$ 表示参数（我们希望将其替换为特定值），称 $X := [X_1, \ldots, X_n]$ 为未知数，我们希望用参数来表示这些未知数。现有不同的方法，下面将对它们进行简要概述。

首先，可以提及 Weispfenning 在 [31] 中首次引入的综合 Gr¨obner 基。综合 Gr¨obner 基可以理解为一个多项式族，对于参数的所有取值，该多项式族经特化后都成为特化系统的 Gr¨obner 基。它们通常由 Gr¨obner 系统构造而来，即一族二元组 (S_i, G_i)，其中 S_i 是参数空间的一个可构造子集，且对于 S_i中的所有参数取值，G_i 经特化后都是一个 Gr¨obner 基。构造这些 S_i 时，旨在使其构成参数空间的一个划分。该方法的主要缺点是划分的规模往往呈指数级增长。此方法的复杂度非常高，而且尚不清楚能否有效实现。

在他的博士论文（[28, 第 7]章）中，Eric Schost 通过在 $\mathbb{Q}(W)[X]$ 中进行运算，将三角集用于求解参数系统。他对

三角集中出现的多项式次数给出的上界并不优于 $d^{o(n^2)}$，其中 d 是初始系统中多项式的最高次数，而且他并未尝试实现该方法。此后，Schost 在 [29] 提出了一种用于计算参数化解的概率算法。其思路是使用形式牛顿算子提升特化系统的解。借助直线程序，他得以将复杂度控制在输出规模的多项式级别。然而，该方法要求雅可比理想为零，也就是说排除了可能存在的重数。

一般而言，研究参数系统十分困难，而要获取有关系统的可靠信息往往需要进行代价高昂的计算。例如，在实几何领域，Collins 在 [4] 中提出了柱面代数分解（CAD），它将空间划分为若干单元，使给定多项式在每个单元上的符号保持不变。已知在最坏情况下，其复杂度相对于变量数呈双指数增长（例如，参见 [6]）。

例如，这种技术可以补充参数空间判别簇的计算。该对象由 [17] 引入，是由那些使特化系统表现出“异常”行为的参数值构成的代数簇，例如出现无穷远根或无穷多个解。这个代数簇有一个非常方便的性质：其补集是若干开子集的并，在这些开子集上，特化系统的解的数量有限且恒定。[17] 中的作者提出了一种计算判别簇的算法；此外，还可以对其补集进行柱面代数分解，从而明确描述上述开子集。然而，计算判别簇的复杂度本质上也呈指数级增长（参见 [23]）。

最后，我们还可以提及 [18] 中的研究：作者计算了半代数公式，用以定义参数空间中的半代数子集；在这些子集中，特化系统具有恒定数量的实解。他们的方法依赖于计算参数化埃尔米特二次型的矩阵，并研究其秩。

1.3 本文的贡献与结构

在第 2 节中，我们引入一般化有理单变量表示（GRUR）的概念，并证明在 $\mathbb{C}(W)$ 中计算的有理单变量表示（RUR）（按照 Rouillier 在 [26] 中提出的定义）具有良好的特化性质。考虑 $t \in \mathbb{C}[X]$ 为一个线性形式，它对几乎所有参数值都能分离特化簇。接着我们证明，除去一个零测集参数代数集后，在 $\mathbb{C}(W)$ 中计算的 RUR$[X]$可特化为特化簇的有理单变量表示，从而说明一般化 RUR 这一名称的合理性。为此，我们采用 Van der Waerden 的方法构造该系统的参数化 u-结式，并研究其特化行为。

遗憾的是，这种方法的计算复杂度过高。事实上，尽管可以将 u-结式表示为两个行列式之商，并从 Macaulay 矩阵计算得到（见 [20]），但要对这个结式进行因式分解，很快就会变得

过于困难。不过，我们可以由此推导出 GRUR 中多项式的次数和高度界。我们将在第3节介绍这一结果，并充分利用 [5] 中证明的某个算术 Nullstellensatz。

在第4节和第5节中，我们提出了两种不同的算法来计算 GRUR。第一种算法依赖于线性代数，更确切地说，依赖于这样一个事实：商代数 $\mathbb{C}(W)[X]/\mathcal{I}_W$ 是一个有限维向量空间，其中 $\mathcal{I}_W$ 是由 $\mathbb{C}(W)[X]$ 中的方程生成的理想。这种方法基于 [26] 的工作。第二种算法基于求值/插值方案。其思路是使用 [8] 中提出的新算法，尽可能多地计算特化有理单变量表示，然后对 GRUR 的系数进行插值。如果初始方程在 X 中的次数不超过 d_X，且在 W 中的次数不超过 d_W，我们证明可以使用 $\tilde{O}(sn^{2s+2}d_X^{2ns+2n}d_W^{2s+1} + n^{s+1}d_X^{2ns+5n}d_W^s)$ 次 $\mathbb{Q}$ 运算计算 GRUR。随后，我们可以利用所计算出的 GRUR 的第一个多项式来处理实根分类问题，并提出一种求解算法。该算法的复杂度高于现有算法，但不需要对系统作任何假设。

2 GRUR 的构造

我们首先介绍一些记号。

– $W := [W_1, \ldots, W_s]$ 是参数， $X := [X_1, \ldots, X_n]$ 是未知数；– 给定参数 $w \in \mathbb{C}^s$的一个取值，我们用 ϕ_w 表示将 W_i 映射到 w_i 的特化态射；– 我们分别用 $<_X :=$ grevlex(X)和 $<_W :=$ grevlex(W)表示变量 X 和 W上的分次逆字典序，并用$<_{X,\ W} :=$grevlex(W) $<$ grevlex(X)表示相应的消元分块序；– 对于上述三个单项式序之一，我们将使用由 “$<_X$” 、 “$<_W$” 或 “$<_{W,\ X}$” 标记的LT、LM和LC记号，分别表示首项、单项式和系数。

2.1 GRUR 的定义

设 $f_1, \ldots, f_n \in \mathbb{C}[W, X]$ 是一族生成一般为零维理想 $\mathcal{I} := \langle f_1, \ldots, f_n\rangle \subseteq \mathbb{C}[W, X]$的多项式。那么，存在 $\mathbb{C}^s$ 的一个测度为 0 的扎里斯基闭子集 $\mathcal{D}$，使得对于参数 $w \in \mathbb{C}^s\backslash\mathcal{D}$的所有取值，特化理想 $\mathcal{I}(w) := \langle f_1(w, X) \ldots, f_n(w, X)\rangle \subseteq \mathbb{C}[X]$ 都是零维的，或者等价地，代数簇 $\mathcal{V}_w := V(I(w)) \subseteq \mathbb{C}^s$ 具有零维。

我们希望将有理单变量表示的概念扩展到参数系统，即希望找到一个单变量多项式族 $\mathcal{F} = \{h_0, h_1, h_{X_1}, \ldots, h_{X_n}\} \subseteq \mathbb{C}(W)[U_0]$ ，使得对于参数 $w \in \mathbb{C}^s$ 的几乎所有取值，以下等价关系成立

$$\begin{cases} f_1(w, X) = 0 \\ \vdots \\ f_n(w, X) = 0 \end{cases} \iff \begin{cases} h_0(U_0, a_1, \ldots, a_n; w) = 0 \\ X_i = \frac{\frac{\partial h}{\partial U_i}(U_0, a_1, \ldots, a_n; w)}{\frac{\partial h}{\partial U_0}(U_0, a_1, \ldots, a_n; w)},\ 1 \leqslant i \leqslant n \end{cases} . \qquad (1)$$

同时保持重数不变。换言之，我们希望族 $\mathcal{F}$ 对于参数的几乎所有取值，都能按照 [26, 定义 3.2] 的意义，特化为 $V(\mathcal{I}(w))$ 的一个（经典）有理单变量表示。这便引出了以下定义。

定义 1. 若对于几乎所有$w \in \mathbb{C}^s$，族 $\mathcal{F} := \{h_0, h_1, h_{X_1}, \ldots, h_{X_n}\}$ 都是 $V(\mathcal{I}_W)$ 的一般化有理单变量表示（GRUR）（分别为通用有理单变量表示候选），即族 $\phi_w(\mathcal{F})$ 定义了 $V(\mathcal{I}(w))$ 的有理单变量表示（分别为有理单变量表示候选），则称该族为 $V(\mathcal{I}_W)$ 的一般化有理单变量表示（GRUR）（分别为通用有理单变量表示候选）。

现在，我们将 f_1、...、f_n 看作 $\mathbb{C}(W)[X]$ 中的元素。它们生成理想 $\mathcal{I}_W \subseteq \mathbb{C}(W)[X]$。记 $\mathcal{G} \subseteq \mathbb{C}[W, X]$ 为理想 $\mathcal{I}$ 关于乘积序 $<_{W,\ X}$ 的一个约化 Gröbner 基。那么，$\mathcal{G} \subseteq \mathbb{C}(W)[X]$ 也是理想 $\mathcal{I}_W$ 关于序 $<_X$ 的一个 Gröbner 基（例如参见 [18]）。然而，它可能不是约化的。我们将代数簇 $\cup_{g\in\mathcal{G}} V(\mathrm{LC}_{<X}(g))$ 记为 $\mathcal{W}_{\mathcal{G}}$。

引理 1. 记 $\mathbb{C}(W)$ 为 $\mathbb{C}(\overline{W})$ 的一个代数闭包。那么代数簇

$$V(I_W) := \left\{ x \in \overline{\mathbb{C}(W)}^n \mid f_1(W, x) = \cdots = f_n(W, x) = 0 \right\}$$

的维数为零。

证明. 对于参数 w 在 $\mathcal{D} \cup \mathcal{W}_{\mathcal{G}}$之外的所有取值，特化理想$\mathcal{I}(w)$ 的维数为零，并且 $\mathcal{G}(w) := \{g(w, X) \quad g \in \mathcal{G}\}$ 是$\mathcal{I}(w)$ 关于 $<_X$ 的 Gr¨obner 基（见 8）。

根据有限性定理（见 [7, §5.3 定理 6]），存在非负整数 $m_1, \ldots, m_n$ 和 $g_1, \ldots, g_n \in \mathcal{G}$，使得每个 g_i 的首单项式 $\mathrm{LM}_{<X}(g_i) = X_i^{m_i}$。根据假设，我们有 $\mathrm{LM}_{<X}(g_i(w, X)) = \mathrm{LM}_{<X}(g_i)$，这也意味着 $V(\mathcal{I}_W)$ 的维数为零。□

知道 $V(\mathcal{I}_W)$ 的维数为零后，我们可以按照引言中的经典有理单变量表示构造过程进行。考虑一个线性形式 $t := a_1X_1 + \cdots + a_nX_n \in \mathbb{C}[X]$（不涉及 W），并考虑多项式 $h := \prod_{x\in V\ (\mathcal{I}_W)} (U_0 - U_1x_1 - \cdots - U_nx_n)^{\mu\ (x)}$，其中 $\mu(x)$ 是 x 的重数。

然后我们按以下方式定义多项式 h_0、h_1、h_{X_1}、.....、h_{X_n}：

$$\begin{cases} h_0(U_0; W) := h(U_0, a_1, \ldots, a_n; W) \\ h_1(U_0; W) := \frac{\partial h}{\partial U_0}(U_0, a_1, \ldots, a_n; W) \\ h_{X_i}(U_0; W) := \frac{\partial h}{\partial U_i}(U_0, a_1, \ldots, a_n; W),\ 1 \leqslant i \leqslant n \end{cases} . \tag{2}$$

定义 2. 如果t 分离 $V(\mathcal{I}_W)$，则称线性形式 $t \in \mathbb{C}[X]$ 是一般分离的；也就是说，对于几乎所有 $w \in \mathbb{C}^s$ 的取值， $V(\mathcal{I}(w))$。

对于 t 分离$V(\mathcal{I}_W)$这一几何事实，可以自然地作出代数重述。

命题 1. 线性形式 $t = a_1X_1 + \cdots + a_nX_n$ 分离 $V(\mathcal{I}_W)$，当且仅当判别式 $\mathrm{Disc}_{U_0}(\overline{h}(a_1, \ldots, a_n; W)) \in \mathbb{C}(W)$ 不恒为零，其中 $\cdot$ 是关于变量 U_0 的无平方因子部分。

证明. 回顾一下， $h := \prod_{x\in V(\mathcal{I}_W)}(U_0 - x_1U_1 - \cdots - x_nU_n)^{\mu(x)}$。那么，关于 U_0 的无平方因子部分为 $\overline{h} = \prod_{x\in V(\mathcal{I}_W)}(U_0 - x_1U_1 - \cdots - x_nU_n)$。换言之，我们消去了几何重数。将 $U_1, \ldots, U_n$ 的值代入 $a_1, \ldots, a_n$ 后，得到 $\overline{h}(U_0, a_1, \ldots, a_n; W) = \prod_{x\in V(\mathcal{I}_W)}(U_0 - t(x))$。当且仅当乘积中出现的线性因子均不重复时，这个多项式才是无平方因子的；也就是说，当且仅当 t 在 $V(\mathcal{I}_W)$ 上是单射时成立。□

备注1. 若一个线性形式分离 $V(\mathcal{I}_W)$，则对于几乎所有 $w \in \mathbb{C}^s$，它也分离 $V(\mathcal{I}(w))$。反过来结论也成立，但两个都能分离 $V(\mathcal{I}_W)$ 的线性形式，可能在那些不能分离特化系统的参数代数集上有所不同。

定理 1. 设 $f_1, \ldots, f_n \in \mathbb{C}[W, X]$ 生成一个零维的一般理想 $\mathcal{I}$。令 $t = a_1X_1 + \cdots + a_nX_n \in \mathbb{C}[X]$ 为线性形式。那么由 2 定义的族 $\mathcal{F}$: $= \{h_0, h_1, h_{X_1}, \ldots, h_{X_n}\}$ 是 $V(\mathcal{I}_W)$ 的 GRUR 候选。此外，若 t 是一般分离的，则 $\mathcal{F}$ 是 $V(\mathcal{I}_W)$ 的 GRUR。

接下来的小节将提供证明定理 1 所需的一些要素。我们在推论 1 中指出需要避开的参数值。

2.2 类 Van der Waerden 方法

该方法的关键思想是 Renegar 在 [25] 中已经采用过的一个思路。其核心是，多项式 h （由此可导出 $\mathcal{F}$ 的元素）是 Van der Waerden 的 u-结式的一个因子。这个结式具有很好的特化性质，可用于研究 h 的特化。我们快速回顾一下 Van der Waerden 的思路（[30, §11.83]）。我们添加一个由 $f_0 = 0$ 给出的新方程，其中 $f_0 := U_0 - U_1X_1 - \cdots - U_nX_n$。这里 $U := [U_0, \ldots, U_n]$ 是彼此独立的新变量。接着，我们引入名为 X_0 的新变量，将 f_0、……、f_n 齐次化为 F_0、……、F_n。注意，$F_0 \in \mathbb{Z}[U][X_0, \ldots, X_n]$、$F_1$、……、$F_n \in \mathbb{C}[W][X_0, \ldots, X_n]$。现在，$F_0$、……、$F_n$ 是关于 $n+1$ 个变量的 $n+1$ 多项式，因此它们的结式是有定义的。它称为 u-结式，记作 Res(F_0,……, F_n)。它是 $\mathbb{C}[W][U_0, \ldots, U_n]$ 的一个元素。

注 2。 u-结式可能恒等于零。在这种情况下，我们下面介绍的方法将失效。例如，当代数簇含有正维分支时，就会出现这种情况。根据我们的假设， $V(\mathcal{I}_W)$ 是零维的，因此不会发生这种情况。如果 $V(\mathcal{I}_W)$ 的射影闭包含有一个无穷远点，结式也可能恒等于零。通过一般变量变换可以避免这个问题（见 [22]）。

在本节余下部分，我们假设 $V(\mathcal{I}_W)$ 在无穷远处没有点。记 $F_i := F_i(0, X_1, \ldots, X_n)$。在这些假设下，结式 $\tilde{}$ $\tilde{}$Res($F_1, \ldots, F_n$) $\in \mathbb{C}[W]$ 不恒等于零，因此可得以下结果。

命题 2. u-结式可分解为

$$Res(F_0,\dots,F_n)(U;W) = Res(\tilde{F_1},\dots,\tilde{F_n})(W) \prod_{x\in V(\mathcal{I}_W)} (U_0 - x_1U_1 - \cdots - x_nU_n)^{\mu(x)}. \tag{3}$$

证明。首先，齐次结式的泊松公式（见 [14, 命题 2.7]）给出 Res($F_0,\dots,F_n$) = Res($F_1,\dots,F_n$) $\cdot$ det(m_{f_0})，其中 m_{f_0}是由 f_0 在商环 $\mathbb{C}(W)[X]/\mathcal{I}_W$ 中诱导的乘法端同态。然后，我们可以应用 Stickelberger 定理 5，得到所述表达式。□

我们回顾一下，$h(U;\ W) = \prod_{x\in V(\mathcal{I}_W)}(U_0 - x_1U_1 - \cdots - x_nU_n)^{\mu(x)}$，并且给定 $t = a_1X_1 + \cdots + a_nX_n$ 时，有 $h_0(U_0;\ W) = h(U_0, a_1,\dots,a_n;\ W)$。

2.3 定理 1 的证明

首先，我们证明族 $\mathcal{F} = \{h_0, h_1, h_{X_1},\dots,h_{X_n}\}$ 是一个 GRUR 候选。我们证明，按照定义 3.2] 中的含义，$\phi_w(\mathcal{F})$ 是 $V(\mathcal{I}(w))$ 的一个 RUR 候选。下面引入一个简短的引理。

引理 2. 对所有 $i \in [\![1, n]\!]$,

$$\frac{\frac{\partial \overline{h}}{\partial U_i}(U_0, a_1,\dots,a_n;W)}{\frac{\partial \overline{h}}{\partial U_0}(U_0, a_1,\dots,a_n;W)} = \frac{h_{X_i}(U_0;W)}{h_1(U_0;W)} \tag{4}$$

其中，$\overline{\cdot}$ 是关于 U_0的无平方因子部分。

证明. 方程（4）中的左侧正是右侧的约化形式。将右侧的分子和分母同时乘以 $\prod_{y\in V(\mathcal{I}_W)}(U_0 - x_1U_1 - \cdots - x_nU_n)^{\mu(x)-1}$，即可得到结果。□

这个引理的含义是，在 Rouillier 给出的有理单变量表示定义中，使用 h_0 或其无平方因子部分来定义有理分式不会产生任何变化。在我们的情形中，我们将使用带重数的公式，因为它们具有更好的特化性质。因此，利用 ϕ_w 与导数可交换这一点，唯一剩下需要证明的是：对于几乎所有的 $w \in \mathbb{C}^s$，$h_0(U_0; w)$ 是商环 $\mathbb{C}[X]/\mathcal{I}(w)$ 中乘以 t 的乘法的特征多项式，也就是说，$h_0(U_0;\ w) = \prod_{x\in V(\mathcal{I}(w))}(U_0 - t(x))^{\mu(x)}$。

基于这一目标，我们来概述一下下文将会出现的 $\mathbb{C}^s$ 代数集：

– 我们回顾一下，$\mathcal{D}$ 是使特化系统不是零维的参数集合；– 我们用 $\mathcal{L}$: $= \cup_{i=0}^{n} V(\mathrm{LT}_{<X}(f_i)) \subseteq \mathbb{C}^s$ 表示这样一组参数：初始方程在 X 中的一个或多个首系数为零；– 我们用 $\mathcal{S}$ 表示这样一组参数：对于这些参数，t 在$V(\mathcal{I}(w))$ 上不是单射；

– 我们用 $\mathcal{W}_\infty$ 表示使特化系统存在无穷远根的参数集合。

注 3. $\mathcal{W}_\infty$ 是代数集这一事实源于 $\mathcal{W}_\infty = \sim \quad \sim V(\mathrm{Res}(F_1, \ldots, F_n))$。

我们先研究公式 (3) 的特化。

引理 3. 对于参数 $w \in \mathbb{C}^s \backslash \mathcal{L}$ 的任意取值，3 中出现的两个结式都可以特化。换言之，

$$\phi_w\Big(\mathit{Res}(F_0, \ldots, F_n)\Big) = \mathit{Res}\left(\phi_w(F_0), \ldots, \phi_w(F_n)\right) \tag{5}$$

and

$$\phi_w\left(\mathit{Res}(\tilde{F}_1, \ldots, \tilde{F}_n)\right) = \mathit{Res}\left(\phi_w(\tilde{F}_1), \ldots, \phi_w(\tilde{F}_n)\right) \tag{6}$$

证明. 只要结式各自的变量次数不变，结式就可以特化。在 $\mathcal{L}$ 之外，$f_0, \ldots, f_n$ 的次数以及 $F_0, \ldots, F_n$ 和 $\sim \quad \sim F_1, \ldots, F_n$ 的次数在特化后都不变，因此两个结式都可以特化。□

这一特化性质使我们能够确定多项式 $h(U; W)$ 特化后的结果。

引理 4. 对于参数 $w \in \mathbb{C}^s \backslash (\mathcal{D} \cup \mathcal{L} \cup \mathcal{W}_\infty)$ 的任意取值，我们有

$$\phi_w\left(h(U; W)\right) = \prod_{x \in \mathcal{V}_w} (U_0 - x_1 U_1 - \cdots - x_n U_n)^{\mu(x)}. \tag{7}$$

证明。首先，我们可以再次使用 [14, 命题 27] 中的泊松公式和 Stickelberger 定理，得到

$$\mathrm{Res}\left(\phi_w(F_0), \ldots, \phi_w(F_n)\right) =$$

$$\mathrm{Res}(\phi_w(\tilde{F}_1), \ldots, \phi_w(\tilde{F}_n)) \prod_{x \in V(\mathcal{I}(w))} (U_0 - x_1 U_1 - \cdots - x_n U_n)^{\mu(x)}. \tag{8}$$

然后，我们可以将 (5) 和 (6) 代入 (8)。由于 $w \notin \mathcal{W}_\infty$，特化系统在无穷远处没有根，因此公式 (8) 非平凡。我们可以将其与 (3) 的特化进行比较，从而得到所需公式。□

现在，我们只需将取值 U_1、……、U_n 代入 (7) 中的 a_1、……、a_n，即可得到

$$\phi_w\left(h(U_0, a_1, \ldots, a_n; W)\right) = \phi_w(h_0) = \prod_{x \in V(\mathcal{I}(w))} (U_0 - t(x))^{\mu(x)}. \tag{9}$$

而该方程右端恰好是商环 $\mathbb{C}[X]/\mathcal{I}(w)$ 中乘以 t 的乘法特征多项式（这再次用到了 Stickelberger 定理）。我们将所有内容总结为以下命题。

命题 3. 对于参数 $w \in \mathbb{C}^s \backslash (\mathcal{D} \cup \mathcal{L} \cup \mathcal{W}_\infty)$ 的任意取值，族 $\phi_w(\mathcal{F})$ 是 $V(\mathcal{I}(w))$ 的一个 RUR 候选。

现在假设线性形式 t 一般分离，并用 $\mathcal{S} \subseteq \mathbb{C}^s$ 表示由满足 t 在 $V(\mathcal{I}(w))$ 上不是单射的 $w \in \mathbb{C}^s$ 构成的零测度代数集。由此立即得到一个推论。

推论 1. 对于参数 $w \in \mathbb{C}^s \backslash (\mathcal{D} \cup \mathcal{L} \cup \mathcal{W}_\infty \cup \mathcal{S})$ 的任意取值，族 $\phi_w(\mathcal{F})$ 是 $V(\mathcal{I}(w))$ 的有理单变量表示。

证明. 根据命题 3，我们知道 $\mathcal{F}$ 专化为 $V(\mathcal{I}(w))$ 的一个 RUR 候选。当 t 分离 $V(\mathcal{I}(w))$ 时，它便成为有理单变量表示。根据定义，当 $w \notin \mathcal{S}$ 时即为如此。

注 4. 我们有包含关系 $\mathcal{D} \subseteq \mathcal{W}_\infty$，因此一般条件可表示为 $w \in \mathbb{C}^s \backslash (\mathcal{W}_\infty \cup \mathcal{L} \cup \mathcal{S})$。这一结论源于以下事实：若 $w \in \mathcal{D}$，则 $V(\mathcal{I}(w))$ 的维数为零，因此其射影闭包与无穷远超平面相交，即 $w \in \mathcal{W}_\infty$。

3 GRUR 的大小

本节给出 GRUR 中多项式的次数和大小的一些界。

下文中，我们用记号 $\mathfrak{h}(f) := \log_2(\|f\|_\infty)$ 表示整数系数多项式 f 的高度。本节中，假设通过通分使 f_1、……、f_n 具有整数系数。我们用 : 表示:

- $d_{1,X}, \ldots, d_{n,X}$ the total degrees of $f_1, \ldots, f_n$ in X and $d_X := \max_{1 \leqslant i \leqslant n} d_{i,X}$;
- $d_{1,W}, \ldots, d_{n,W}$ the total degrees of $f_1, \ldots, f_n$ in W and $d_W := \max_{1 \leqslant i \leqslant n} d_{i,W}$;
- $c := \max_{1 \leqslant i \leqslant n} \|f_i\|_\infty$ the maximum coefficient among $f_1, \ldots, f_n$ and $\tau := \max_{1 \leqslant i \leqslant n} \mathfrak{h}(f_i)$.

3.1 h 的界

本节所述的工作大量运用了 [5] 中介绍的算术 Nullstellensatz¨。我们衷心感谢 Teresa Krick 提供这一参考文献。

定理 2。存在 $\Delta \in \mathbb{Z}[W][U]$ 和 $P \in \mathbb{Z}[W]$，使得

$$h(U; W) = \frac{\Delta(U; W)}{P(W)}$$

具有以下界:

– $\deg_U(\Delta) \leqslant d_X^n$; – $\deg_W(\Delta) \leqslant (n+1) d_X^n d_W$; – $\deg_W(P) \leqslant n d_X^{n-1} d_W$; – $\mathfrak{h}(\Delta)\ \mathfrak{h}(P) \leqslant O\big(n d_X^n \tau + n d_X^n d_W \log_2(s+1)\big)$.

证明。我们首先沿用 [5, 例 4.18 和 4.37] 的思路，并考虑总次数为 $d_0, \ldots, d_n$的一般多项式

$$\mathbf{F}_j := \sum_{|\alpha|=d_j} u_{j,\alpha} X^\alpha,\ 0 \leqslant j \leqslant n$$

其中 $\mathbf{u}_j := \{u_{j,\alpha},\ |\alpha| = d_j\}$ 和 $X^\alpha = X_0^{\alpha_0} \cdots X_n^{\alpha_n}$。记 $\mathbf{u} := \{\mathbf{u}_1、\ \ldots、\ \mathbf{u}_n\}$。这些一般系数稍后将特化为上一节中 $F_0、\ \ldots、\ F_n$ 的系数。

将 [5, 中的算术 Nullstellensatz 定理 4.28] 应用于 $V = \mathbb{A}^n_{\mathbb{Q}}$ 和 $\mathrm{F}_0、\ \ldots、\ \mathrm{F}_n$，可知存在 $\alpha \in \mathbb{Z}[\mathbf{u}]$ 和 $g_0、\ \ldots、\ g_n \in \mathbb{Z}[\mathbf{u}\ X]$，使得

$$g_0(\mathbf{u}, X)\mathbf{F}_0 + \cdots + g_n(\mathbf{u}, X)\mathbf{F}_n = \alpha \tag{10}$$

其次数和高度满足以下界：

- $\deg_{\mathbf{u}_l}(\alpha) \leqslant \prod_{\substack{j=0 \\ j\neq l}}^{n} d_j,\ 0 \leqslant l \leqslant n$;
- $\mathfrak{h}(\alpha) \leqslant d_X^{n-1}(6n+10)\log_2(n+2)$.

结式 $\mathrm{Res}(\mathrm{F}_0、\ \ldots、\ \mathrm{F}_n)$ 生成消去理想 $\langle \mathrm{F}_0、\ \ldots、\ \mathrm{F}_n\rangle \cap \mathbb{Z}[\mathbf{u}]$，因此存在某个 $\Lambda \in \mathbb{Z}[\mathbf{u}]$，使得 $\alpha = \Lambda\,\mathrm{Res}(\mathrm{F}_0、\ \ldots、\ \mathrm{F}_n)$。众所周知（例如参见 [7, §3.3, 定理 3.1]），$\mathrm{Res}(\mathrm{F}_0、\ \ldots、\ \mathrm{F}_n)$ 的关于 $\deg_{u_l}$ 的偏次数等于 $\prod_{\substack{j=0 \\ j\neq l}}^{n} d_j$。换言之，$\Lambda$ 关于每个变量的偏次数均为零，即 $\Lambda \in \mathbb{Z}$。

于是，我们可以将系数 $\mathbf{u}$ 特化为 $F_0、\ \ldots\ldots、\ F_n$ 的系数。关系式 (10) 变为

$$G_0(W, X)F_0 + \cdots + G_n(W, X)F_n = \Lambda\,\mathrm{Res}(F_0, \ldots, F_n)$$

其中 $G_0、\ \ldots\ldots、\ G_n \in \mathbb{Z}[W, X]$。

根据命题 2，我们知道 $\mathrm{Res}(F_0, \ldots, F_n)$ 可因式分解为乘积 $\tilde{}\qquad\tilde{}\mathrm{uct}\ C(W)h(U;\ W)$，其中 $C = \mathrm{Res}(F_1, \ldots, F_n)$。

记 $\Delta := \Lambda\,\mathrm{Res}(F_0, \ldots, F_n) \in \mathbb{Z}[W][U]$。这意味着我们有

$$h(U; W) = \frac{\Delta(U; W)}{P(W)} \tag{11}$$

其中 $P(W) := \Lambda C(W)$。

现在我们要做的是给出关于 W 的次数界，以及关于 Δ 和 ΛC 的高度界，从而推导出 GRUR 中多项式的界。根据 $h(U;\ W)$ 的定义，我们知道 $\deg_U(\Delta) \leqslant d_X^n$。

由 [5, 定理 4.28] 给出的关于方程 (10) 的界可以推导出关于 Δ的界。事实上，我们将方程 (10) 中的$F_0、\ \ldots\ldots、\ F_n$ 的系数特化，这些系数在 W中的次数至多为 d_W。对于每个 $l \in [\![0, n]\!]$，α关于 $\mathbf{u}_l$ 的偏次数有界于d_X^n，因此关于 $\mathbf{u}$ 的总次数有界于 $(n+1)d_X^n$，从而 $\deg_W(\Delta)$ 6 $(n+1)d_X^n d_W$。

对于高度界，我们使用了 [5, 引理 2。37]

引理 5。设 $f_1, \dots, f_r \in \mathbb{Z}[x_1, \dots, x_k]$ 的总次数有界于 d，位数有界于 τ，并设 $g \in \mathbb{Z}[y_1, \dots, y_r]$。则

$$\mathfrak{h}(f_1 \cdots f_r) \leqslant \sum_{i=1}^{r} \mathfrak{h}(f_i) + \log_2(k+1) \sum_{i=2}^{r} \deg(f_i),$$

and

$$\mathfrak{h}(g(f_1, \dots, f_r)) \leqslant \mathfrak{h}(g) + \deg(g)(\tau + \log_2(r+1) + d\log_2(k+1)).$$

在我们的情形中，f_i 是 F_0、……、F_n 的系数，因此 $r \leqslant n(d_X+1)^n+(n+1)$ 和 $k = s$。利用 α 的界，并仅保留主导项，我们得到

$$\mathfrak{h}(\Delta) \leqslant O\big(nd_X^n\tau + nd_X^n d_W \log_2(s+1)\big).$$

除此之外，由于 $\mathfrak{h}(\Lambda) \leqslant \mathfrak{h}(\Delta)$，该界对 Λ 也成立。

我们可以采用非常类似的推理，得到 $\tilde{}\quad\tilde{}\quad\tilde{}\quad\tilde{}C$ 的高度上界，因为它是 F_1、……、F_n 的结式。事实上，F_1、……、F_n 在 X 中的次数与 F_1、……、F_n 相同，因此可以取 τ 作为它们的高度界。记 $\mathbf{u}' := \mathbf{u}_1$、……、$\mathbf{u}_n$。我们首先对一般多项式 $\mathbf{F}_1$、……、$\mathbf{F}_n$ 应用 [5] 中的定理 4.28，从而得到 $\mathbf{u}'$] 和 z_1、……、$z_n \in \mathbb{Z}[\mathbf{u}'、X]$ 的存在，使得

$$z_1(\mathbf{u}', X)\mathbf{F}_1 + \cdots + z_n(\mathbf{u}', X)\mathbf{F}_n = \beta$$

满足以下次数和高度界：

- $\deg_{\mathbf{u}_l}(\beta) \leqslant \prod_{\substack{j=1 \\ j \neq l}}^{n} d_j \leqslant d_X^{n-1},\ 1 \leqslant l \leqslant n$；
- $\mathfrak{h}(\beta) \leqslant d_X^{n-2}(6n+10)\log_2(n+2)$.

此外，$\beta = \Lambda' \mathrm{Res}(\mathbf{F}_1, \dots, \mathbf{F}_n)$ 的 $\Lambda' \in \mathbb{Z}$ 与之前一样。然后，我们可以应用引理 5，得到 $\Lambda' C$ 的高度界，并将其作为 C 的高度界。同样，我们只保留主导项。

$$\mathfrak{h}(C) \leqslant O\big(nd_X^{n-1}\tau + nd_X^{n-1}d_W \log_2(s+1)\big). \tag{12}$$

由于 $\mathfrak{h}(\Lambda C) = \mathfrak{h}(\Lambda)+\mathfrak{h}(C)$，我们得到 $\mathfrak{h}(P) = \mathfrak{h}(\Lambda C) \leqslant O\big(nd_X^n\tau+nd_X^n d_W\log_2(s+1)\big)$。

对于次数，我们利用这样一个事实：$\mathrm{Res}(\mathbf{F}_1, \dots, \mathbf{F}_n)$ 关于 $\mathbf{u}'$ 的总次数有上界 nd_X^{n-1}，因此 C（这也意味着 P）关于 W 的次数至多为 $nd_X^{n-1}d_W$。□

3.2 GRUR 多项式的界

既然我们已经得到了 $h(U; W)$ 的次数和高度的界，就可以推出族 $\mathcal{F}$ 中多项式的次数和高度的界。对于某个 $k \geqslant 0$，当 $f = O(g\log_2^k(g))$ 时，我们记作 $f = \tilde{O}(g)$。

推论 2. 假设 $= a_1X_1 + \cdots + a_nX_n \in \mathbb{Q}[X]$ 是一个一般分离形式。那么，GRUR 的多项式 $h_0, h_1, h_{X_1}, \ldots, h_{X_n}$ 的高度有如下界

$$O\big(nd_X^n\tau + nd_X^n d_W \log_2(s+1) + n^2 d_X^n \log_2(d_X)\big) = \tilde{O}\big(nd_X^n\tau + nd_X^n d_W \log_2(s+1)\big)$$

且在 W 中的次数不超过

$$\kappa := (n+1)d_X^n d_W$$

我们将高度和次数分别定义为对应分子和分母中的最大值。

证明。记 τ_t 为线性形式 t 的高度。引理 2.1]，中表明，可以找到一个线性形式，在集合 $\mathcal{T} = \big\{X_1 + kX_2 + \cdots + k^{n-1}X_n,\ 0 \leqslant k \leqslant nD(D-1)/2\big\}$ 中分离 $V(\mathcal{I}_W)$。换言之，所选线性形式的系数不会大于 $(nd_X^{2n})^{n-1}$，这意味着 $\tau_t \leqslant O(n \log_2(n) + n^2 \log_2(d_X))$。

我们先来看多项式 $h_0(U_0; W)$，它由 $h_0(U_0; W) = h(U_0, a_1, \ldots, a_n; W) = \Delta(U_0, a_1, \ldots, a_n; W)/P(W)$ 得到。对变量 U 进行特化不会影响分母 P，也不会改变 Δ 在 W 中的次数界。对于高度，我们可以再次利用引理 5 得到

$$\begin{aligned}\mathfrak{h}(\Delta(U_0, a_1, \ldots, a_n; W)) &\leqslant \mathfrak{h}(\Delta) + \deg_U(\Delta)(\tau_t + \log_2(n+1)) \\ &\leqslant \mathfrak{h}(\Delta) + d_X^n\tau_t + d_X^n \log_2(n+1)\end{aligned}$$

并保留主导项，

$$\mathfrak{h}(\Delta(U_0, a_1, \ldots, a_n; W)) \leqslant O(nd_X^n\tau + nd_X^n d_W \log_2(s+1) + n^2 d_X^n \log_2(d_X)).$$

于是得到多项式 $h_1, h_{X_1}, \ldots, h_{X_n}$，如下所示

$$h_1(U_0; W) = \frac{\partial h}{\partial U_1}(U_0, a_1, \ldots, a_n; W) = \frac{\frac{\partial \Delta}{\partial U_1}(U_0, a_1, \ldots, a_n; W)}{P(W)}$$

and

$$h_{X_k}(U_0; W) = \frac{\partial h}{\partial U_k}(U_0, a_1, \ldots, a_n; W) = \frac{\frac{\partial \Delta}{\partial U_k}(U_0, a_1, \ldots, a_n; W)}{P(W)},\ 1 \leqslant k \leqslant n.$$

每个 $\partial\Delta/\partial U_i$ 的高度上界为 $\mathfrak{h}(\Delta) + n\log_2(d_X)$，并再次使用引理 5，可得

$$\begin{aligned}\mathfrak{h}\left(\frac{\partial \Delta}{\partial U_i}(U_0, a_1, \ldots, a_n; W)\right) &\leqslant \mathfrak{h}(\Delta) + n\log_2(d_X) + d_X^n\tau_t + d_X^n \log_2(n+1) \\ &\leqslant O(nd_X^n\tau + nd_X^n d_W \log_2(s+1) + n^2 d_X^n \log_2(d_X)).\end{aligned}$$

由于 P 的高度不超过该值，因此证明了 $h_1, h_{X_1}, \ldots, h_{X_n}$ 的高度界。

在接下来的两节中，我们将介绍两种拉斯维加斯算法，用于计算 $\mathcal{F}$ 的多项式。第一种基于线性代数，第二种则基于求值／插值方案。

4 第一种算法：线性代数方法

在本小节中，我们将同时处理泛型商代数 $\mathcal{A}_W := \mathbb{C}(W)[X]/\mathcal{I}_W$ 和针对取值 $w \in \mathbb{C}^s$ 的特化商代数，记作 $\mathcal{A}(w) := \mathbb{C}[X]/\mathcal{I}(w)$。与其中一个商代数相关的每个对象都将带有上标 $\mathcal{A}_W$ 或 $\mathcal{A}(w)$（或下标），以便加以区分。这一区分对于证明特化性质尤其有用。对于任意 $v \in \mathbb{C}(W)[X]$，我们分别将迹和特征多项式记为 $\mathrm{Trace}^{\mathcal{A}_W}(v)$ 和 $\chi_v^{\mathcal{A}_W}$，其对象为

$$\begin{aligned} m_v^{\mathcal{A}_W} \ : \ \mathcal{A}_W &\longrightarrow \mathcal{A}_W. \\ [f]_{\mathcal{A}_W} &\longmapsto [fv]_{\mathcal{A}_W} \end{aligned}$$

当我们将 $\mathcal{A}_W$ 替换为 $\mathcal{A}(w)$，并特化到 $w \in \mathbb{C}^s \backslash \mathcal{D}$ 时，我们通过对先前的记号作相应替换，为 $v \in \mathbb{C}[X]$ 选用类似的记号。

4.1 预计算

这种计算族 $\mathcal{F}$ 中多项式的方法需要一些预备条件，我们现在予以说明。

· Gr¨obner 基：我们用 $\mathcal{G}$ 表示 $\mathcal{I} \subseteq \mathbb{C}[W, X]$ 关于块序 $<_{W,\ X}$ 的一个约化 Gr¨obner 基。回顾一下，将 $\mathcal{G}$ 视为 $\mathbb{C}(W)[X]$ 的子集时，也可以将其解释为 $\mathcal{I}_W$ 关于序 $<_X$ 的一个 Gr¨obner 基。下文中，我们假定 $\mathcal{G}$ 已约化。

· 商环的基：$= \{[p_1]_{\mathcal{A}_W}, \ldots, [p_D]_{\mathcal{A}_W}\}$ 可通过保留所有不能被 $\mathcal{G}$约化的单项式，从 $\mathcal{G}$ 中计算得到 $\mathcal{B}_{\mathcal{A}_W}$： $\mathcal{A}_W$。

· 乘法矩阵：我们还需要商环 $\mathcal{A}_W$中每个变量 $M_{X_1}^{\mathcal{A}_W}$、……、 $M_{X_n}^{\mathcal{A}_W}$对应的乘法矩阵。可以按照 FGLM 的方法，参照 [10, 命题 21]来计算。

· 乘法张量：为了避免一遍又一遍地重复相同的计算，可以计算乘法张量

$$\mathrm{MT}(\mathcal{A}_W) := \{\overrightarrow{[p_i p_j]}_{\mathcal{A}_W},\ 1 \leqslant i, j \leqslant D\}$$

其中 $\overrightarrow{[\cdot]}_{\mathcal{A}_W}$ 是相对于基 $\mathcal{B}_{\mathcal{A}_W}$的坐标。

4.2 F 的计算

本小节给出的公式直接改编自 Rouillier 在 [26, §4]中的工作。

$\boldsymbol{h_0}$ 与 $\boldsymbol{h_1}$ 的计算。我们回顾$h_0 = \chi_t^{\mathcal{A}_W}$。尽管如此，牛顿公式可以用迹非常优美地表述，如下面的引理所示。

引理 6。设$\chi_t^{\mathcal{A}_W} = \sum_{i=0}^{D} b_i U_0^{D-i}$，其中 $b_0 = 1$。则$\chi_t^{\mathcal{A}_W}$的系数满足下列方程：

$$(D-k)b_k = \sum_{i=0}^{k} b_{k-i}\, Trace^{\mathcal{A}_W}(t^i), \qquad 0 \leqslant k \leqslant D. \tag{13}$$

由 (13) 给出的方程构成一个三角线性系统，求解起来很方便。此外，该系统仅依赖于迹 $\mathrm{Trace}^{\mathcal{A}_W}(t^i)$。

一旦得到 $\chi_t^{\mathcal{A}_W} = h_0$，我们就可以直接对其求导得到 h_1。

计算 $\boldsymbol{h_{X_1}, \ldots, h_{X_n}}$我们可以用可计算的闭式公式表示多项式 $h_{X_1}, \ldots, h_{X_n}$，这些公式仅取决于 t 和 h_0。当我们决定保留 GRUR 的分数而不约简时，它们与定理 3.1]公式类似（见引理 2）。

引理 7. 沿用记号 $h_0 = \chi_t^{\mathcal{A}_W} = \sum_{i=0}^{D} b_i T^{D-i}$，我们得到，对于每个 $j \in [\![1, n]\!]$,

$$h_{X_j}(U_0; W) = \sum_{i=0}^{D-1} Trace^{\mathcal{A}_W}(X_j t^i) H_{D-i-1}(U_0; W) \tag{14}$$

其中 $H_i(U_0; W) := \sum_{j=0}^{i} b_j U_0^{i-j}$是 h_0的第 ¨个 H ¨orner 多项式。

证明。回顾一下，$\chi_t^{\mathcal{A}_W}(U_0) = \prod_{x \in V(\mathcal{I}_W)} (U_0 - t(x))^{\mu(x)}$。于是我们可以将 h_{X_i} 改写为

$$\begin{aligned}
h_{X_i}(U_0; W) &= \sum_{x \in V(\mathcal{I}_W)} \mu(x) x_i (U_0 - t(x))^{\mu(x)-1} \prod_{\substack{y \in V(\mathcal{I}_W) \\ y \neq x}} (U_0 - t(y))^{\mu(y)} \\
&= \sum_{x \in V(\mathcal{I}_W)} \frac{\mu(x) x_i \prod_{y \in V(\mathcal{I}_W)} (U_0 - t(y))^{\mu(y)}}{U_0 - t(x)} \\
&= \chi_t^{\mathcal{A}_W}(U_0) \sum_{x \in V(\mathcal{I}_W)} \frac{\mu(x) x_i}{U_0 - t(x)} \\
&= \chi_t^{\mathcal{A}_W}(U_0) \sum_{x \in V(\mathcal{I}_W)} \sum_{i=0}^{+\infty} \frac{\mu(x) x_i t^i(x)}{U_0^{i+1}} = \chi_t^{\mathcal{A}_W}(U_0) \sum_{i=0}^{+\infty} \frac{\mathrm{Trace}^{\mathcal{A}_W}(X_i t^i)}{U_0^{i+1}}.
\end{aligned}$$

最后一个等式是通过交换求和符号，并使用 Stickelberger 定理给出的 $\mathrm{Trace}(X_i t^i)$ 表达式得到的。接着，我们可以利用 $\chi_t^{\mathcal{A}_W}$ 的展开式，得到

$$h_{X_i}(U_0; W) = \sum_{i=0}^{+\infty} \sum_{j=0}^{D} b_j\, \mathrm{Trace}^{\mathcal{A}_W}(X_i t^i) U_0^{D-j-i-1}. \tag{15}$$

(15) 的左边是一个多项式，因此上述求和中 i 和 j 的取值必然受到限制。更确切地说， $D-i-j-1$ 必须是非负数。这意味着 i 必须小于或等于 $D-1$，并且对于 i 的每个取值， j 都必须小于或等于 $D-i-1$。于是 (15) 变为

$$\begin{aligned} h_{X_i}(U_0;W) &= \sum_{i=0}^{D-1} \mathrm{Trace}^{\mathcal{A}_W}(X_i t^i) \sum_{j=0}^{D-i-1} b_j U_0^{D-j-i-1} \\ &= \sum_{i=0}^{D-1} \mathrm{Trace}^{\mathcal{A}_W}(X_i t^i) H_{D-i-1}(U_0;W) \end{aligned}$$

这就是所述公式。 □

4.3 公式的特化

现在我们证明引理 7 中给出的公式具有良好的特化性质。主要依赖于迹，因此我们需要确保它们能够良好特化的条件。

格罗布纳基的特化 令我们考虑 $w \in \mathbb{C}^s$ 和 $\mathcal{G}(w) := \{\phi_w(g) \quad g \in \mathcal{G}\}$。我们回顾一下 $\mathcal{W}_{\mathcal{G}} = \cup_{g\in\mathcal{G}} V($首项系数$_{<_X}(g))$。下面的引理给出了参数化格罗布纳基的一个特化性质。在 [24, 定理 2.6], 中，针对模格罗布纳基也给出了类似结果。

引理 8. 对所有 $w \in \mathbb{C}^s \backslash \mathcal{W}_{\mathcal{G}}$，族 $\mathcal{G}(w)$ 都是特化理想 $\mathcal{I}(w)$ 关于序反向字典序(X) 的格罗布纳基。

证明。由于唯一出现的分母是 $<_X$ 中元素的首项之积，并且根据假设它们不为零， $\mathcal{G}$ 中元素的 S-多项式的所有约化序列都与特化态射 ϕ_w 可交换。

此外，每个 S-多项式都约化为零，因为 $\mathcal{G}$ 是一个格罗布纳基。这对于 $\mathcal{G}(w)$ 中元素的 S 多项式同样成立，这些多项式是 $\mathcal{G}$中元素的 S-多项式的特化。结论由布赫伯格判据给出。□

这一结果对商环 $\mathcal{A}(w)$ 的维数具有重要影响。

推论 3。对于所有 $w \in \mathbb{C}^s \backslash (\mathcal{D} \cup \mathcal{W}_{\mathcal{G}})$，商环 $\mathcal{A}_W$ 和 $\mathcal{A}(w)$ 作为向量空间具有相同的维数 D 。

此外，如果 $\mathcal{B}_{\mathcal{A}_W} = \{[p_1]_{\mathcal{A}_W}, \ldots, [p_D]_{\mathcal{A}_W}\}$ 是 $\mathcal{A}_W$的一个 $\mathbb{C}(W)$-基，那么 $\mathcal{B}(w) := \{[p_1]_{\mathcal{A}(w)}, \ldots, [p_D]_{\mathcal{A}(w)}\}$ 是 $\mathcal{A}(w)$ 的一个 $\mathbb{C}$-基。

证明。根据我们的假设， $\mathcal{G}$ and$\mathcal{G}(w)$中的元素具有相同的首单项式，这意味着两个 Gr¨obner 基中的不可约单项式相同。□

标准形的特化 记 $\mathrm{NF}_{\mathcal{G}}(f)$ 为元素 f of $\mathbb{C}(W)[X]$ 关于 $\mathcal{G}$ 的标准形，记 $\mathrm{NF}^{\mathcal{G}(w)}(g)$ 为元素 g of $\mathbb{C}[X]$ 关于 $\mathcal{G}(w)$ 的标准形。特化性质的关键在于以下命题。

命题 4. 设 $w \in \mathbb{C}^s \backslash (\mathcal{D} \cup \mathcal{W}_{\mathcal{G}})$ 和 $v \in \mathbb{C}(W)[X]$，且没有分母在 w 处为零。则有

$$NF_{\mathcal{G}(w)}\left(\phi_w(v)\right) = \phi_w\left(NF_{\mathcal{G}}(v)\right).$$

证明. 首先说明， v 可以唯一地写成

$$v = \sum_{g \in \mathcal{G}} v_g \cdot g + \mathrm{NF}_{\mathcal{G}}(v) \tag{16}$$

其中每个 v_g 都是 $\mathbb{C}(W)[X]$ 的一个元素。它们是通过使用 $\mathcal{G}$ 逐步约化得到的，因此可能出现的唯一新分母是 $\mathcal{G}$ 的首项的乘积。换言之，(16) 中没有分母在 w 处为零，这意味着我们可以在 w 处对其进行特化，得到

$$\phi_w(v) = \sum_{g \in \mathcal{G}} \phi_w(v_g) \cdot \phi_w(g) + \phi_w(\mathrm{NF}_{\mathcal{G}}(v)). \tag{17}$$

根据假设，我们知道每个 $g \in \mathcal{G}$ 都满足关系 $\mathrm{LM}_{<X}(g) = \mathrm{LM}_{<X}(\phi_w(g))$。此外，出现在 $\mathrm{NF}_{\mathcal{G}}(v)$ 中的 X 的每个单项式（因而也出现在 $\phi_w(\mathrm{NF}_{\mathcal{G}}(v))$ 中）都不能被 $\mathcal{G}$ 的任何元素的首单项式整除（因而也不能被 $\mathcal{G}(w)$ 的任何元素的首单项式整除）。

根据引理 8， $\mathcal{G}(w)$ 是 $\mathcal{I}(w)$ 的一个 Gr¨obner 基，因此 $\phi_w(v)$ 关于 $\mathcal{G}(w)$ 的正规形是唯一确定的；借助 (17)，我们可以将其认作 $\phi_w(\mathrm{NF}_{\mathcal{G}}(v))$。□

由此直接得到从 $\mathcal{A}_W$ 到 $\mathcal{A}(w)$ 时的坐标特化。

推论 4. 设 $w \in \mathbb{C}^s \backslash (\mathcal{D} \cup \mathcal{W}_{\mathcal{G}})$ 和 $v \in \mathbb{C}(W)[X]$，且在 w处分母均不为零。分别记它们关于基 $\mathcal{B}_{\mathcal{A}_W}$ 和 $\mathcal{B}_{\mathcal{A}(w)}$ 在 $\mathcal{A}_W$ 和 $\mathcal{A}(w)$ 中的坐标为 $\overrightarrow{[\cdot]_{\mathcal{A}_W}}$ 和 $\overrightarrow{[\cdot]_{\mathcal{A}(w)}}$。则有

$$\overrightarrow{[\phi_w(v)]_{\mathcal{A}(w)}} = \phi_w\left(\overrightarrow{[v]_{\mathcal{A}_W}}\right)$$

其中 ϕ_w 自然地作用于每个坐标。

证明。出发点是这样一个事实： $\mathbb{C}(W)[X]$ 中的任意元素，或 $\mathbb{C}[X]$，都可以在 $\mathcal{A}_W$ 或 $\mathcal{A}(w)$ 中由其标准形表示。特别地，根据推论 4，我们得到

$$[\phi_w(v)]_{\mathcal{A}(w)} = [\mathrm{NF}_{\mathcal{G}(w)}(\phi_w(v))]_{\mathcal{A}(w)} = [\phi_w(\mathrm{NF}_{\mathcal{G}}(v))]_{\mathcal{A}(w)}.$$

接下来，写作 $\mathrm{NF}_{\mathcal{G}}(v) = \sum_{i=1}^{n} c_i p_i$，其中每个 c_i 都是 $\mathbb{C}(W)$ 中分母不为零的元素。这意味着 $[\mathrm{NF}_{\mathcal{G}}(v)]_{\mathcal{A}_W} = (c_1, \ldots, c_n)$。然后我们可以应用 ϕ_w，得到

$$\phi_w(\mathrm{NF}_{\mathcal{G}}(v)) = \sum_{i=1}^{n} \phi_w(c_i) p_i. \tag{18}$$

现在回顾一下（推论 3）： $\mathcal{A}_W$ 和 $\mathcal{A}$（w）在各自的基中具有相同的单项式，因此我们可以将 18 解释为

$$\overrightarrow{[\mathrm{NF}_{\mathcal{G}}(v)]_{\mathcal{A}_W}} = (\phi_w(c_1), \ldots, \phi_w(c_n)) = \phi_w((c_1, \ldots, c_n)).$$

□

乘法矩阵的特化 我们可以推导乘法矩阵的特化。

引理 9. 设 $w \in \mathbb{C}^s \setminus (\mathcal{D} \cup \mathcal{W}_{\mathcal{G}})$。那么对于任意 $v \in \mathbb{C}(W)[X]$，若其分母在 w 处不为零，则有

$$\phi_w\left(M_v^{\mathcal{A}_W}\right) = M_v^{\mathcal{A}(w)}$$

其中 ϕ_w 是逐项应用的。

证明. 对于每个 $i \in [\![1, D]\!]$，$M_v^{\mathcal{A}_W}$的第 i列由 $[vp_i]_{\mathcal{A}_W}$关于 $\mathcal{B}_{\mathcal{A}_W}$的坐标给出。然后我们可以利用推论 4 得到$\phi_w(\overrightarrow{[vp_i]_{\mathcal{A}_W}}) = \overrightarrow{[vp_i]_{\mathcal{A}(w)}}$，它是 $M_v^{\mathcal{A}(w)}$的第 i列。□

由此直接得到迹的特化。

推论 5. 设 $w \in \mathbb{C}^s \setminus (\mathcal{D} \cup \mathcal{W}_{\mathcal{G}})$。那么，对于任意 $v \in \mathbb{C}(W)[X]$，若其分母在 w 处不为零，则有

$$\phi_w\left(Trace^{\mathcal{A}_W}(v)\right) = Trace^{\mathcal{A}(w)}(\phi_w(v)).$$

$\boldsymbol{h_0}$ 和 $\boldsymbol{h_1}$ 的特化 以下引理表明，利用迹的计算，$\mathcal{F}$ 的前两个多项式可以很好地特化。

引理 10. 设 $w \in \mathbb{C}^s \setminus (\mathcal{D} \cup \mathcal{W}_{\mathcal{G}})$。那么我们有

$$\phi_w\left(\chi_t^{\mathcal{A}_W}\right) = \chi_t^{\mathcal{A}(w)}$$

特别是， $\chi_t^{\mathcal{A}(w)}$ 的 H ¨orner 多项式可通过对$\chi_t^{\mathcal{A}_W}$的相应多项式应用 ϕ_w 得到。

此外，我们有

$$\phi_w\left(\frac{d\chi_w^{\mathcal{A}_W}}{dT}\right) = \frac{d\chi_t^{\mathcal{A}(w)}}{dT}.$$

证明。第一点是将引理 9 与特化和行列式可交换这一事实结合应用而得出的

$$\begin{aligned}\phi_w\left(\chi_t^{\mathcal{A}_W}\right) &= \phi_w\left(\det(U_0 I_D - M_t^{\mathcal{A}_W})\right)\\ &= \det\left(TI_D - \phi_w(M_t^{\mathcal{A}_W})\right) = \det\left(U_0 I_D - M_t^{\mathcal{A}(w)}\right) = \chi_t^{\mathcal{A}(w)}.\end{aligned}$$

第二部分源于特化与求导可交换这一事实。□

h_{X_1}、……、 h_{X_n}的特化

引理 11。设 $w \in \mathbb{C}^s \backslash (\mathcal{D} \cup \mathcal{W}_{\mathcal{G}})$。则对于每个 $i \in [\![1, n]\!]$，我们有

$$\phi_w(h_{X_i})(U_0; W) = \sum_{i=0}^{D-1} Trace^{\mathcal{A}(w)}(X_i t^i)\phi_w(H_{D-i-1})(U_0; W)$$

且 $\phi_w(H_{D-i-1})$ 是 $\chi_t^{\mathcal{A}(w)}$ 的第 $(D-i-1)$ 个 H ¨orner 多项式。

证明。这是推论 5 和引理 10 的直接推论。

F 的特化 我们可以将前面的结果概括为以下定理。

定理 3. 假设 $t \in \mathbb{C}[X]$ 是一个线性形式，并且族 $\mathcal{F} = \{h_0, h_1, h_{X_1}, \ldots, h_{X_n}\}$ 是使用引理 6 和 7 中给出的公式计算得到的。那么对于所有的 $w \in \mathbb{C}^s \backslash (\mathcal{D} \cup \mathcal{W}_{\mathcal{G}})$，族 $\phi_w(\mathcal{F})$ 都是 $V(\mathcal{I}(w))$ 的 RUR 候选。

此外，若假设 t 在测度为 0 的扎里斯基闭子集 $\mathcal{S}$ 之外分离特化簇，那么对于所有的 $w \in \mathbb{C}^s \backslash (\mathcal{D} \cup \mathcal{W}_{\mathcal{G}} \cup \mathcal{S})$，$\phi_w(\mathcal{F})$ 都是 $V(\mathcal{I}(w))$ 的有理单变量表示。

4.4 证明 t 是否一般分离

现在我们给出一个判据，以有效检验给定的线性形式 t 是否一般分离。主要问题在于，我们无法直接计算多项式 $h(U_0, \ldots, U_n)$。然而，我们可以计算特定的实例 $h(U_0, a_1, \ldots, a_n)$，其中参数取值为 $a_1, \ldots, a_n \in \mathbb{C}$。如下引理所示，这已经足够。

引理 12. 设 $w \in \mathbb{C}^s \backslash (\mathcal{D} \cup \mathcal{W}_{\mathcal{G}})$ 使得 $\mathrm{Disc}^{U_0}(\overline{\chi_t^{\mathcal{A}_W}})(w) \neq 0$。那么 t 一般分离，当且仅当 t 分离特化簇 $V(\mathcal{I}(w))$。

证明。若 t 分离 $V(\mathcal{I}_W)$，则我们可以写成 $\overline{\chi_t^{\mathcal{A}_W}} = \prod_{x \in V(\mathcal{I}_W)}(T - t(x))$。这是相当经典的：此时判别式由判别式 $_T(\overline{\chi_t^{\mathcal{A}_W}}) = \prod_{y \neq x}(t(x) -$

$t(y))^2$, 给出，并且使 t 不分离 $V(\mathcal{I}(w))$的参数集合因此由 $V($判别式$_T(\overline{\chi_t^{A_W}}))$给出。根据假设， w 确实是该代数簇之外的一个值。

反过来，假设形式 t 分离 $V(\mathcal{I}(w))$。采用 §1.2 中的记号，这意味着判别式 $\mathrm{Disc}_{U_0}(\overline{h})$ 在 (w,a) 处不为零，其中 $a=(a_1,\dots,a_n)$ 是 t 的系数。特别地，$\mathrm{Disc}_{U_0}(\overline{h}(U_0,a_1,\dots,a_n)) \in\mathbb{C}(W)$ 不恒为零。此外， $\overline{h}(U_0,a_1,\dots,a_n)$ 关于 U_0 是首一的，因此可以写成

$$\begin{aligned}\mathrm{Disc}_{U_0}(\overline{h}(U_0,\dots,U_n))(a_1,\dots,a_n) &= \mathrm{Disc}_{U_0}(\overline{h}(U_0,a_1,\dots,a_n)) \\ &= \mathrm{Disc}_{U_0}\left(\prod_{x\in V(\mathcal{I}_W)}(U_0-t(x))\right)\neq 0.\end{aligned}$$

这恰好意味着 t 在 $V(\mathcal{I}_W)$ 上是单射，因此 t 是一般分离的。□

换言之，我们可以通过检查 t 是否分离某个特定的特化簇，来判断它是否一般分离。例如，可以使用 [8] 中提出的新算法来完成这项检查。

4.5 关于不同的一般性层级

考虑到前几节中引入的需要避开的不同代数集，我们认为有必要总结一下它们的含义。推论 1 表明，GRUR 可以在 $\mathcal{D}\cup\mathcal{L}\cup\mathcal{W}_\infty\cup\mathcal{S}$ 之外进行特化。

– 在 $\mathcal{D}\cup\mathcal{W}_\infty\cup\mathcal{L}$之外，特化系统中按重数计的根的数量恒定。其数量为 D，即 h_0 的次数；等价地，它是商环 $\mathbb{C}(W)[X]/\mathcal{I}_W$ 作为 $\mathbb{C}(W)$-向量空间的维数。– 在 $\mathcal{D}\cup\mathcal{W}_\infty\cup\mathcal{S}\cup\mathcal{L}$ 之外，特化系统中互异根的数量恒定。其数量为 d，即当 t 一般分离时 $\overline{h_0}$ 的次数。

在定理 3 中，我们证明了，如果使用线性代数在商环 $\mathbb{C}(W)[X]/\mathcal{I}_W$中计算 $\mathcal{F}$，那么对于 $\mathcal{W}_\mathcal{G}$ 之外的参数，特化成立。这是商环 $\mathcal{A}_W$ 中的计算能够特化的条件，而算法计算 $\mathcal{F}$的方式只是将它们提升了。

4.6 算法

我们在此提出首个拉斯维加斯算法来计算 $\mathcal{F}$。子算法可在附录中找到。所有计算均使用从集合 $\mathcal{T}:=\{X_1+kX_2+\cdots+k^{n-1}X_n,\ k\in[\![1,D(D-1)/2]\!]\}$ 中选定的一个固定线性形式进行；该集合至少包含一个能够分离 $V(\mathcal{I}_W)$ 的线性形式（参见 [26, 引理 2.1]）。该

所谓的迹向量 VTr 1 指向量 $(\text{Trace}^{\mathcal{A}_W}(p_1)\ ..\ ., \text{Trace}^{\mathcal{A}_W}(p_D))^T$，它后来被证明可以简化某些计算。

算法 1 GRUR-LA

要求：$\mathcal{G}$ 关于 $<_X$ 的约化 Gr¨obner 基 $\mathcal{I}_W$；一组基 $\mathcal{B}_{\mathcal{A}}$ $_W$ 属于 $\mathcal{A}_W$；乘法矩阵 M_{X_1}，...，M_{X_n} 关于 X_1，...，X_n，取自 $\mathcal{A}_W$；MT($\mathcal{A}_W$) 为乘法张量 $\mathcal{A}_W$。

确保：$\mathcal{F} = \{h_0, h_1, h_{X_1}, \ldots, h_{X_n}\}$ 是 $V(\mathcal{I}_W)$的一个一般化有理单变量表示。

步骤 0：计算 VTr 1 迹向量

步骤 1：选择一个尚未选过的线性形式 t，使其属于 $\mathcal{T}$

当 t 不是一般分离的时，执行

$h_0 \leftarrow$ 特征多项式(MT($\mathcal{A}_W$) M_t, VTr 1)

使用 DRR 测试 t 是否分离

如果 t是分离的，则

返回 $\mathcal{F} = \{\chi_t, \chi_t', \text{GRUR 多项式}(h_0, M_{X_1}, \ldots, M_{X_n}, \text{VTr 1})\}$

else

返回步骤 1。

结束 if

结束 while

5 第二种算法：求值／插值方案

5.1 算法介绍

我们在此提出一种用于计算 $\mathcal{F}$ 的第二种算法。原因在于，算法 1 需要计算由 $f_1, \ldots, f_n$ 生成的理想的 Gr¨obner 基。这个 Gr¨obner 基对参数的依赖难以控制，因此参数的次数很可能会急剧增长。此外，计算 t 的特征多项式需要计算 $i \in [\![1, D]\!]$ 的 $\text{Trace}^{\mathcal{A}_W}(t^i)$，其内存占用可能会急剧增大，尽管我们知道最终结果的规模是可控的（参见推论 2 的界）。基于这些原因，我们提出第二种采用求值/插值方案的方法。

下面给出所提出的算法。本节将对每个步骤进行精确研究。

算法 2 *GRUR-EI* 要求：多项式 f_1、...、$f_n \in \mathbb{Q}[W_1,\ldots,W_s,X_1,\ldots,X_n] = \mathbb{Q}[W,X]$ 构成一个一般零维系统，其关于 X 的次数不超过 d_X，关于 W 的次数不超过 d_W。确保：$\mathcal{F} = \{h_0, h_1, h_{X_1},\ldots,h_{X_n}\} \subseteq \mathbb{Q}(W)[T]$ 是 $V(\mathcal{I}_W)$ 的一般化有理单变量表示。步骤 0：计算一个网格 $\mathcal{A} \subseteq \mathbb{Q}^s$，其中至少包含 $((n+1)d_X^n d_W + 1)^s$ 个点 $w \notin (\mathcal{D} \cup \mathcal{L} \cup \mathcal{S})$。步骤 1：选择一个尚未选过的线性形式 $t \in \mathcal{T}$。步骤 2：对每个 $w \in \mathcal{A}$，使用算法 $BlackBoxRUR$ 计算该系统的特化有理单变量表示，并最终检查 t 是否一般分离。如果 t 不是一般分离，则返回步骤 1。结束 if。步骤 3：使用已计算的有理单变量表示插值得到 h_0、h_1、h_{X_1}、...、h_{X_n}。返回 $\mathcal{F} = \{h_0, h_1, h_{X_1},\ldots,h_{X_n}\}$

注 5. 实际上，最好先尝试令 t 为其中一个变量。如果都不行，再从 $\mathcal{T}$ 中选取元素。此外，实验表明，通常只需尝试几次，就能找到一般分离形式。

5.2 GRUR-EI 算法的复杂度分析

步骤 0 的复杂度 由推论 2 可知，GRUR 中多项式关于 W 的次数不超过 $\kappa := (n+1)d_X^n d_W$。因此，我们至少需要 $\binom{\kappa+s}{s} \leqslant (\kappa+1)^s$ 个插值点。我们的思路是估算定义 $\mathcal{D}$、$\mathcal{L}$ 和 $\mathcal{S}$ 的多项式的次数，然后在 $\mathbb{Q}^s$ 中构造一个网格，其中包含足够多的有效插值点。

命题 5 $q = \kappa' + nd_X^{n-1}d_X + nd_W$ $\mathcal{A} = A_{k_0}^s$ $k_0 =$. 令 $\lceil q + \kappa + 1^{\,s}/q^{s-1}\rceil$ $O\,n^s d_X^{2ns} d_W^s$ $\mathbb{Q}$: 。其中 ( ) 的网格由 中的 ( ) 个点构成，且至少包含 $(\kappa+1)^s$ 个值 $w \in \mathbb{Q}^s \backslash (\mathcal{D} \cup \mathcal{L} \cup \mathcal{S})$。

˜ ˜证明。对于 $\mathcal{D}$，我们回顾一下，$\mathcal{D} \subseteq \mathcal{W}_\infty = V(C)$，其中 $C = \mathrm{Res}(F_1,\ldots,F_n)$˜，且 $F_i = F_i(0, X_1,\ldots,X_n)$（见注 4）。因此，只要 $C(w) \neq 0$，在 w 处的特化系统就有有限个解。我们还回顾一下，$\deg_W(C) \leqslant nd_X^{n-1}d_W$。

对于 $\mathcal{L}$，记 $L(W) := \prod_{i=1}^n \mathrm{LT}_{<x}(f_i)(W)$。那么 $\mathcal{L} = V(L)$，并且 L 在 W 中的次数有上界 nd_W。

对于 $\mathcal{S}$，我们写作 $h_0(U_0; W) = \Delta(U_0; W)/p(W)$，其中 $\Delta \in \mathbb{Z}[U_0, W]$ 且 $p \in \mathbb{Z}[W]$。回顾一下，只要 t 一般分离，$\mathcal{S} = V(\text{判别式}_{U_0}(\overline{\Delta}))$。由于 $\deg_W(\Delta) \leqslant \kappa = (n+1)d_X^n d_W$，[27, 命题 8.45] 说明该判别式在 W 中的次数有上界 $\kappa' := 2(n+1)d_X^{2n}d_W$。

现在，为了找到足够多的合适插值点，我们构造一个网格 $A_k \times \cdots \times A_k = A_k^s$，其中 $A_k = [\![1,k]\!]$，并寻找一个值 k_0，使得 $A_{k_0}^s$ 中包含足够多的参数值，且对于这些参数值，$C(W)$、$L(W)$和 $\mathrm{Disc}_{U_0}(\overline{\Delta})(W)$ 均不为零。

其主要依据是 Schwartz-Zippel定理（[32, 命题97，第§12]节）。该定理指出，总次数为 d 的非零多项式 $F \in \mathbb{Q}[X_1, \ldots, X_n]$ 在网格 S^n 上至多有 $d|S|^{n-1}$ 个零点。

这里，我们取 F 为 $\mathrm{Disc}_T(\overline{\Delta}) \cdot C \cdot L \subseteq \mathbb{Z}[W]$，其在 W 中的次数不超过 $\kappa' + nd_X^{n-1}d_W + nd_W$。记 $q := \kappa' + nd_X^{n-1}d_X + nd_W$。我们要找到 $k_0 \geqslant 0$，使得 $|A_{k_0}|^s - q|A_{k_0}|^{s-1} \geqslant (\kappa+1)^s$。考虑 $g\colon\ x \mapsto x^s - qx^{s-1} - (\kappa+1)^s = x^{s-1}(x-q) - (\kappa+1)^s$。显然，对于 $x \in [0, q]$，$g(x) \leqslant 0$，因此 $k_0 \geqslant q$。此外，g 在 $[q, +\infty[$ 上递增。记 x_0 为方程 $g(x) = 0$ 的解。那么对于所有 $x \geqslant x_0$，都有 $g(x) \geqslant 0$。此外，$x_0 > q$，因此 $x_0^{s-1} > q^{s-1}$，进而 $x_0^{s-1}(x_0 - q) = (\kappa+1)^s > q^{s-1}(x_0 - q)$。换言之，我们证明了 $x_0 < q + (\kappa+1)^s/q^{s-1}$，因此选择 $k_0 := \lceil q + (\kappa+1)^s/q^{s-1} \rceil$，其中 $\lceil \cdot \rceil$ 是向上取整函数。就复杂度而言，注意到 $k_0 = O(q) = O(nd_X^{2n}d_W)$。□

步骤 2 的复杂度 首先，我们描述 BlackBoxRUR 算法，并估算其复杂度。

算法 3 BlackBoxRUR

要求：构成零维系统的多项式 $g_1, \ldots, g_n \in \mathbb{Q}[X_1, \ldots, X_n]$，以及一个线性形式 $t \in \mathbb{Q}[X_1, \ldots, X_n]$。

确保：$\mathcal{F} = \{h_0, h_1, h_{X_1}, \ldots, h_{X_n}\} \subseteq \mathbb{Q}[T]$ 是 $V(g_1, \ldots, g_n)$ 的一个有理单变量表示。

步骤 1：计算 $\langle g_1, \ldots, g_n \rangle$ 关于序 $\lrcorner X$ 的 Gröbner 基 $\mathcal{G}$。

步骤 2：计算乘法矩阵 $M_{X_1}, \ldots, M_{X_n}$，对应于乘法商环 $\mathbb{Q}[X]/\langle g_1, \ldots, g_n \rangle$ 中各变量的乘法。

步骤 3：如果 t 分离 $V(g_1, \ldots, g_n)$，则计算 $\mathcal{F}$ 关于 t 的有理单变量表示（RUR）$V(g_1, \ldots, g_n)$ 至 t。

返回 $\mathcal{F}$ 或 "False"

命题 6. 对次数不超过 d 的多项式，调用一次 BlackBoxRUR 至多需要在 $\mathbb{Q}$ 中进行 $\tilde{O}(nd^{3n})$ 次运算。

证明。我们分别研究该算法的每一步。

· 步骤 1：此处的关键要素是我们直接证明的如下引理。我们回顾，若对每个 $i \in [\![2, n]\!]$，g_i 在商环 $\mathbb{Q}[X]/\langle g_1, \ldots, g_{i-1} \rangle$ 中都不是零因子，则族 $g_1, \ldots, g_n$ 是正则序列。

引理 13. 设 $g_1, \ldots, g_n$ 为 $\mathbb{Q}[X_1, \ldots, X_n]$ 中的元素序列，使得 $V(\langle g_1, \ldots, g_n \rangle)$ 为零维。则序列 $g_1, \ldots, g_n$ 是正则的。

证明。为证明这一点，我们使用理想的高度理论（例如参见 [21]）。由于 $\mathbb{Q}[X]$ 是一个 Cohen-Macaulay 环，要证明序列 $g_1, \ldots, g_n$ 是正则的，等价于证明对每个 $i \in [\![1, n]\!]$，都有 $\mathrm{ht}(\langle f_1, \ldots, f_i \rangle) = i$，其中 ht 表示高度。下文中，我们用 $\mathcal{J}_i := \langle g_1, \ldots, g_i \rangle, 1 \leqslant i \leqslant n$ 表示。

设 $\mathfrak{p} \supseteq \mathcal{J}_n$ 是一个素理想。那么我们有

$$\mathrm{ht}(\mathfrak{p}) + \dim_{Krull}\left(\frac{\mathbb{Q}[X]}{\mathfrak{p}}\right) = \dim_{Krull}(\mathbb{Q}[X]) = n \tag{19}$$

其中 $\dim_{Krull}$ 表示 Krull 维数（见 [13, 定理 1.8A]）。由于$\mathfrak{p} \supseteq \mathcal{J}_n$，我们有 $V(\mathfrak{p}) \subseteq V(\mathcal{J}_n)$。于是 $V(\mathfrak{p})$ 也是有限的，因此 $\mathbb{Q}[X]/\mathfrak{p}$的 Krull 维数为零，这意味着方程 (19) 给出 $\mathrm{ht}(\mathfrak{p}) = n$，从而 $\mathrm{ht}(\mathcal{J}_n) = n$。

此外，Krull 主理想定理（见 [21, 定理18 §12]）指出，对每个 $i \in [\![1, n]\!]$, $\mathrm{ht}(\mathcal{J}_i) \leqslant i$。向一个理想添加一个生成元至多使其高度增加 1，因此 $\mathrm{ht}(\mathcal{J}_n) = n$ 迫使这些不等式中的每一个都成为等式。□

在调用 BlackBoxRUR 期间，序列 $g_1, \ldots, g_n$ 满足引理 13 的假设，因此是一个正则序列。作者在 [2, 命题6] 中证明，计算 $\langle g_1, \ldots, g_n\rangle$ 的 Gr¨obner 基的复杂度属于 $O(\binom{n+d_{reg}}{n}^{\omega})$，其中 ω 为线性代数指数。对 d_{reg}的一个常用界是 Macaulay 界 $d_{reg} \leqslant nd - n + 1$。换言之，关于序 $<_X$的 $\langle g_1, \ldots, g_n\rangle$ 的 Gr¨obner 基可在 $\mathbb{Q}$ 中以 $O(\binom{n+d_{reg}}{n}^{\omega}) = O(nd^{wn})$ 次运算计算得到。

· 步骤 2：已知 $\langle g_1, \ldots, g_n\rangle$ 的 Gr¨obner 基后，可以用 $O(nd^{3n})$ 次运算，在 $\mathbb{Q}$ 中计算乘法矩阵 $M_{X_1}, \ldots, M_{X_n}$（参见命题 3.1] [10, ）。

· 步骤 3：此步骤采用 [8, 算法6] 中提出的算法。给定变量 $\mathbb{Q}[X]/\langle g_1, \ldots, g_n\rangle$ 的乘法矩阵 $M_{X_1}, \ldots, M_{X_n}$，以及线性形式 t，该算法将返回 "False"（如果 t 不能分离 $V(\langle g_1, \ldots, g_n\rangle)$），否则将计算关于 t 的根基的一个（约化）有理单变量表示，所需运算次数为 $\tilde{O}(nd^{3n})$，且在 $\mathbb{Q}$ 中进行。将该约化有理单变量表示转换为 $\langle g_1, \ldots, g_n\rangle$ 的有理单变量表示，可以通过将 $V(\sqrt{\langle g_1, \ldots, g_n\rangle})$ 的约化有理单变量表示中的第一个多项式替换为 t 的特征多项式来完成（该特征多项式可用 $\tilde{O}(d^{3n})$ 次运算在 $\mathbb{Q}$ 中计算）。因此，此步骤的总体复杂度为 $\tilde{O}(nd^{3n})$。

因此，BlackBoxRUR 算法的总体复杂度为 $\tilde{O}(nd^{3n})$。□

推论 6。GRUR-EI 算法中的步骤 2 需要在 $\mathbb{Q}$ 中进行 $\tilde{O}(n^{s+2}d_X^{2ns+3n}d_W^s(d_X^{2n} + d_W^s))$ 次运算。

证明。对于参数 $w \in \mathcal{A}$ 的每个取值，我们希望将 f_i's 特化为 w。一次特化可使用 $O(nd_W^s d_X^n)$ 完成。事实上，每个 f_i 都可以写成 $f_i = \sum_{|\alpha| \leqslant d_X} c_{i,\alpha} X^\alpha$，其中 $c_{i,\alpha} \in \mathbb{Q}[W]$，且 $\deg_W(c_{i,\alpha}) \leqslant d_W$。通过按次数递增的顺序依次计算，可以使用 $\binom{d_W+s}{s}$ 次运算在 $\mathbb{Q}$ 中计算出 W 中所有次数小于或等于 d_W 的单项式。由于每个 f_i 在 X 中至多由 $\binom{d_X+n}{n}$ 个单项式构成，计算 $f_1(w, X) \ldots, f_n(w, X)$ 所需的运算总数为 $O(n\binom{d_W+s}{s}\binom{d_X+n}{n}) = O(nd_W^s d_X^n)$。

我们最多需要进行 $\binom{\kappa+s}{s}+(\kappa'+nd_X^{n-1}d_W+nd_W)k_0^{s-1} = O(n^s d_X^{2ns} d_W^s)$ 次求值。因此，这些求值的总成本为 $O(n^{s+1}d_X^{2ns+n}d_W^{2s})$。

然后，对于这些特化系统中的每一个，我们使用 BlackBoxRUR 算法，在 $\mathbb{Q}$ 中执行 $\tilde{O}(nd_X^{3n})$ 次额外运算。计算所有特化有理单变量表示需要在 $\mathbb{Q}$ 中进行 $\tilde{O}(n^{s+1}d_X^{2ns+3n}d_W^s)$ 次运算。对所有系统进行求值并为每个值 $w \in \mathcal{A}$ 使用黑盒的成本，因此最多需要在 $\mathbb{Q}$ 中进行 $\tilde{O}(n^{s+1}d_X^{2ns+n}d_W^s(d_X^{2n}+d_W^s))$ 次运算。

现在，步骤 2 的这一部分会一直运行，直到找到一种一般分离形式。用于选择候选项的集合 $\mathcal{T}$ 的大小至多为 $nd_X^n(d_X-1) = O(nd_X^{2n})$，并且保证至少包含一种一般分离形式，因此前面的计算至多执行 $O(nd_X^{2n})$ 次。最终复杂度为 $\tilde{O}(n^{s+2}d_X^{2ns+3n}d_W^s(d_X^{2n}+d_W^s))$。□

注 6。Schwartz 和 Zippel 的结果保证，在网格 $\mathcal{A}$ 上，至多有 $\kappa' k_0^{s-1}$ 个点使得判别式 $U_0(\overline{h}_0)$ 为零。如果在步骤 2 的计算过程中，BlackBoxRUR 返回“False”的次数超过 $\kappa' k_0^{s-1}$ 次，那么我们就知道判别式 $_{U_0}\,\overline{h}_0$ 恒等于零。在这种情况下，t 不是一般分离形式，GRUR-EI 算法应返回步骤 1。

步骤 3 的复杂度 我们用 $I(n,d)$ 表示在 $\mathbb{Q}$ 中，对 n 个变量、总次数为 d 的多项式根据其在 $\binom{d+n}{n}$ 个点上的取值进行插值所需运算次数的上界。

命题 7. GRUR-EI 算法的步骤 3 在 $\mathbb{Q}$中需要 $O(nd_X^n I(\kappa,s))$ 次运算。

证明. 我们需要对 h_0 的 $2(D+1)$ 个分子和分母，以及 $h_1, h_{X_1}, \ldots, h_{X_n}$ 的 $2(n+1)D$ 个分子和分母进行插值。它们的 W 次数都不超过 κ。这意味着插值部分在 $\mathbb{Q}$中需要 $O(nd_X^n I(\kappa,s))$ 次运算。□

总体复杂度 我们将复杂度结果总结为以下定理。

定理 4. 在 GRUR-EI 算法中，

– 求值部分在 $\mathbb{Q}$中至多需要 $\tilde{O}(n^{s+2}d_X^{2ns+3n}d_W^s(d_X^{2n}+d_W^s))$ 次运算；– 插值部分在 $\mathbb{Q}$中至多需要 $O(nd_X^n I(\kappa,s))$ 次运算。

因此，GRUR-EI 算法可以使用 $\tilde{O}(n^{s+2}d_X^{2ns+3n}d_W^s(d_X^{2n}+d_W^s)+nd_X^n I(\kappa,s))$ 次运算在 $\mathbb{Q}$ 中执行。

现在，我们可以利用已知的插值复杂度给出更精确的表达式。

推论 7。GRUR-EI 算法至多可以使用

$$\tilde{O}(sn^{2s+2}d_X^{2ns+2n}d_W^{2s+1}+n^{s+1}d_X^{2ns+5n}d_W^s)$$

$\mathbb{Q}$中的运算。

证明。 [15] 中提出的算法允许对一个含有 n 个变量、总次数为 d 且至多有 θ 项的多项式进行插值，所需算术运算次数为 $O(dn\log_2(n)\theta M(\theta)\log_2(\theta))$。这里，$M(\theta)$ 是两个次数小于 θ 的一元多项式相乘的复杂度上界。我们可以采用经典的 Sch¨onhage 界，即 $M(\theta) = O(\theta\log_2(\theta)\log_2\log_2(\theta))$。在我们的情形下，$d \leqslant \kappa$ 且 $\theta \leqslant (\kappa+1)^s$；按照我们的记号，单次插值的代价为 $I(\kappa,s) = \tilde{O}(sn^{2s+1}d_X^{2ns+n}d_W^{2s+1})$ 次算术运算。将其代入定理 4 中得到的复杂度，我们可知，GRUR 多项式可以通过 $\tilde{O}\left(sn^{2s+2}d_X^{2ns+2n}d_W^{2s+1}\right)$ 次运算在 $\mathbb{Q}$ 中计算得到。□

5.3 实根分类

该问题在于寻找描述半代数集 $\mathcal{S}_1$、……、$\mathcal{S}_l \subseteq \mathbb{R}^s$ 的多项式公式，使得它们的并集在 $\mathbb{R}^s$ 中稠密，并且在每个半代数集上方，特化系统具有恒定数量的实根。除此之外，我们还希望能够计算出这些连通分支中的每个分支上的一个点。

在 [18], 中，作者通过计算参数化 Hermite 矩阵来处理这一问题，即矩阵 $\mathcal{H} := \left(\text{迹}^{\mathcal{A}_W}(p_ip_j)\right)_{1\leqslant i,\ j\leqslant D}$ 其中我们回顾一下，$\mathcal{B} = \{[p_1]_{\mathcal{A}_W},\ldots,[p_D]_{\mathcal{A}_W}\}$ 是 $\mathcal{A}_W$ 的一个基。作者证明，可以通过 Hermite 矩阵的主子式描述所寻找的半代数集，因为这些主子式编码了使 $\mathcal{H}$ 的符号差发生变化的参数值（从而也编码了不同实根数量发生变化的参数值）。他们的算法具有一般性，并证明其复杂度至多为 $\tilde{O}\left(\binom{s+\mathfrak{D}}{s}2^{3s}n^{2s+1}d^{3ns+2(n+s)+1}\right)$，其中 d 是方程的总次数，且 $\mathfrak{D} = n(d-1)d^n$。为达到这一复杂度，作者对针对块序 $<_{X,\ W}$ 计算出的 Gröbner 基作出了一些假设 ¨，这些假设能够很好地控制在计算 $\mathcal{H}$ 期间参数次数可能出现的爆炸（见 [18, 假设 B 和 C]）。这里我们提出一种一般方法，其估计复杂度更高，但不依赖于这些假设。

描述半代数集 $\mathcal{S}_1,\ldots,\mathcal{S}_l$ 的公式可以通过计算 Sturm-Habicht（或 Sylvester-Habicht）序列，或者更确切地说，通过计算该序列的首项系数得出。我们采用 [27, Notation 4.21] 中给出的定义，而我们的主要工具将是 [12, Theorem 3]，用于计算该系统的实根个数。给定 $\mathbb{A}$ 一个环以及 $P,Q \in \mathbb{A}[U_0]$，用 $\text{sres}(P,Q)$ 表示 P 和 Q 的带符号子结式序列。P 的 Sturm-Habicht 序列由 $\text{sres}(P,P')$ 给出。

$\mathcal{F} = \{h_0,h_1,h_{X_1},\ldots,X_n\}$ 构成 $V(\mathcal{I}_W)$ 的一般化有理单变量表示这一事实，可以改述为：对于几乎所有 $w \in \mathbb{C}^s$，代数集之间的态射

$$\begin{aligned}\Psi_w\ :\ V(\phi_w(h_0)) &\longrightarrow V(\mathcal{I}(w))\\ y &\longmapsto \left(\frac{\phi_w(h_{X_1})(y)}{\phi_w(h_1)(y)},\ldots,\frac{\phi_w(h_{X_n})(y)}{\phi_w(h_1)(y)}\right)\end{aligned}$$

保持重数不变，同时也保持实根的数量。换句话说，$V(\mathcal{I}(w))$ 的实根数量恰好等于 $\phi_w(h_0)$ 的实根数量 =

$\chi^{\mathcal{I}(w)}$。我们回顾一下， h_0 可以表示为 $h_0 = \Delta/P$ 的形式计算，其中 $\Delta \in \mathbb{Z}[W][U_0]$ 且 $P \in \mathbb{Z}[W]$。 h_0的实根数量与 Δ的实根数量相同。

由于 $\phi_w(\Delta)$ 是一元多项式， [12, 定理 3] 保证其实根的个数等于关于变量 U_0 计算得到的序列 sres(Δ) $\phi_w(\Delta)\phi_w(\Delta)'$) 中符号变化的次数（见 [12, §1]）。使用子结式的一大优势在于，它们具有非常好的特化性质。事实上，对于每个 $w \in \mathbb{C}^s$，只要 Δ 在 U_0 中的首系数在 w 处不为零，Sturm-Habicht 序列就具有如下特化性质：$\phi_w\big(\text{sres}(\Delta, \Delta')\big) = \text{sres}\big(\phi_w(\Delta)\ \phi_w(\Delta)'\big)$。

Sturm-Habicht 序列 sres(Δ, Δ') 由有理数域上的多项式构成，这些多项式描述了半代数集 $\mathcal{S}_1, \ldots, \mathcal{S}_l \subseteq \mathbb{R}^s$，在这些集合上， $V(\mathcal{I}(w))$ 的实根个数保持不变。被排除的参数值是 GRUR 无法特化的那些值，也就是属于 $\mathcal{D} \cup \mathcal{L} \cup \mathcal{W}_\infty \cup \mathcal{S}$ 的值（见推论 1），以及 Δ 的首系数为零时对应的值。这些代数集的并集是零测集，因此这些 S_i 的并集确实在 $\mathbb{R}^s$ 中稠密。由此得到以下算法，其复杂度将在命题 8 中研究。

算法 4 实根分类

要求：多项式 $f_1, \ldots, f_n \in \mathbb{Z}[W, X]$，它们生成一个泛型零维的理想 $\mathcal{I}$。

确保：多项式 P_1、.....、 $P_D \in \mathbb{Z}[W]$ 是半代数集的公式，用于求解实根分类问题，且每个集合中至少包含一个点。

步骤 1：用 $h_0 = \Delta/P$ 计算 $V(\mathcal{I}_W)$ 的一个 GRUR $\mathcal{F} = \{h_0, h_1, h_{X_1}, \ldots, h_{X_n}\}$。

步骤 2：计算子结式序列 $\text{sres}(\Delta, \Delta') = \{P_1, \ldots, P_D\}$。

步骤 3：计算一个集合 $\mathcal{P}$，其中每个连通分支至少包含一个点，该集合属于半代数集 $\mathbb{Q} = \{P_1 \neq 0, \ldots, P_D \neq 0\}$。

返回 $P_1, \ldots, P_D$ 和 $\mathcal{P}$

命题 8. 给定生成一个泛型零维理想 $\mathcal{I}$ 的多项式 $f_1, .., f_n \in \mathbb{Z}[W, X]$，算法 5.3 可解决实根分类问题，且最多可使用

$$\tilde{O}\big(2^{6s+1} n^{3s+1} d_X^{7ns+3n} d_W^{3s+1}\big)$$

在 $\mathbb{Q}$中的运算。

证明。上一小节的讨论表明，我们可以通过至多 $\tilde{O}\big(sn^{2s+2} d_X^{2ns+2n} d_W^{2s+1}\big)$次在 $\mathbb{Q}$ 中的运算，计算出 $V(\mathcal{I}_W)$的 GRUR 的元素。这就是步骤 1 的代价。我们写作 $h_0 = \Delta/P$，其中$\Delta \in \mathbb{Q}[W, T]$ 且 $P \in \mathbb{Q}[W]$。

接下来，我们需要计算 Sturm-Habicht 序列 sres(Δ, Δ')。根据推论 2 中得到的界，我们知道 Δ 的总次数有界

为 $\kappa + d_X^n$，高度有界于 $\tilde{O}\big(nd_X^n\tau + nd_X^n d_W \log_2(s+1)\big)$。其思路是使用二进制分割，将 Δ 和 Δ' 转换为关于 $\mathbb{Z}[Y][T]$ 的多项式，计算转换后多项式的子结式序列，然后使用逆二进制分割恢复 $\mathbb{Z}[W]$ 中的结果。为此，我们需要对预期结果的高度和次数分别给出界。根据 [27, 命题 8.45] ，我们知道 $\mathrm{sres}(\Delta, \Delta')$ 中每个多项式的次数有界于 $\kappa' := 2(n+1)d_X^{2n} d_W$。

环同态 $\Theta\colon\ \mathbb{Z}[W][T] \to \mathbb{Z}[Y][T]$，满足 $W_1 \mapsto Y, W_2 \mapsto Y^{\kappa'+1}, \ldots, W_s \mapsto Y^{\kappa'^{s-1}+1}$，其中 T 是一个新变量。通过计算 $\mathrm{sres}(\Delta, \Delta')$，我们可以得到 $\mathrm{sres}(\Theta(\Delta)\ \Theta(\Delta')) = \Theta(\mathrm{sres}(\Delta, \Delta'))$（例如参见 [9, §3], [16, 定理 3.3]）。由于 Δ 在 W 中的次数有上界 κ，我们知道 $\Theta(\Delta)$ 在 Y 中的次数有上界 $\kappa(\kappa'^{s-1}+1)$，即 $\deg_Y(\Delta) = O(2^{s-1}n^s d_X^{2ns-n} d_W^s)$。根据 [11, 推论 11.18], ，我们可以使用 $\tilde{O}(2^{s-1}n^s d_X^{2ns} d_W^s)$ 次运算，在 $\mathbb{Q}$ 中计算 $\mathrm{sres}(\Theta(\Delta)\ \Theta(\Delta'))$。由此，我们可以解码 $\mathrm{sres}(\Theta(\Delta)\ \Theta(\Delta'))$ 中每个多项式的首项系数，并得到多项式 $P_1, \ldots, P_D \in \mathbb{Z}[W]$。因此，步骤 2 的总开销是在 $\mathbb{Q}$ 中进行 $\tilde{O}(2^{s-1}n^s d_X^{2ns} d_W^s)$ 次运算。

现在， [12, 定理 3] 指出，对于每个参数值 $w \in \mathbb{R}^s$， Δ 的实根数由修正符号变差数给出。当在 w处求值时，某个 P_i 为零，当且仅当该数发生变化。由 $P_1 \neq 0$、.....、 $P_D \neq 0$ 定义的半代数 $\mathcal{Q}$ 具有这样的性质： Δ 的实根数在其每个连通分支上都是常数。

最后一步是实际计算$\mathcal{Q}$的每个连通分支中的一个点。例如，可以使用[18, 推论 3]中提出的概率算法来完成这一任务。后者需要在 $\mathbb{Q}$ 中执行 $\tilde{O}\big(2^{6s+1}n^{3s+1}d_X^{7ns+2n+s}d_W^{3s^2+1}\big)$ 次运算，以计算出 $\mathbb{Q}^s$ 中的至多 $O(4^s n^s d_X^{3ns} d_W^s)$ 个点的集合，并且该集合至少与 $\mathcal{Q}$的每个连通分支相交一次。

整个方法的复杂度主要由最后一步决定。□

注 7。我们只需 h_0 执行算法 5.3。不过，由于整体复杂度由最后一步决定，这并不会改变复杂度上界。

注 8。利用子结式序列中出现的次数的已知上界，可以使用 [19, 算法 4] 中介绍的半 gcd 算法，使步骤 2 的复杂度达到 $\tilde{O}(n^s d_X^{2ns+n} d_W^s)$。不过，由于复杂度主要由最后一步决定，这不会改变整体复杂度。

6 附录

6.1 Stickelberger 定理

为简便起见，我们将这一结果称为 Stickelberger 定理。该定理见 [1, §2.3.1 推论 3.6]。

定理 5（Stickelberger）。设 K为一个域， $\mathcal{I} \subseteq K[X_1, \ldots, X_n]$ 为一个零维理想。设 m_p 为商环 $K[X_1, \ldots, X_n]/\mathcal{I}$中由乘以 p 定义的端同态。则:

– m_p 的特征多项式为$\prod_{x \in V(\mathcal{I})}(T - p(x))^{\mu(x)}$ ； – m_p 的行列式为 $\prod_{x \in V(\mathcal{I})} p(x)^{\mu(x)}$ ； – m_p 的迹为$\sum_{x \in V(\mathcal{I})} \mu(x)p(x)$ ；

其中 $\mu(x)$是 x的重数。

6.2 GRUR-LA 的子算法

算法 5 QuotientBasis

要求： $\mathcal{G}$ 一个 Gr¨obner 基，即 $\mathcal{I}_W$ 关于反向字典序(X)的基。

确保： $\mathcal{B}$ $\mathcal{A}_W$的基。

```
如果 1 可由 G 约化，则返回 ∅
结束如果
B ← {[1]}
L ← [X_1, ..., X_n] ； L' ← [1]
当 L' ≠ ∅ 时
    L' ← ∅
    对于 m ∈ L ，执行
        如果 m 不能被 G 约化，则
            B ← B ∪ {[m]}
            L' ← L' ∪ {m · X_1, ..., m · X_n}
            L ← L'
        结束条件判断
    结束循环
结束 while 循环
返回 B
```

算法 6 MultiplicationMatrices

要求： $\mathcal{G}$ 一个关于 $<_X$ 的 Gr¨obner 基； $B(\mathcal{G})$ 为来自一个基的单项式集合 $\mathcal{B}_{\mathcal{A}_W}$ 属于 $\mathcal{A}_W$。

确保： $\mathcal{A}_W$ 中关于 X_1、...、X_n 的乘法矩阵 M_{X_1}、...、M_{X_n}。

使用 $<_X$ 计算 $M(\mathcal{G})$，并对 $B(\mathcal{G}) \cup M(\mathcal{G})$ 排序。

对于 $m \in B(\mathcal{G}) \cup M(\mathcal{G})$，执行

如果 $m \in B(\mathcal{G})$，则

写作 $m = p_i$，其中 $i \in [\![1, D]\!]$。于是 $\overrightarrow{[m]} \leftarrow [\delta_{l,i},\ 1 \leqslant l \leqslant D]^T$。

结束条件判断

如果 $m = \mathrm{LT}_{<_X}(g)$，其中某个 $g \in \mathcal{G}$ 写作 $g = m + \sum_{l=1}^{D} a_l p_l$，则

$\overrightarrow{[m]} \leftarrow [-a_1, \ldots, -a_D]^T$。

else

写入 $m = X_j m'$，其中 $m' = X_s b$。

对于 $u = 1 \ldots D$，执行

$\overrightarrow{[m]}_u \leftarrow \sum_{v=1}^{D} \overrightarrow{[X_s b]}_v \overrightarrow{[X_j p_v]}_u$.

结束循环

结束条件判断

结束循环

对于 i= 1 . . . n，执行

构建 $M = \left(\overrightarrow{[X_i p_1]} \mid \cdots \mid \overrightarrow{[X_i p_D]}\right)$

结束循环

返回 $M_{X_1}, \ldots, M_{X_n}$

算法 7 乘法张量

要求： $\mathcal{B}$是 $\mathcal{A}_W$和 $M_{X_1}, \ldots, M_{X_n}$的一组基。

确保：乘法张量 MT($\mathcal{A}_W$)。

MT($\mathcal{A}_W$) $\leftarrow \emptyset$

$\mathcal{M} \leftarrow \{p_i p_j,\ 1 \leqslant i, j \leqslant D\}$。

按 $<_X$ 对 $\mathcal{M}$ 排序

对于总次数为 0 或 1 的 $m \in \mathcal{M}$，执行

MT($\mathcal{A}_W$) $\leftarrow$ MT($\mathcal{A}_W$) $\cup [m]$

结束循环

对于总次数大于或等于 2 的 $m \in \mathcal{M}$

写出 $m = X_j m'$，使得 deg(m') < deg(m)

$\overrightarrow{[m]} \leftarrow M_{X_j} \cdot \overrightarrow{[m']}$

MT($\mathcal{A}_W$) $\leftarrow$ MT($\mathcal{A}_W$) $\cup [m]$

结束循环

返回 MT($\mathcal{A}_W$)

算法8 特征多项式

要求：MT ($\mathcal{A}_W$)； M_t 在 $\mathcal{A}_W$ 中的 t 乘法矩阵；VTr1。
确保： χ_t t的特征多项式。
$N_0 \leftarrow D$。
$\overrightarrow{v} \leftarrow [1, 0, \ldots, 0]^T$。
对于 $i = 1, \ldots, D$ **do**
$\overrightarrow{v} \leftarrow M_t \cdot \overrightarrow{v}$。
$N_i \leftarrow$ 迹(t^i) $= \overrightarrow{v}$ ·代数簇Tr(1)。
结束循环
求解三角系统 $\{(D-k)b_k = \sum_{j=0}^{k} b_{k-j} N_j\}_{k \in [\![1, D]\!]}$ 其未知数是 b_k。
返回 $\chi_t = T^D + \sum_{k=0}^{D-1} b_k U_0^{D-k}$。

算法 9 RUR 多项式

要求： $\chi_t = \sum_{i=0}^{D} b_i T^{D-i}$ ； $M_{X_1}, \ldots, M_{X_n}$ 的乘法矩阵 X_1、...、 X_n 位于 $\mathcal{A}_W$； VTr 1。
确保： $h_{X_1}, \ldots, h_{X_n}$。
对于 $i = 1, \ldots, D$ **do**
$H_i(T) \leftarrow \sum_{j=0}^{i} b_j T^{i-j}$.
结束 for
for $k = 1, \ldots, n$ **do**
for $i = 0 \ldots, D-1$ 执行
迹($X_k t^i$) $\leftarrow \overrightarrow{X_k t^i}$ · 代数簇迹 1.
结束循环
$h_{X_k} \leftarrow \frac{\sum_{i=0}^{D-1} \text{迹}(X_k t^i) H_{D-1-i}(T) \partial \chi_t}{\partial T}$.
结束循环
返回 h_{X_1}、.....、 h_{X_n}。

算法 10 SeparationCheck

要求：线性形式 $t = a_1 X_1 + \cdots + a_n X_n \in \mathbb{C}[X]$； χ_t 在 χ_t 中的特征多项式-式 t； $\mathcal{G}$ 对于 $<_X$ 的 $\mathcal{I}_W$ 的一个约化 Gr¨obner 基。
确保：如果 t 是一般分离的，则返回 True，否则返回 False。
计算 Disc(χ_t)
如果 $Disc(\chi_t) = 0$ ，则返回 (False)
结束 if
选择 $w \in \mathbb{C}^s$ ，使得 $w \notin \cup_{g \in \mathcal{G}} V$(首项系数$_{<_X}$)； $V(\mathcal{I}(w))$ 的维数为零，并且判别式(χ_t)(w) $\neq 0$
使用 [8, 算法 6] ，通过 $\mathcal{G}(w)$ 判断 t 是否为分离的
返回给出的答案

参考文献

1. Hans Sterk Arjeh M. Cohen, Hans Cuypers. *Some Tapas of Computer Algebra*。Springer Berlin Heidelberg，https://doi.org/10.1007/978-3-662-03891-8，1999年。 2. Magali Bardet、Jean-Charles Faug`ere 和 Bruno Salvy。半正则二次多项式系统正则度指数的渐近行为。载于 *MEGA 2005 - 8th International Symposium on Effective Methods in Algebraic Geometry*，第 1–17 页，意大利撒丁岛阿尔盖罗波尔图孔特，2005年5月。 3. John Canny。广义特征多项式。*Journal of Symbolic Computation* 9 3 241 250, 1990 ，( )：–。计算代数复杂性专题编辑。 4. George E. Collins。通过柱面代数分解对实闭域进行量词消去。载于 H. Brakhage 编，《*Automata Theory and Formal Languages* 134 183, 1975 》，第 – 页，柏林、海德堡，。Springer Berlin Heidelberg。 5. Carlos D'Andrea、Teresa Krick 和 Martin Sombra。多射影空间中簇的高度与算术零点定理，2012年。 6. James H. Davenport 和 Joos Heintz。实数上的量词消去是双指数级的。 *Journal of Symbolic Computation*，5(1)：29–35，1988年。 7. Donal O'Shea David A. Cox, John Little。《 *Using Algebraic Geometry*》。《数学研究生教材》。Springer New York, NY，https://doi.org/10 138611，2005 1007. /b。 8. Alexander Demin、Fabrice Rouillier 和 Joao Ruiz。基于字典序 Groebner 基读取有理单变量表示，2025年。 9. Dimitrios I. Diochnos、Ioannis Z. Emiris 和 Elias P. Tsigaridas。实数域上求解二元系统的渐近复杂度与实际复杂度。*Journal of Symbolic Computation* 44 7 818 835, 2009 ，( )：–，7月。

10. J.C. Faug`ere 、 P. Gianni 、 D. Lazard 和 T. Mora。通过序变换高效计算零维 Gröbner 基。{ }, *Journal of Symbolic Computation* 16 4 329 344, 1993 ( )：–。 11. Joachim Von Zur Gathen 和 Jurgen Gerhard。《 *Modern Computer Algebra*》。Cambridge University Press，美国，第 2 版，2003年。 12. L. Gonzalez、H. Lombardi、T. Recio 和 M.-F. Roy。Sturm-Habicht 序列。载于 *Proceedings of the ACM-SIGSAM 1989 International Symposium on Symbolic and Algebraic Computation* 89, 136 146, 1989 ，ISSAC '，第 – 页，纽约，NY，美国，。计算机协会。 13. Robin Hartshorne。《*Algebraic Geometry*》。Springer New York, NY，https://doi.org/10.1007/978-1-4757-3849-0，第 1 版，1977年。 14. J.P Jouanolou。结式的形式体系。 *Advances in Mathematics*，90(2)：117–263，1991年。 15. Erich Kaltofen 和 Lakshman Yagati。改进的稀疏多元多项式插值算法。载于 P. Gianni 编，《 *Symbolic and Algebraic Computation*》，第 467–474 页，柏林、海德堡，1989年。S pringer Berlin Heidelberg。 16. J. Klose。多元多项式的二进制分割。 *Journal of Complexity*，11 3 330( )：–343，1995年。 17. Daniel Lazard 和 Fabrice Rouillier。求解参数多项式系统。*Journal of Symbolic J.* , ( )：–。*Symb. Comput.* 42 6 636 667, 2007

18. Huu Phuoc Le 和 Mohab Safey El Din。通过埃尔米特矩阵求解实数域上的参数多项式方程组。*Computation* 112 25 61, 2022 ，：–。

19. Gr´egoire Lecerf。Lickteig-Roy 次结式算法的复杂度。*Journal of Symbolic Computation*，92：243–268，2019年。

20. F. S. Macaulay。消元中的一些公式。 *Proceedings of The London Mathematical Society* 3 27, 1902 ，第 – 页。 21. Hideyuki Matsumura。《 *Commutative Algebra* 56 *Math Lecture Notes*》，第 卷，。 *Series* 1980 Benjamin/Cummings Publishing Company，。 22. Alexander P. Morgan。避免多项式系统无穷远解的一种变换。 *Applied Mathematics and Computation*，18(1)：77–86，1986年。 23. Guillaume Moroz。参数多项式方程与不等式系统的求解复杂度。研究报告 RR-5929，INRIA，2006年。 24. Masayuki Noro 和 Kazuhiro Yokoyama。计算零维理想有理单变量表示的模方法。 *Journal of Symbolic Computation* 28 1 243 263, 1999 ，( )：–。 25. James Renegar。实数一阶理论的计算复杂度与几何。第一部分：引言、预备知识、半代数集的几何、实数存在理论的判定问题。 *Journal of Symbolic Computation* 13 3 255 299, 1992 ，( )：–。 26. Fabrice Rouillier。通过有理单变量表示求解零维多项式系统。研究报告 RR-3426，INRIA，1998年。 27. Marie-Fran ¸ *Algorithms in Real Algebraic Geometry* 2006 coise Roy Saugata Basu, Richard Pollack。{ }。Springer Berlin Heidelberg，。 28. ´Eric Schost。《 *Sur la résolution des systèmes polynomiaux à paramètres*》。博士论文，2001年。 29. ´Eric Schost。计算参数几何消解。 *Applicable Algebra in Engineering Communication and Computing* 13 5 349 393, 2003 ，，( )：–。 30. B. L. Waerden。《 *Moderne Algebra*》，第 2 卷。Springer Berlin Heidelberg，1931年。 31. Volker Weispfenning。综合 Gro ¨ 14 1 1 30, obner 基。 1992 *J. Symb. Comput.*，( )：–。 32. Richard Zippel。《 *Effective Polynomial Computation*》。Springer New York, NY，https://doi.org/10.1007/978-1-4615-3188-3，2012年。