# 面向只读代数分支程序无序确定性黑盒多项式恒等式测试的代数刚性框架

Shalender Singh*[1], Vishnupriya Singh[2]

**摘要**

对于只读一次无关代数分支程序，确定性黑盒多项式恒等式测试（PIT）是代数复杂性中的一个核心开放问题，尤其是在缺少变量排序信息的情况下。以往的确定性算法要么依赖顺序信息，要么因采用组合隔离技术而产生显著开销。

本文基于相关矩阵字代数的内部结构，为只读代数分支程序提出了一种代数刚性框架。我们证明，非零宽度为$w$ 的只读代数分支程序所诱导的字代数，其有效代数自由度会塌缩至至多为$w^2$维，且与变量数量无关。这种刚性使我们能够通过内在代数不变量确定性地构造见证，从而绕过以往工作中使用的秩集中、隔离引理和概率工具。

因此，我们得到了首个面向只读代数分支程序的无序确定性黑盒多项式恒等式测试算法，其运行时间为准多项式时间 $n \cdot (wd)^{O(w^2)}$。这表明，仅凭代数刚性就足以对该模型中的多项式恒等式测试进行去随机化，而无需假设存在排序信息。

该框架进一步明确了实现完全多项式时间复杂度所剩的唯一障碍。我们提出模稳定性猜想，断言一旦模数超过关于 $w$ 和单变量次数的多项式阈值，宽度为-$w$ 的只读代数分支程序在哈希到循环商环 $\mathbb{K}[\lambda]/\lambda^r - 1$ 后便保持稳定。该猜想自然源于刚性所揭示的低维系数结构，并得到大量实验证据的支持。

在该猜想成立的前提下，我们的方法可得出一个针对只读代数分支程序的完全多项式时间确定性黑盒多项式恒等式检验算法，其复杂度与已知最佳白盒算法相当，并将黑盒问题归结为一个具体的代数稳定性问题。

## 1. 引言

多项式恒等式测试（PIT）是一个算法问题，旨在判定给定的算术电路是否计算出零多项式。随机化多项式恒等式测试可追溯至 DeMillo–Lipton 和 Schwartz–Zippel 的早期工作；他们证明，次数有界的非零多项式在有限求值集 [l–3] 上不可能于过大比例的点处取零。尽管受限模型已取得数十年的进展，一般电路的确定性多项式恒等式测试仍是代数复杂性理论中的核心开放问题之一。多项式恒等式测试的重要性还源于其与电路下界的深刻联系：针对一般算术电路的多项式时间确定性多项式恒等式测试，将带来重要的下界推论（尤其是 Kabanets–Impagliazzo 定理及其推广）[4,5]。Shpilka–Yehudayoff 和 Saxena 的综述提供了更广泛的背景，包括命中集、生成元和结构限制在去随机化中的作用 [6,7]。

一种特别结构化且研究充分的多项式恒等性检验模型是**只读一次无关代数分支程序**（ROABP）类。ROABP 描述了一种自然的分层计算：变量按固定顺序读取，且每个变量恰好出现在一层中。在白盒模型中，

借助对代数分支程序及相关只读一次模型的代数刻画和线性代数刻画，已知存在多项式时间多项式恒等式检验方法（例如，针对代数分支程序的经典 Raz–Shpilka 方法及其后续改进；综述见 [6,8]）。在黑盒设置中，过去十年间，针对只读代数分支程序的确定性多项式恒等式测试取得了长足进展，推动这一进展的是一系列技术，包括秩／求值维数度量，移位后的秩集中，以及基隔离权重赋值。Forbes–Shpilka 首次为已知变量顺序的只读代数分支程序构造出准多项式规模的黑盒命中集，并在有界宽度情形下取得了更强的界 [9]。Forbes–Saptharishi–Shpilka 为多线性只读一次代数分支程序开发了伪随机性和命中集，即使变量顺序可能变化也适用，为迈向“任意顺序”情形迈出了关键一步 [10]。Agrawal–Gurjar–Korwar–Saxena 提出了基隔离技术，为未知顺序只读代数分支程序实现了准多项式时间黑盒多项式恒等性检验，并将该方法与稳健的“低支撑集中”观点联系起来 [11,12]。后续研究还针对特殊情形（例如常数宽度、交换／结构化变体）进行了进一步改进，包括常数宽度及相关顺序／结构限制下的改进构造 [13]。较新的论文继续改进只读代数分支程序及相关代数分支程序模型的显式命中集，并阐明相邻模型中的结构障碍和下界现象（例如，改进的显式命中集 [14], 、针对只读代数分支程序和常数宽度只读代数分支程序的轨道命中框架 [15–17], ，以及只读代数分支程序之和的新指数下界 [18]）。此外，近期研究还探讨了与只读代数分支程序变量顺序相关的困难性和等价性测试问题，凸显了顺序现象本质上具有内在性，而非技术性产物 [19]。

尽管取得了这些进展，现有的只读代数分支程序去随机化范式总体上仍带有**组合—插值**的特点：它们通过哈希、移位或权重赋值来隔离系数，再利用低支撑集中或偏导数维数论证进行重构 [9–14]。这些方法功能强大，但并未明确利用底层**矩阵乘积计算**更深层的代数结构。在只读代数分支程序中，每一层都会贡献一个多项式矩阵，而计算所得多项式是最终乘积中指定的一个元素。这表明，恒等式测试或许不仅能通过系数隔离来实现，还可以利用由系数矩阵生成的矩阵代数的刚性来实现。

本文工作提出了一种用于只读代数分支程序确定性多项式恒等式检验的新型代数刚性框架，其核心是由程序的系数矩阵生成的**矩阵词代数**。具体而言，宽度为 $w$ 的只读代数分支程序自然会导出 $\mathrm{Mat}_w(\mathbb{K})$ 的一个有限生成子代数（即由其层系数矩阵生成的代数）。我们证明，在适当的乘法特化下，这个代数必然呈现刚性二分：它要么坍缩为与零计算相符的退化代数，要么成为全矩阵代数 $\mathrm{Mat}_w(\mathbb{K})$。在全代数情形下，非零性有一个明确的代数见证，可表述为行列式条件（“满秩见证”），从而将多项式恒等式检验转化为检测某个非零结构化多项式。

一个关键的结构性推论是**有效的低支撑生成原理**：尽管只读代数分支程序可能依赖于$n$个变量，但在我们的特化下，可以迫使它生成的全矩阵代数仅由$O(w^2)$个有效变量方向生成，从而将恒等式测试归约为一个有界支撑重构问题。为了以算法方式实现这一方法，我们需要能够从矩阵代数中提取代数见证、且不依赖非构造性谱论论证的工具。因此，我们提出一种**无特征值（有理）投影算子提取机制**，将凯莱–哈密顿定理与矩阵多项式恒等式（尤其是阿米楚尔–列维茨基恒等式）结合起来[20,21]。该机制提供了一种规范的方法，仅通过多项式运算即可分离出秩一矩阵方向（进而见证全矩阵代数的生成）。

最后，该方法必须确保构造所需的所有代数非退化条件——活跃块的泛性、投影算子子式的非零性、秩分离

约束以及次数三角化不等式——在单一显式特化下同时成立。我们不隐式地确定这种特化，也不依赖概率论证，而是通过显式的**有限多项式避零**策略，以确定性方式进行。构造中的每一种潜在失效模式，都被编码为某个具体代数约束多项式的消失；第4–6节为所有此类约束建立了统一的次数界，且该界与最终编码中所用的曲线参数无关。随后，通用并集策略将这些约束汇总为一个总次数受控的单一避开条件。通过确定性地搜索一个规模超过此界的有限域，我们保证存在一个不属于公共零点集的特化，从而确保所有代数要求同时得到满足。

至关重要的是，这一步避零并非对前文所建立的结构分析的替代，而是对其最终的整合。约束多项式本身源自矩阵词代数的内在性质——其韦德伯恩–伯恩赛德块结构、简单分量的刚性，以及无特征值投影算子提取机制。有限搜索所做的只是验证：这些代数性质能够以具体且无随机性的方式实现。尽管“有限检验蕴含全局正确性”这一相关范式也出现在确定性素性测试及其他去随机化结果中 [22], ，本文的应用却要复杂得多，涉及非交换代数结构、模分解和次数敏感消元，其复杂程度远超该领域中出现的数论恒等式。在这里，有限多项式避零充当一种统一工具，将深层代数结构转化为显式的确定性命中集。

**结果概述**。
本文建立了两个层次的结果。首先，我们基于矩阵词代数刚性，给出一个无条件的确定性黑盒多项式恒等式检验框架，其运行时间关于 n 为多项式级、关于宽度 w 为拟多项式级。其次，在假设模稳定性猜想（猜想 4.7）成立的条件下，同一框架可导出一个完全多项式时间的确定性黑盒多项式恒等式检验算法。

**主要贡献**。

除针对宽度有界的只读代数分支程序设计确定性多项式恒等式检验算法外，本文工作还在代数复杂性领域发展了若干具有独立研究价值的结构工具：

1. 针对由代数程序生成的矩阵字代数建立刚性理论，将韦德伯恩–伯恩赛德结构与特化下的稳定性相结合。2. 提出一种有效的秩集中原理，表明非零只读代数分支程序计算至多归约为$w^2$ 个代数方向。3. 提出一种无特征值（有理数）方法，仅利用多项式恒等式和幂等元提升来提取秩一投影算子。4. 提出一种次数三角化技术，确保首项唯一，并防止曲线代入时发生消去。5. 提出一种通用的有限避开框架，将所有代数非退化约束汇总为一个有界次数条件，从而无需进行结构性分类讨论即可得到显式确定性命中集。

## 2. 预备知识与定义

全文中，设$\mathbb{K}$ 表示一个代数闭域，其特征为零或严格大于$2w$。所有多项式和矩阵均取自$\mathbb{K}$。

### 2.1 只读一次无关代数分支程序（ROABP）

一个宽度为$w$、变量为$x_1, \dots, x_n$ 的**只读代数分支程序（ROABP）**是一个具有$n+1$ 层的分层有向无环图，其中：

- 每一层 $i$ 最多有 $w$ 个节点，
- $i-1$ $i$ $x_i$ 层
- 与层之间的边标记为关于 的一元多项式。计算按固定变量顺序 $x_1$、…、 $x_n$进行。

等价地，ROABP 计算如下形式的多项式：

$$C(x_1, \dots, x_n) = e_1^\top \prod_{i=1}^{n} A_i\,(x_i)\; e_w,$$

其中：

- $A_i(x_i)$ ∈ 矩阵$_w(\mathbb{K}[x_i])$，
- $e_1$、 $e_w \in \mathbb{K}^w$ 为首个和最后一个标准基向量。

每个矩阵多项式可展开为

$$A_i(x_i) = \sum_{j=0}^{d} A_{i,j}\; x_i^j,$$

其中 $d$ 是单变量次数上界，且 $A_{i,j}$ ∈Mat$_w(\mathbb{K})$。

### 2.2 矩阵词代数

ROABP 的系数矩阵生成一个非交换代数。

定义 *2.1*（矩阵词代数）

令 B $= \mathbb{K}\langle A_{i,j} : 1 \le i \le n, 0 \le j \le d \rangle \subseteq$ Mat$_w(\mathbb{K})$ 表示由所有 ROABP 系数矩阵生成的矩阵词代数。B 中的元素是矩阵词$A_{i_1\, j_1} A_{i_2\, j_2} \cdots A_{i_k\, j_k}$ $X \mapsto$ ,,, $e_1^\top X e_w$ 的有限线性组合。当且仅当双线性泛函在 B 中的所有矩阵词上均为零时，ROABP 计算出的就是零多项式。

### 2.3 特征标与乘法特化

为分析 B 的结构，我们引入乘法特征替换。

定义 *2.2*（乘法特征）

乘法特征是一个映射 $\chi: x_i \mapsto \omega^{t_i}$，其中 $\omega$ 是单位根，且 $t_i \in \mathbb{Z}$。在这种特化下，每个矩阵多项式都会取值为一个数值矩阵：

$$A_i(\chi) = \sum_{j=0}^{d} A_{i,j}\; \omega^{j t_i}.$$

这会诱导出一个特化矩阵字代数 $\mathrm{B}(\chi) = \mathbb{K}A_i(\chi) \subseteq \mathrm{Mat}_w(\mathbb{K})$。

### 2.4 $\mathbf{Mat}_w$（$\mathbb{K}$）的代数结构

我们将使用两个描述全矩阵代数的经典多项式恒等式。

定理 *2.3*（凯莱–哈密顿）

每个矩阵 $X \in \mathrm{Mat}_w(\mathbb{K})$ 都满足其特征多项式：$X^w + c_{w-1}X^{w-1} + \cdots + c_0 I = 0$。

定理 *2.4*（*Amitsur–Levitzki*）

代数 $\mathrm{Mat}_w(\mathbb{K})$ 满足次数为 $2w$ 的标准多项式恒等式：

$$\sum_{\sigma \in S_{2w}} \operatorname{sgn}(\sigma) X_{\sigma(1)} X_{\sigma(2)} \cdots X_{\sigma(2w)} = 0.$$

这些恒等式对长矩阵字的行为施加了严格约束，并将用于控制代数依赖关系。

### 2.5 行列式、伴随矩阵与投影算子

对于方阵 $X$，记：

- $\det(X)$ 表示其行列式，
- $\operatorname{adj}(X)$ 表示其伴随矩阵。

回顾恒等式：$X \cdot \operatorname{adj}(X) = \det(X)\, I$。若 $\mu$ 是 $X$的单特征值，则 $\operatorname{adj}(\mu I - X)$ 的秩为一，并定义了一个秩一特征投影算子，将向量投影到相应的特征子空间上。我们将利用判别式和结式构造此类投影算子，而不进行除法，也不显式提取特征值。

### 2.6 代数曲线与克罗内克代换

本文工作中的一个核心技术手段是沿一元代数曲线进行代入。

定义 *2.5*（曲线代入）

固定互不相同的常数 $\alpha_1$、…、 $\alpha_n \in \mathbb{K}$，以及一个较大的整数 $B$。定义 $x_i = (\lambda + \alpha_i)^B$。

这种代入确保了次数分离：指数模式不同的单项式会映射为 $\lambda$ 中次数各不相同的一元单项式，从而避免消去。

这是一种**克罗内克代换**，经过调整以控制结构化矩阵词表达式。

### 2.7 有限多项式避零

我们将反复使用以下基本的代数原理。

引理 *2.6*（有限多项式避零）

设 $f_1(\lambda)$、……、 $f_R(\lambda) \in \mathbb{K}[\lambda]$ 均为非零多项式。那么，它们的乘积

$$f(\lambda) = \prod_{i=1}^{R} f_i(\lambda)$$

在 $\mathbb{K}$ 中至多有 $\deg(f)$ 个根。因此，任何满足 $|L| > \deg(f)$ 的集合 $L \subseteq \mathbb{K}$ 都包含一点 $\lambda^\star$，使得对于所有 $i$，$f_i(\lambda^\star) \neq 0$。该引理以显式有限消去取代随机性。

### 2.8 记号约定

- $w$ 表示 ROABP 宽度。
- $d$ 表示个别次数上界。
- $n$ 表示变量的数量。
- B 表示矩阵词代数。
- $\chi$ 表示乘法特征专门化。
- $\lambda$ 表示曲线参数。大 O 界隐藏绝对常数，但不隐藏关于 $w$ 和 $d$ 的多项式依赖。

## 3. 矩阵词代数刚性

在本节中，我们分析由 ROABP 系数矩阵生成的代数，并确立一种推动证明其余部分的刚性现象。

### 3.1 矩阵词代数

回顾一下，宽度为 $w$ 的只读代数分支程序定义了矩阵词代数

$$\mathcal{B} = \mathbb{K}\langle A_{i,j} : 1 \le i \le n, 0 \le j \le d \rangle \subseteq \mathrm{Mat}_w(\mathbb{K}).$$

这是 $\mathbb{K}$ 上的有限维非交换代数。
计算所得多项式恒为零，当且仅当双线性泛函 $X \mapsto e_1^\top X e_w$ 在 B 的所有元素上取零值。

### 3.2 特化后的活跃单块

现在，我们用对特化矩阵字代数的精确结构刻画，取代不正确的“完整矩阵二分”。关键在于，尽管该代数未必等于全矩阵代数，**任何非零的 ROABP 计算都必须在其半单商的至少一个简单矩阵块中存续**。

Let 令 $\mathrm{B}(\chi) \subseteq \mathrm{Mat}_w(\mathbb{K})$ 表示乘法特化后的矩阵字代数 .

引理 *3.1*（活跃简单商块的存在性）

令 $J = J(\mathrm{B}(\chi))$ 表示 $\mathrm{B}(\chi)$ 的雅各布森根。那么半单商 $\mathrm{B}^{-}(\chi) := \mathrm{B}(\chi)/J$

存在韦德伯恩分解 $\mathrm{B}^{-}(\chi) \cong \bigoplus_{t=1}^{k} \mathrm{Mat}_{d_t}(\mathbb{K})$，其中 $1 \le d_t \le w$ 为整数。

如果该只读代数分支程序计算出一个非零多项式，那么至少存在一个索引 $t^{\setminus *}$，使得诱导投影 $\psi_{t^{\setminus *}}$: $\mathrm{B}(\chi) \longrightarrow \mathrm{Mat}_{d_{t^{\setminus *}}}(\mathbb{K})$ 将该 ROABP 计算映射为一个非零矩阵值字。

我们将该因子 $\mathrm{Mat}_{d_{t^{\setminus *}}}(\mathbb{K})$ 称为活跃单块，并记 $r := d_{t^{\setminus *}}$。

证明

由于 $\mathrm{B}(\chi)$ 是域$\mathbb{K}$上的有限维代数，Wedderburn–Malcev理论表明，其商代数关于雅各布森根分解为简单矩阵代数的直和：$\mathrm{B}(\chi)/J \cong \bigoplus_{t=1}^{k} \mathrm{Mat}_{d_t}(\mathbb{K})$。

令 $\pi$：$\mathrm{B}(\chi) \to \mathrm{B}^{-}(\chi)$ 表示商映射，并令 $\psi_t$ 表示到第 $t$ 个矩阵块的坐标投影。

令 $W$ 表示 ROABP 在特化下计算得到的矩阵字。当且仅当 $W$ 不是 $\mathrm{B}(\chi)$ 中的零矩阵时，输出多项式非零。若对所有 $t$ 都有 $\psi_t(\pi(W)) = 0$，则 $\pi(W) = 0$，因此 $W \in J$。

但 $J$ 完全由幂零元构成，因此，对 $J$ 中元素作足够长的乘积，其计算结果必为零。这将迫使 ROABP 的输出恒等于零，与计算所得多项式非零的假设矛盾。

因此，至少存在一个指标 $t^{\setminus *}$，使得 $\psi_{t^{\setminus *}}(\pi(W)) \neq 0$，从而在 $\mathrm{Mat}_r(\mathbb{K})$ 中得到所需的非零同态像。■

**固定假设（活跃简单块情形）**

此后，我们固定一个满射代数同态 $\psi$：$\mathrm{B}(\chi) \longrightarrow \mathrm{Mat}_r(\mathbb{K})$，使得 ROABP计算在 $\psi$ 下的像非零。

所有后续的结构性构造——行列式见证、投影算子提取、轨道张成、次数三角化和有限回避——都将在这个活跃单块内部进行，或通过其经由 $\psi$ 的诱导作用进行。

引理 *3.1.1*（活跃块的一般稳定性）。

设 $\mathrm{B}$ 是由有理函数域$\mathbb{K}(\mathbf{x})$ 上的只读代数分支程序系数矩阵生成的字代数。设 $\mathrm{B} \otimes_{\mathbb{K}(\mathbf{x})} \mathbb{K}(\mathbf{x})^{-} \cong \bigoplus_{i=1}^{t} \mathrm{Mat}_{d_i}(\mathbb{K}(\mathbf{x})^{-})$ 是其韦德伯恩分解。
那么存在一个扎里斯基开稠密子集 $\Omega \subseteq \mathbb{K}^m$，使得对每个特化 $\chi \in \Omega$，特化代数 $\mathrm{B}(\chi)$ 都具有相同的简单块维数多重集 $\{d_1, \ldots, d_t\}$。特别地，活跃单块的指标 $r$ 在 $\Omega$ 上是稳定的。

证明。

域上的有限维代数 B 的结构由其结构常数中一组有限多项式恒等式的秩决定（例如单模的维数、乘法算子的秩，或等价地，在固定基下描述乘法的结构矩阵的秩）。

具体而言，固定一个 $\mathbb{K}(\mathbf{x})$-基 $\{W_1, \dots, W_N\}$，它是 B 的一组基。乘法表由结构常数编码

$$W_i W_j = \sum_{k=1}^{N} c_{ij}^{k}(\mathbf{x})\, W_k,$$

其中每个 $c_{ij}^{k}(\mathbf{x}) \in \mathbb{K}(\mathbf{x})$ 都是有理函数。通分后，这些函数可以写成多项式之比。

B 的韦德伯恩分解（即单矩阵块的数量和大小）由以下因素决定：

- 雅各布森根的维数，• 单模的维数，以及• 等价地，某些显式乘法映射和中心幂等投影的秩；这些都是关于结构常数的代数条件。

这些条件可以表示为矩阵 $A_i(\mathbf{x})$ 的系数中的有限个多项式行列式非零，其中这些矩阵定义了只读代数分支程序。因此，特化集合 $\chi$ 中使 $\mathrm{B}(\chi)$ 的半单商与 B 在 $\mathbb{K}(\mathbf{x})$ 上具有相同韦德伯恩块维数的特化，构成一个扎里斯基开集 $\Omega \subseteq \mathbb{K}^m$。

由于一般纤维（在 $\mathbb{K}(\mathbf{x})$ 上）实现了特定的块分解，因此该开集非空且稠密。因此，对所有 $\chi \in \Omega$，块维数 $\{d_1, \dots, d_t\}$——尤其是活跃块的指标 $r$ ——在特化下保持不变。■

根据引理 3.1.1，我们可以并且将会选择所有后续特化 $\chi$，使其属于扎里斯基开稳定集 Ω，从而确保活跃块指标 $r$ 在特化下保持不变。

引理 *3.1.2*（不可约块满性——舒尔 + 伯恩赛德）

设 $\mathbb{K}$ 为代数闭域，且设 $\mathcal{A} \subseteq \mathrm{Mat}_w(\mathbb{K})$ 为一个 $\mathbb{K}$-子代数。令 $V = \mathbb{K}^w$ 为自然左 $\mathcal{A}$-模。

固定 $V$ 作为 $\mathcal{A}$-模的一条合成列，$0 = V_0 \subset V_1 \subset \cdots \subset V_k = V$，并将不可约因子记为 $S_i := V_i/V_{i-1}, d_i := \dim_{\mathbb{K}}(S_i)$。

对于每个 $i$，令 $\phi_i: \mathcal{A} \to \mathrm{End}_{\mathbb{K}}(S_i)$ 为诱导表示。

然后 $\phi_i(\mathcal{A}) = \text{结束}_{\mathbb{K}}(S_i) \cong \text{矩阵}_{d_i}(\mathbb{K})$。

证明

令 $B_i := \phi_i(\mathcal{A}) \subseteq \mathrm{End}_{\mathbb{K}}(S_i)$。由于 $S_i$ 作为 $\mathcal{A}$-模是不可约的，像代数 $B_i$ 在 $S_i$上不可约地作用。

根据**舒尔引理**（在代数闭域上），$B_i$ 在 $\mathrm{End}_{\mathbb{K}}(S_i)$ 中的中心化子仅由标量构成：$\mathrm{End}^{B_i}(S_i) = \mathbb{K} \cdot I$。

根据**伯恩赛德定理**（等价地，也可由双中心化子定理或稠密定理得出），中心化子仅由标量构成的不可约矩阵代数必定与整个自同态代数相同。因此 $B_i = \mathrm{End}_{\mathbb{K}}(S_i) \cong \mathrm{Mat}_{d_i}(\mathbb{K})$，得证。□

引理 *3.1.3*（根的幂零指数界）

设 $J := J(\mathcal{A})$ 是 $\mathcal{A} \subseteq \mathrm{Mat}_w(\mathbb{K})$ 的雅各布森根。那么 $J^w = 0$。等价地，$J$ 中任意 $w$ 个元素的乘积都是零矩阵。

证明

由于 $J$ 是有限维代数中的幂零理想，$J$ 中的每个元素在有限维向量空间 $V = \mathbb{K}^w$ 上的作用都是幂零的。

考虑由 $J$ 生成的 $\mathrm{End}_{\mathbb{K}}(V)$ 的结合子代数。这是一个完全由幂零算子构成的有限维代数。根据**恩格尔定理**（将其应用于这些算子在换位子运算下生成的李代数），存在 $V$ 的一个基，使得 $J$ 中的每个算子在该基下都是严格上三角的。因此，任意 $w$ 个这样的算子的乘积都为零，从而 $J^w = 0$。 □

注。
如果不想使用恩格尔定理，也可以根据以下标准事实得到相同结论：代数闭域上 $\mathrm{End}(V)$ 的任意幂零子代数都可以同时化为严格上三角形式。

注 *3.1.4*（分块图景与“存续”）

引理 3.1.2 表明，每个合成因子 $S_i$ 都支持一个全矩阵像 $\phi_i(\mathcal{A}) \cong \mathrm{Mat}_{d_i}(\mathbb{K})$。因此，选定一个合成列后，$\mathcal{A}$ 在 $V$ 上的表示可以写成分块上三角形式：对角块对应于作用在不可约商上的全矩阵代数，而严格上三角的非对角块则由根 $J(\mathcal{A})$控制。

根据引理 3.1.3，根满足 $J^w = 0$。特别地，一旦乘法长度达到 $w$，完全由根因子构成的任何贡献都会消失。因此，任何非零计算都必须在半单商 $\mathcal{A}/J(\mathcal{A})$中具有非平凡像，进而至少在一个对角简单块 $\mathrm{Mat}_{d_i}(\mathbb{K})$中具有非平凡像。

### 3.3 化归到活跃简单块情形

识别出一个活跃简单商块后，我们现在正式将恒等式测试问题归约为该块内部的计算。

回顾引理 3.1，存在一个满射代数同态 $\psi$: B($\chi$) $\longrightarrow$ Mat $_r$(𝕂)，使得 ROABP计算在 $\psi$下的像非零。我们将 Mat $_r$(𝕂) 称为活跃单块。

引理 *3.2*（到活跃块的可靠归约）

令 $W(x_1, \ldots, x_n)$ 表示只读代数分支程序在特化下计算的矩阵字。当且仅当 $\psi(W(x_1, \ldots, x_n)) = 0$ in Mat $_r$(𝕂) 时，计算所得多项式恒等于零。

特别地，对原始只读代数分支程序进行确定性恒等式检验，可归约为对其在活跃块中的投影计算进行恒等式检验。

证明

如果 $W(x)$ 在 B($\chi$) 中恒等于零，那么显然，它在任意同态（包括 $\psi$）下的像也为零。

反之，假设 $\psi(W(x)) = 0$。那么 $W(x)$ 属于 $\psi$ 的核，而该核包含雅各布森根 $J$(B($\chi$))。

**情形 1**（$n \geq w$）。由引理 3.1.3，$J^w = 0$。由于只读代数分支程序的乘积长度满足 $n \geq w$，若生成元位于某个子代数中，且乘积映射为 $J$，则该乘积为零。

**情形 2**（$n < w$）。如引理 3.3.1 中所述，此情形通过直接网格求值（$w + 1$）处理，不依赖于根的消失性质。

因此，非零性　原始计算的非零性等价于活跃单块中的非零性。 ■

**推论 3.3（可靠性链）**。
令 $C(x_1, \ldots, x_n)$ 设其为只读代数分支程序计算得到的标量多项式，并令 $W(x)$ 为对应的矩阵字。于是 $C \equiv 0 \iff \exists\, \chi, \exists\, \lambda$ 使得 $\psi\,(W(\gamma_\lambda(\chi(x)))) \neq 0$。

证明。
多项式恒等式在一般特化 $\chi$ （引理 3.1.1）和保持次数的曲线代入 $\gamma_\lambda$ （引理 5.5）下仍然成立。由于雅各布森根的贡献在足够长的乘积中会消失（注 3.1.4），同态 $\psi$ 保持非零性。因此，非零的标量输出意味着在活跃块上的取值非零。□

引理 *3.3.1*（活跃块充分性）

令 B($\chi$) 为特化字代数，$\psi$: B($\chi$) $\to$ Mat $_r$(𝕂) 为映射到活跃单块的同态。若任一代数证书 $W \in$ B($\chi$) 在 $\psi$ 下非零（即 $\psi(W) \neq 0$），则 ROABP 多项式 $C$ 非零。因此，PIT 构造可以在活跃块内进行，而不会损失正确性。

证明。我们用逆否命题进行论证。假设 $C \equiv 0$。

**情形 1 ($n < w$)**。 在此情况下，ROABP 计算的是一个总次数为 $<w$ 的多项式。这被视为基本情形：通过在大小为 $w+1$ 的网格上求值，即可确定性地进行恒等式测试，无需调用根基结构。

**情形 2**（$n \geq w$）。映射$\psi$ 经由半单商$\mathrm{B}^{-}(\chi) = \mathrm{B}(\chi)/J$分解。若$\psi(W) \neq 0$，则$W \notin J$。在有限维代数中，任一元素$W \notin J$ 在某个单矩阵块中具有非零像（由Wedderburn–Malcev）。由于活跃块定义为到这样一个块的投影，$\psi(W) \neq 0$ 意味着该计算在半单商中是非平凡的，从而$C \equiv/0$。反之，若$C \equiv 0$，则该计算必须在半单商中为零，从而迫使$\psi(W) = 0$。□

证明。

我们分离出本文实际使用的两个蕴含关系。

**(1) 非零像蕴含非零元素**。
由于$\psi$ 是环同态，$\psi(0) = 0$。因此，若$X \in \mathrm{B}(\chi)$满足$\psi(X) \neq 0$，则必然有$X \neq 0$ 属于$\mathrm{B}(\chi)$。（等价地，$X = 0 \Rightarrow \psi(X) = 0$；取逆否命题。）

**（2）活跃块中的任意非零见证都意味着 $C \equiv/0$**。
令 $M(x) \in \mathrm{B}(\chi)$ 表示对应于只读代数分支程序计算的矩阵值字，因此，对于固定的起始/终止向量 $s$、$t \in \mathbb{K}^w$ （通常为 $s = e_1$、 $t = e_w$），有 $C(x) = s^{\top} M(x)\, t$ 。将 $\psi$ 逐项作用于 $M(x)$，得到矩阵 $\psi(M(x)) \in \mathrm{Mat}_r(\mathbb{K}[x])$。由于 $\psi$ 是 $\mathbb{K}$-线性且具有乘法性，$\psi(M(x))$ 正是通过活跃块表示执行的同一乘积计算。

现在考虑该框架生成的任意证书（投影算子、配对、行列式见证等）。在所有情况下，证书都是一个显式代数表达式 $W(x) \in \mathrm{B}(\chi)$（可能需要先添加辅助参数，再对其进行特化），其正确性论证证明：$\psi(W(x)) \neq 0 \Longrightarrow \psi(M(x)) \neq 0$。

此外，根据“活跃”块的定义，该块中至少存在一个标量泛函（行/列选择，或由秩一投影算子诱导的双线性型），能够从 $\psi(M(x))$ 中提取出一个非零标量多项式。具体而言，使用秩一探针 $\Pi$ 和传递字 $U_i, V_j$ （如第 4 节所述），论文采用如下形式的标量提取

$$p_{ij}(x) := e_1^{\top}\, \psi(U_i)\, \psi(\Pi)\, \psi(M(x))\, \psi(V_j)\, e_w,$$

且配对的非退化性保证，$\psi(M(x)) \neq 0$ 蕴含对于某些 $i, j$，有 $p_{ij}(x) \equiv/0$ 。由于 $p_{ij}(x)$ 是由固定的 $\mathbb{K}$-线性泛函和固定字的乘法从 $M(x)$ 得到的，因此它是 ROABP 计算的合法标量多项式推论。因此 $C \equiv/0$。

最后请注意，逆否方向显然成立：如果 $C \equiv 0$ 作为标量多项式，那么对 $C$ 有贡献的 $M(x)$ 的每个矩阵条目，在任意特化下都恒为零，因此 $\psi(M(x))$ 以及每个导出块证书的取值均为 0 $\psi \cdot$ $C \equiv$ 。因此，观察到任何满足 $() \neq 0$ 0 的证书，就可以排除 。这证明了该引理。□

**推论：约化代数状态空间**

在活跃块内，字代数变成一个**全矩阵代数**：$\psi(\mathrm{B}(\chi)) = \mathrm{Mat}_r(\mathbb{K})$。

此后，所有代数运算都将通过在 Mat $_r(\mathbb{K})$ 上的诱导作用来解释。特别是：

- $r^2$ 矩阵字被视为维数
- 为 的全矩阵代数中的元素。任何非零元素都能在此块内生成秩一结构；• 代数见证（行列式、伴随矩阵、投影算子）只需证明其在此商中的非零性。

这将有效代数维数从$w^2$ 降至$r^2$，其中$r \le w$，且不失一般性。

**固定假设（活跃块工作机制）**

从此处开始，我们固定满同态$\psi$: B($\chi$) → Mat $_r(\mathbb{K})$，并在像代数 Mat $_r(\mathbb{K})$ 内进行所有结构性论证。

为简化记号，我们将继续把矩阵字写作 B($\chi$) 中的元素，同时理解为所有非退化条件均通过 $\psi$进行评估。

**为何此约化是最优的**

这种约简严格弱于假设全矩阵生成，但恰好足以支持确定性多项式恒等式测试：

- 它适用于对角、三角和可约只读代数分支程序，• 它消除了错误的不可约性假设，• 它保证每一步行列式见证和投影算子提取都针对非平凡的代数分支，• 它避免了此前有限避零论证中的循环论证。

因此，后续各节可以将活跃块内的字代数视为全代数，而无须断言整体上是全代数。

### 3.4 全矩阵代数的低支持生成

（有效维数坍缩定理）

将问题约简至全矩阵机制后，我们现在证明：只读代数分支程序生成的矩阵词代数虽然源自任意多个输入变量，实际上却仅由 $O(w^2)$ 个有效方向生成。这揭示了有界宽度分支程序所诱导的全矩阵代数中固有的维数坍缩现象。

关于活跃块约化的注：在本节及后续各节中，我们都在活跃块同态的核模下进行工作。因此，根据引理 3.3.1，我们实际上可以在不失一般性的前提下作此假设。

**约定（在活跃块上工作）**。在第 3.4–7 节中，每当我们用到张成、投影算子提取、配对非退化性或“全矩阵”恒等式时，这些陈述均应用于活跃简单块像 $\psi$(B($\chi$)) = Mat$_r(\mathbb{K})$。形式上，我们在 ker ($\psi$) 模掉的意义下工作；因此，诸如“$X = 0$”这样的等式应理解为“$\psi(X) = 0$”，除非另有明确说明。

定理 *3.5*（活跃块生成与有效维数界）。

设 $C$ 是域 $\mathbb{K}$ 上宽度为 $w$ 的只读代数分支程序所计算的多项式，且 $\mathrm{B}(\chi) \subseteq \mathrm{Mat}_w(\mathbb{K})$ 是特化字代数。设 $\psi\colon \mathrm{B}(\chi) \twoheadrightarrow \mathrm{Mat}_r(\mathbb{K})$ 是映到一个活跃单块的满同态（按第 3.3 节的定义），即只读代数分支程序的输出在诱导的块求值下非零。

假设 $\psi(\mathrm{B}(\chi)) = \mathrm{Mat}_r(\mathbb{K})$。那么：

1. **(活跃块张成)** 存在矩阵字 $W_1, \ldots, W_m \in \mathrm{B}(\chi)$，满足 $m \le r^2$，使得 $\mathrm{span}_{\mathbb{K}}\{\psi(W_1), \ldots, \psi(W_m)\} = \mathrm{Mat}_r(\mathbb{K})$。

等价地，像代数 $\psi(\mathrm{B}(\chi))$（作为 $\mathbb{K}$-代数）由至多 $r^2$ 个元素生成。

2. **(安全统一上界)** 尤其是，由于 $r \le w$，我们可以在复杂度核算中处处使用 $m \le w^2$ 作为上界，而不影响正确性。

证明。

我们通过同态 $\psi$ 完全在活跃单块内进行。

步骤 ***1***：活跃块中的维数界

全矩阵代数 $\mathrm{Mat}_r(\mathbb{K})$ 是一个向量空间，其在域K $\mathbb{K}$ 上的维数为 $r^2$。因此，任何线性张成等于 $\mathrm{Mat}_r(\mathbb{K})$ 的子集都包含一个大小至多为 $r^2$ 的线性无关子集。

令 $S := \{\psi(A_1(\chi)), \ldots, \psi(A_n(\chi))\} \subseteq \mathrm{Mat}_r(\mathbb{K})$ 为特化的只读代数分支程序层在同态 $\psi$ 下的像集。

根据活跃块的定义，由 $S$ 生成的代数等于 $\mathrm{Mat}_r(\mathbb{K})$。特别地，$S$ 的线性张成就是整个 $\mathrm{Mat}_r(\mathbb{K})$。

步骤 ***3:*** 从生成元中提取一组基

由于 $S$作为向量空间张成 $\mathrm{Mat}_r(\mathbb{K})$，我们可以选取一个线性无关子集 $\{\psi(A_{i_1}(\chi)), \ldots, \psi(A_{i_m}(\chi))\}$, $m \le r^2$，它构成 $\mathrm{Mat}_r(\mathbb{K})$ 的向量空间基。

为这些基元素选取任意原像 $A_{i_1}(\chi), \ldots, A_{i_m}(\chi) \in \mathrm{B}(\chi)$。

步骤 ***3:*** 活跃块内对乘法封闭

令 $\mathrm{B}' \subseteq \mathrm{B}(\chi)$ 表示由 $A_{i_1}(\chi)$、……、$A_{i_m}(\chi)$ 生成的子代数。由于它们的像构成 $\mathrm{Mat}_r(\mathbb{K})$ 的向量空间基，$\mathrm{Mat}_r(\mathbb{K})$ 中的每个元素都可以表示为这些像的线性组合。特别地，$\psi(\mathrm{B}(\chi))$ 中元素的任意乘积都可展开为 $\mathbb{K}$-线性组合：$\psi(A_{i_1}(\chi))$、……、$\psi(A_{i_m}(\chi))$。因此，$\psi(\mathrm{B}') = \mathrm{Mat}_r(\mathbb{K})$，即，活跃单块完全由至多 $r^2$ 个特化的只读代数分支程序层的像生成。

步骤 ***4***：结论

我们得出结论：活跃块 Mat $_r(\mathbb{K})$ 由至多 $r^2$ 个源自 ROABP 层的元素代数生成。由于 $r \le w$，这给出了 $w^2$ 个生成元的统一上界。这确立了后续代数构造所需的低支撑生成性质。□

推论 *3.6*（活跃块变量约化）。

设 $C(x_1, \dots, x_n)$ 是由宽度为 $w$ 的只读代数分支程序计算的多项式，并设 $\psi$: B($\chi$) $\twoheadrightarrow$ Mat $_r(\mathbb{K})$ 是到活跃单块上的满同态，其中 $\psi(C) \neq 0$。则存在指标 $i_1, \dots, i_m$，满足 $m \le r^2 \le w^2$，以及显式的线性形式

$$y_j = \sum_{k=1}^{n} \gamma_{j,k}\, x_k (1 \le j \le m),$$

使得 ROABP计算可分解为 $C(x_1, \dots, x_n) = \tilde{C}(y_1, \dots, y_m)$，其中当 $C$ 非零时，$\tilde{C}$ 也非零。

特别地，对于 $C$ 的恒等式测试可确定性地约化为对至多含有 $r^2 \le w^2$ 个有效变量的多项式进行恒等式测试，而与原始变量数 $n$ 无关。

证明。

根据定理 3.5，活跃块 Mat $_r(\mathbb{K})$ 可由至多 $\mathbb{K}$ 个特化的只读代数分支程序层的像生成，作为一个代数。

$$\psi(A_{i_1}(\chi)), \dots, \psi(A_{i_m}(\chi))$$

因此，模去 $\psi$ 的核后，每个前缀乘积 $A_1(x_1) \cdots A_k(x_k)$ 都可以唯一地展开为这些生成元的线性组合，其系数为标量多项式。由此，ROABP计算对输入变量 $x_1$、…、 $x_n$ 的所有标量依赖，都经由至多 $r^2$ 个线性形式。

具体而言，选取由所选层生成的活跃块的一组基，可导出线性形式 $y_1$、…、 $y_m$，使得计算所得多项式可写为 $C(x_1, \dots, x_n) = \tilde{C}(y_1, \dots, y_m)$。

由于 $\psi(C) \neq 0$，此变换保持非零性。因此，$C$ 的黑盒恒等式测试可归约为至多 $r^2 \le w^2$ 个变量上的恒等式测试。□

**概念意义**

该定理表明，**有界宽度会限制代数表达能力**：一旦生成的代数达到最大，就无法编码真正的高维变化。相反，计算会收缩到一个规模与宽度的平方成正比的受控代数核心。这一现象是矩阵字代数所固有的，并不依赖于组合稀疏性或系数隔离。

**3.5 推论：低支撑见证依赖**

推论 *3.4*

存在一个　　张成词集 $\mathcal{W} = \{W_1, \dots, W_{w^2}\}$，仅使用由 $I$ 索引的生成元，使得

$$\mathrm{span}\{W_a(\chi)\} = \mathrm{Mat}_w(\mathbb{K}).$$

证明

从引理 3.3 中构造的稳定化张成空间 $V_L$ 提取一个基。■

**3.6 满矩阵行列式见证**

现在，我们构造一个行列式多项式，用以证明字代数是满的　　.

引理 *3.5*（满矩阵见证）

设 $\mathcal{W} = \{W_1, \dots, W_{w^2}\}$ 如推论 3.4 所述。定义 $K_{ab} = e_1^{\top} W_a(\chi)\, W_b'(\chi)\, e_w, 1 \le a, b \le w^2$,

其中 $\{W_b'\}$ 是另一个张成词集。令 $\Delta := \det(K)$。则：$\Delta \neq 0 \iff \mathrm{B}(\chi) = \mathrm{Mat}_w(\mathbb{K})$。

证明

双线性配对 $(X, Y) \mapsto e_1^{\top} XY e_w$ 在 $\mathrm{Mat}_w(\mathbb{K})$ 上非退化，当且仅当该代数张成所有矩阵方向。因此，格拉姆矩阵 $K$ 恰好在全矩阵情形下是非奇异的。■

**3.7 结构总结**

我们已经证明：

1. 在特化下，矩阵词代数要么是平凡的，要么是全矩阵代数。2. 在全矩阵情形下，至多使用 $w^2$ 个有效变量方向即可生成该代数。3. 可通过一个至多依赖 $w^2$ 个变量的行列式见证多项式来认证其全矩阵性。

这种秩集中现象将确定性恒等式测试归约为一个低支持代数问题，后续章节将通过投影算子提取、次数三角化和代数曲线命中来利用这一点。

**4. 从全矩阵词代数中无特征值地提取（有理）秩一投影算子**

在本节中，我们始终采用第 3 节中的活跃简单块假设。也就是说，我们固定一个满射代数同态 $\psi$: $\mathrm{B}(\chi) \longrightarrow \mathrm{Mat}_r(\mathbb{K})$，使得 ROABP计算在 $\psi$ 下的像非零。

我们的目标是构造一个元素 $\Pi \in \mathrm{B}(\chi)$，使其像 $\psi(\Pi)$ 在 $\mathrm{Mat}_r(\mathbb{K})$ 中是一个秩一幂等元。重要的是，$\Pi$ 在整个 $w \times w$ 表示中不必是秩一的——只需在活跃块中秩一，这就足以进行多项式恒等式检验。

### 4.1 定向幂等元构造（活跃块中的凯莱–哈密顿）

定理 *4.1*（定向秩一投影算子提升）

存在一个矩阵字 $W \in \mathrm{B}(\Phi\ W$ $\Pi$ $\chi$ $w \to w$ $\mathbb{K}$ $=$ $)$ 和一个多项式映射 $\Phi$:Mat $(\mathbb{K})$ Mat $(\mathbb{K})$，使得 $\Pi$: ( ) 满足 $\psi(\ )$ 是 Mat $_r(\ )$ 中的非零秩一幂等元。

证明
步骤 ***1*** — 活跃块内的简单谱

由于 $\psi(\mathrm{B}(\chi)) = \mathrm{Mat}_r(\mathbb{K})$，存在 $M \in \mathrm{B}(\chi)$，使得 $\psi(M)$ 在 Mat $_r(\mathbb{K})$ 中有互异特征值。（这是因为具有简单谱的矩阵构成 Mat $_r$ 的扎里斯基开稠密子集。）第 6 节中的判别式多项式现在仅定义在 $r \times r$ 块上，从而确保它不恒等于零。

步骤 ***2*** — 凯莱–哈密顿投影算子构造

将原始的凯莱–哈密顿多项式构造应用于 $M$，得到 $E := p(M)$，使得 $\psi(E)$ 是 Mat $_r(\mathbb{K})$ 中的一个非零幂等元。

注意：由于存在幂零根基分量，$E$ 在整个代数中可能不是幂等元，但应用 $\psi$ 后，幂等性成立。

步骤 ***3*** — 通过牛顿迭代提升幂等元。

将 $E = E_{\mathrm{ss}} + N$ 写为 $N \in J$ $\chi$ $q_{k+1}\ t\ = q_k\ t\ \ 2 - q_k\ t\ \ q_0\ t\ =(\mathrm{B}(\ ))$。应用牛顿迭代 ( ) ( )( ( )), () 。由于雅各布森根满足 (引理 . . )，二次收敛意味着经过 $k = \lceil \log_2 w \rceil$ 次迭代后，我们得到一个元素 $\Pi = q_k(E)$，满足 $\Pi^2 = \Pi, \psi(\Pi) = \psi(E)$。

多项式次数在每一步都翻倍，因此 $\deg(\Pi) \le 2^k \deg(E) \le 2w^2 = \mathrm{poly}(w)$。

步骤 ***4*** — 秩一细化

在 Mat $_r(\mathbb{K})$ 中，将已有的 **Amitsur–Levitzki + Cayley–Hamilton 秩约化链**应用于 $\psi(\Pi)$，从而在活跃块中得到一个秩一幂等元。

通过与 B 中相同的多项式映射复合，我们得到一个满足定理的提升 $\Pi$ 。■

**提升的次数控制**

我们通过牛顿迭代 $q_{k+1}(t) = q_k(t)(2 - q_k(t)), q_0(t)$ 实现幂等元提升：$= t$。

归纳地，经过 $k$ 步后，元素 $q_k(E)$ 模理想 $J^{2^k}$ 是一个幂等元，其中 $J$ 表示雅各布森根。由于 $J$ 的幂零指数至多为 $w$（引理 3.1.3），取 $k = \lceil \log_2 w \rceil$ 可确保 $J^{2^k} \subseteq J^w = 0$。因此，进行 $O(\log w)$ 次迭代即可得到真正的幂等元。

对于每个 i 迭代后，多项式的次数加倍。因此，最终次数满足

$$\deg(q_{\text{final}}) \le 2^{\lceil \log_2 w \rceil} \deg(E) \le 2w \cdot w = 2w^2,$$

该次数仍受多项式界限约束。

### 4.2 通过凯莱–哈密顿定理构造非零幂等元

现在，我们仅使用凯莱–哈密顿定理来构造一个非零幂等元，而不进行特征值提取或解析谱分解。此构造将**应用**于第 3 节中确定的活跃单块。

引理 *4.2*（通过 *Cayley–Hamilton* 定理构造的多项式幂等元）

设 $M \in \mathrm{B}(\chi)$，并考虑其在活跃块同态 $\psi: \mathrm{B}(\chi) \to \mathrm{Mat}_r(\mathbb{K})$ 下的像 $\psi(M) \in \mathrm{Mat}_r(\mathbb{K})$。

那么存在一个非零多项式 $p(t) \in \mathbb{K}[t]$，$\deg p \le r-1$，使得 $E := p(M)$ 满足 $\psi(E)^2 = \psi(E)$，$\psi(E) \neq 0$。也就是说，$\psi(E)$ 是活跃矩阵块中的一个非零幂等元。

证明

令 $\mu_{\psi(M)}(t)$ 表示 $\psi(M)$ 的最小多项式。根据凯莱–哈密顿定理，$\deg \mu_{\psi(M)} \le r$。

将 $\mu_{\psi(M)}$ 在 $\mathbb{K}$ 上分解为两两互素的主因子：$\mu_{\psi(M)}(t) = f_1(t)^{e_1} f_2(t)^{e_2} \cdots f_s(t)^{e_s}$，

其中 $f_i(t)$ 均不可约且两两互素。

固定一个指标 $j$，并定义

$$g_j(t) := \prod_{i \neq j} f_i(t)^{e_i}.$$

由于这些因子互素，根据贝祖等式，存在多项式 $a(t), b(t) \in \mathbb{K}[t]$，使得 $a(t) g_j(t) + b(t) f_j(t)^{e_j} = 1$。

定义 $p(t) := a(t) g_j(t)$。

代入 $\psi(M)$，得到 $p(\psi(M))^2 = p(\psi(M))$，

因为 $f_j(\psi(M))^{e_j} = 0$。因此，$p(\psi(M))$ 是一个幂等元。

此外，$p(\psi(M)) \neq 0$，因为它在对应于 $f_j$ 的主分量上充当恒等元。

最后，$\deg p(t) = \deg g_j(t) \le \deg \mu_{\psi(M)} - 1 \le r - 1$。

定义 $E := p(M) \in \mathrm{B}(\chi)$。应用 $\psi$，我们得出：$\psi(E) = p(\psi(M))$ 是 $\mathrm{Mat}_r(\mathbb{K})$ 中的非零幂等元。■

**解释：**

这就在字代数中构造出了一个非零代数幂等元，使得：

- 幂等性在**活跃块内**成立，• 不使用特征值计算，• 不需要域扩张，• 不涉及解析谱论论证。

该论证仅依赖于最小多项式，因此在任意特征为零或特征严格大于 $2w$ 的域上均成立。

### 4.3 通过 Amitsur–Levitzki 刚性进行秩约化

引理 4.2 中的投影算子秩可能大于一。现在我们证明，多项式恒等式会迫使秩约化。

引理*4.3*（角代数内的严格秩下降）

设 $E \in \mathrm{Mat}_w(\mathbb{K})$ 是一个非零幂等元，并令 $r := \mathrm{rank}(E)$。若 $r > 1$，则存在一个元素 $A \in \mathrm{Mat}_w(\mathbb{K})$ 和一个多项式 $p(t) \in \mathbb{K}[t]$，满足 $\deg p \le r - 1$，使得 $E' := p(EAE)$ 是一个非零幂等元，且满足 $E' \neq E$，因此 $\mathrm{rank}(E') < \mathrm{rank}(E)$。

证明：

令 $\mathcal{A}_E := E\,\mathrm{Mat}_w(\mathbb{K})\,E$。

则 $\mathcal{A}_E$ 是一个含幺代数，其单位元为 $E$。众所周知（在选取一个使 $E = \mathrm{diag}(I_r, 0)$ 的基后，这一点显而易见），$\mathcal{A}_E \cong \mathrm{Mat}_r(\mathbb{K})$。

特别地，$\mathcal{A}_E$ 含有具有指定有理标准形的元素。

选取两个首一、非常数且互素的多项式 $f$、$g \in \mathbb{K}[t]$，满足 $\deg f + \deg g \le r$。

（例如，如果 $\mathbb{K}$ 至少有两个元素，则取 $f(t) = t$ 和 $g(t) = t - 1$；否则取任意两个不同的不可约多项式。这样的 $f$、$g$ 总是存在的；如果需要，还可以乘以额外的互素因子来调整次数。）

令 $C(f)$ 和 $C(g)$ 分别表示 $f$ 和 $g$的伴随矩阵。通过分块对角矩阵 $T_0$ 定义 $T_0 \in \mathrm{Mat}_r(\mathbb{K})$ 中的一个元素：$= \mathrm{diag}(C(f), C(g), 0_{r-\deg f-\deg g})$。

那么，$T_0$ 的最小多项式是 $\mu_{T_0}(t) = \mathrm{lcm}(f(t), g(t), t)$；特别地，它被乘积 $f(t)g(t)$ 整除，其中 $\gcd(f, g) = 1$。通过同构 $\mathcal{A}_E \cong \mathrm{Mat}_r(\mathbb{K})$ 传递 $T_0$，我们得到一个元素 $T \in \mathcal{A}_E$。由于 $\mathcal{A}_E = E\mathrm{Mat}_w(\mathbb{K})E$，我们可以将 $T = EAE$ 写成某个 $A \in \mathrm{Mat}_w(\mathbb{K})$。

现在对含幺代数（$\mathcal{A}_E$, $E$）中的元素 $T$ 应用无特征值幂等元提取（与引理 4.2 中相同的机制）。具体来说，由于 $\mu_T$ 至少有两个互素的主因子，存在多项式 $u(t), v(t) \in \mathbb{K}[t]$，使得 $u(t)\,f(t)^e + v(t)\,\mu_T{}_{(t)\,f(t)_e} = 1$ 对于 $f$-主因子 $f(t)^e$ 而言

$\mu_T(t)$。令 $p(t) := u(t)\, f(t)^e$，标准的贝祖定理／中国剩余定理论证表明，$E' := p(T)$ 是 $\mathcal{A}_E$ 中的一个幂等元，并且还有 $0 \neq E' \neq E$。

（事实上，$E'$ 在 $f$ 主分量上起恒等作用，在其互补的主分量上作用为 0；按构造，这两个分量都非零，因为 $f$ 和 $g$ 都出现在 $\mu_T$ 中。）

最后，$E' \neq E$ 意味着 $\mathrm{Im}(E')$ 是 $\mathrm{Im}(E)$ 的真非零子空间，因此 $\mathrm{rank}(E') < \mathrm{rank}(E)$。

次数界 $\deg p \leq r-1$ 成立，是因为可以在 $\mathrm{Mat}_r(\mathbb{K})$ 中选取次数至多为 $\deg \mu_T - 1 \leq r-1$ 的 $p$。 ■

注（*Amitsur–Levitzki* 定理的作用：安全地说明）

**Amitsur–Levitzki** 的作用可以明确地作为背景来说明：$\mathcal{A}_E \cong \mathrm{Mat}_r(\mathbb{K})$ 是一个 PI-次数为 $2r$ 的多项式恒等式代数。然而，上述秩下降本身是通过最小多项式主分解证明的，这种方法严格来说更安全，也更加明确。

推论 *4.3*（有限秩下降至秩一）

至多迭代引理4.3 $w-1$ 次，可得到秩一幂等元 $\Pi$，它是通过对形如 $EAE$ 的角元素反复应用多项式而得到的。

### 4.4 通过有限回避进行无特征值（有理）秩一投影算子提取

现在，我们以纯代数、无特征值（有理）且确定性的方式，完成从整个矩阵词代数中提取秩一投影算子的过程。唯一剩下的障碍，是确保凯莱–哈密顿构造和基于多项式恒等式的构造所要求的所有非退化条件能够同时成立。我们通过有限多项式规避论证**来解决这一问题**。

在本节中，始终假设 $\mathrm{B}(\chi) = \mathrm{Mat}_w(\mathbb{K})$。

#### 4.4.1 次数增长与约束预算

我们追踪 th 构造中出现的每个约束多项式的总代数次数。

引理 *4.7*（谱约束的次数界）

设 $M \in \mathrm{Mat}_w(\mathbb{K})$。那么：

1. $M$ 的特征多项式系数在矩阵元素中的次数至多为 $w$。 2. 特征多项式的判别式次数至多为 $O(w^3)$。 3. $\mathrm{adj}\ (\mu I - M)$ 的每个元素在 $M$ 的元素中的次数至多为 $w-1$，在 $\mu$ 中的次数至多为 $w-1$。 4. $\mu I - M$ 的任意固定 $(w-1) \times (w-1)$ 子式的次数至多为 $w-1$。 5. 消去特征多项式与此类子式之间的 $\mu$ 所得的结式次数至多为 $\mathrm{poly}(w)$。

因此，保证存在非零的基于伴随矩阵的投影算子所需的所有代数约束，其总次数均由 $D_\star = \mathrm{poly}(w)$界定。

证明

每个界都由行列式、子式、判别式和结式的标准次数增长估计得出。所有运算都是关于矩阵元素的多项式，且每一步引入的乘法次数增长至多为 $O(w)$。■

### 4.4.2 有限多项式避零

现在我们保证存在一个特化，使其避开所有约束多项式的公共零点集。

引理 *4.8*（有限避零引理）

设 $F \in \mathbb{K}[t_1, \dots, t_m]$ 是一个总次数至多为 $D_\star$的非零多项式。那么，对于任意网格 $S^m \subset \mathbb{K}^m$ ，若 $|S| > D_\star$ ，就存在其中一点，使得 $F$ 在该点不为零。

证明

根据标准的 Schwartz–Zippel–DeMillo–Lipton 计数论证，次数至多为 $D_\star$ 的非零多项式不可能在每个坐标上的大小均超过 $D_\star$ 的笛卡尔积网格上处处为零。■

我们从有限避零集与扎里斯基开稳定集 Ω 的交集中选取 $\chi$ （引理 3.1.1），从而保留活跃块结构。

### 4.4.3 非退化特化的存在性

结合引理 4.7 和引理 4.8，我们得到：

推论 *4.9*（良好谱特化的存在性）

存在一种对矩阵词代数中出现的辅助参数进行的特化，使得：

1. 所得矩阵 $M$ 至少有一个单特征值。2. 对应的伴随矩阵 $\mathrm{adj}\ (\mu I - M)$ 非零。
3. 投影算子提取所需的所有多项式约束均同时满足。

### 4.4.4 秩一投影算子提取

现在我们进行代数提取。

引理 *4.10*（非零多项式投影算子）

在推论 4.9 的特化下，存在一个次数至多为 $w - 1$ 的多项式 $p(t)$，使得 $E = p(M)$ 是一个非零幂等元。

证明

根据凯莱–哈密顿定理，$M$满足其特征多项式。选取与某个特征值对应因子的互补因子，可得到一个多项式，它会湮灭所有其他广义特征子空间，并作为投影算子作用于一个非零不变子空间。■

引理 *4.11*（无 *PI* 的角代数秩一提取）

设$\mathbb{K}$ 是一个域，且 $\mathrm{char}(\mathbb{K}) = 0$ 或 $\mathrm{char}(\mathbb{K}) > w$。
设$E \in \mathrm{Mat}_w(\mathbb{K})$是一个秩为$r \geq 1$的非零幂等元。那么：

1. 角代数$E\mathrm{Mat}_w(\mathbb{K})E$ 同构于 $\mathrm{Mat}_r(\mathbb{K})$。2. 若$r \geq 2$，则存在矩阵$A, B \in \mathrm{Mat}_w(\mathbb{K})$，使得对于某些$\lambda, \mu \in \mathbb{K}$,

$$\Pi := \ \mathrm{adj}\ (\mu E - E(A + \lambda B)E)$$

是一个相差非零标量的非零秩一投影算子。用任意一个非零元素归一化后（由有限回避可保证其存在），Π 可以缩放为严格的幂等元。

3. 此外，存在一个显式的约束多项式 $F_E(\lambda;\ A, B)\ \in \mathbb{K}[\lambda, \{A_{ij}\}, \{B_{ij}\}]$，使得

$$\deg\ F_E \leq 4r^2 - 4r \leq 4w^2 - 4w,$$

使得 $F_E(\lambda; A, B)\ \neq 0$，就存在一个 $\mu$，使得 Π 定义良好、非零且秩为一。因此，可以通过在任意大小为 $> 4w^2 - 4w$ 的网格上进行有限多项式避零来得到 Π。

**证明**

步骤 ***1***（角是全矩阵代数）。
由于 $E$ 是秩为 $r$ 的幂等元，存在 $P \in \mathrm{GL}_w(\mathbb{K})$，使得

$$PEP^{-1} = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}.$$

通过 $P$ 的共轭可得到

$$E\mathrm{Mat}_w(\mathbb{K})E \ \cong\ \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}\ \mathrm{Mat}_w(\mathbb{K}) \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}\ \cong\ \mathrm{Mat}_r(\mathbb{K}).$$

这就证明了 (1)。

步骤 ***2***（在角代数中构造一个“一般铅笔”。）
固定 $r \geq 2$。考虑角线性铅笔 $T(\lambda) := E(A + \lambda B)E \in E\mathrm{Mat}_w(\mathbb{K})E$ .

令 $p(\mu, \lambda) := \det\ (\mu E - T(\lambda))$，其中行列式在角代数中解释（等价地，先用 $P$ 进行共轭，再取 $r \times r$ 左上角块的行列式）。

那么，$p(\mu, \lambda)$ 是一个二元多项式，其中：$\deg\ _\mu p = r$、$\deg\ _\lambda p \leq r$，且 $p$ 是 $A$、$B$ 的元素的多项式。

步骤 ***3***（单特征值 + 非零伴随矩阵是代数开条件）。

令 $D(\lambda; A, B) := \mathrm{Disc}_{\mu}(p(\mu, \lambda))$，并令 $m(\mu, \lambda)$ 为 $\mu E - T(\lambda)$ 的任意固定的 $(r-1)$ 阶 $\times (r-1)$ 子式（同样在角块中计算）。

定义 $R(\lambda;\ A, B) := \mathrm{Res}_{\mu}(p(\mu, \lambda),\ m(\mu, \lambda))$，并设 $F_E(\lambda;\ A, B) := D(\lambda;\ A, B) \cdot R(\lambda;\ A, B)$ .

- 若 $D(\lambda;\ A, B) \neq 0$，则对于 $p(\mu, \lambda)$ 的每个根 $\mu$，其在角代数中的特征值都是单特征值；因此 $\mathrm{rank}(\mu E - T(\lambda)) = r - 1$。• 若进一步有 $R(\lambda;\ A, B) \neq 0$，则存在一个根 $\mu$，使得某个 $(r-1)$ 阶 $\times (r-1)$ 子式非零，因此 $\mathrm{adj}\ (\mu E - T(\lambda)) \neq 0$。

对于这样的（$\lambda$；$A$，$B$），定义 $\Pi$: $= \mathrm{adj}\ (\mu E - T(\lambda)) \in E\mathrm{Mat}_w(\mathbb{K})E$。

$r$ 阶的标准伴随矩阵线性代数给出：秩$(\Pi) = 1$。

最后，由于 Π 秩为一且属于角代数，在乘以一个非零标量后（这不会影响秩），我们得到一个幂等元：$\Pi^2 \propto \Pi$。

（等价地，也可以用 Π的任意非零元素进行归一化；如果你坚持在不进行缩放的情况下实现严格的幂等性，则可以稍后以同样的方式通过有限回避来完成归一化。）

步骤 ***4***（次数界）。
与全局情形完全相同，$\lambda$ 中的次数界由以下内容推出：

- $_{\lambda} p \leq r$ 次 ，次
- $_{\lambda} D \leq 2r-2$ $_{\lambda} p \leq 2r-2$ $r$ ( )次 ( ), 次 $_{\lambda} R \leq r$
- $r-1 + r-1\ r = 2r$

( ) ( ) $(r-1)$, 因此 次 $_{\lambda} F_E \leq (2r-2)r + 2r(r-1) = 4r^2 - 4r$。

对于 $A, B$ 中元素的次数，同样的界也成立（相差至多相同的多项式因子）。这就证明了 (3)。

步骤 ***5***（有限回避）。

由于 $F_E \equiv /0$（选择 $A, B$，使角块为具有互异特征值的对角矩阵，例如角块中为 $A = \mathrm{diag}(1,2, \ldots, r)$，且 $B = 0$），引理 4.8 表明，在任意大小为 $>$ 次 $F_E$ 的网格上，都存在 $(\lambda;\ A, B)$，满足 $F_E(\lambda;\ A, B) \neq 0$。对于这样的选择，上述构造会产生所需的秩一角幂等元 Π。■

引理 *4.12*（秩下降的终止）

反复应用引理 4.11 会使秩严格下降，并且至多经过 $w-1$ 步便会终止于一个秩一幂等元。

证明

秩是一个不超过 $w$ 的正整数，并且每一步都会严格递减。■

### 4.4.5 主定理：确定性秩一投影算子提取

定理 *4.* *13* 通过有限回避进行无特征值（有理）秩一投影算子提取 )

假设在特化 $\chi$ 下，$\mathrm{B}(\chi) = \mathrm{Mat}_w(\mathbb{K})$。

那么存在一个显式多项式映射 $\Phi\colon \mathrm{Mat}_w(\mathbb{K}) \longrightarrow \mathrm{Mat}_w(\mathbb{K})$，以及一个矩阵字 $W \in \mathrm{B}(\chi)$，使得 $\Phi(W)$ 是非零秩一幂等元，且构造中的每一步均由总次数为 $O(w^2)$ 的显式多项式约束所控制。特别地，可以通过有限多项式避零，在大小为关于 $w$ 的多项式的网格上确定性地完成提取。

证明

我们分四个代数阶段进行，每个阶段都由有限多项式避零所控制 e.

步骤 ***1***：构造可逆矩阵字

根据引理 4.1，行列式见证多项式 $\Delta(\mathbf{z}) = \det\left(\sum_{j=1}^{w^2} z_j W_j\right)$ 非零。因此，存在一种特化 $\mathbf{z}^*$，使得 $M := \sum_{j=1}^{w^2} z_j^* W_j$ 可逆。由于 $\deg(\Delta) \le w$，引理 4.8（有限回避）保证可从大小为 $> w$ 的网格中选出这样的值。因此，$M \in \mathrm{B}(\chi)$ 可逆。

步骤 ***2***：提取非零幂等元（凯莱–哈密顿）

根据引理 4.2，存在一个次数至多为 $w-1$ 的多项式 $p(t)$，使得 $E := p(M)$ 是一个非零幂等元：$E^2 = E, E \neq 0$。$p$ 的所有系数都是 $M$ 的元素的多项式函数，因此关于只读代数分支程序参数呈多项式依赖。不使用除法。

令 $r := \mathrm{rank}(E) \ge 1$。

步骤 ***3***：角代数中的秩一提取（使用引理 4.11）

如果 $r = 1$，则我们就完成了。

假设 $r \ge 2$。将引理 4.11 应用于幂等元 $E$，存在矩阵 $A, B \in \mathrm{Mat}_w(\mathbb{K})$ 和一个标量 $\lambda$，满足单个显式多项式非零条件 $F_E(\lambda; A, B) \neq 0$，其中

$$\deg F_E \le 4r^2 - 4r \le 4w^2 - 4w,$$

使得对于某个特征值 $\mu$，$\Pi := \mathrm{adj}(\mu E - E(A + \lambda B)E)$ 是一个位于角代数 $E\mathrm{Mat}_w(\mathbb{K})E \subseteq \mathrm{Mat}_w(\mathbb{K})$ 内的非零秩一幂等元。

步骤 ***4***：字代数内的有限回避实现

由于 $\mathrm{B}(\chi) = \mathrm{Mat}_w(\mathbb{K})$，我们可以选取 $A$和 $B$为第 3 节中张成集里的矩阵字，从而确保：
$A\ B \in \chi$ 4 $F_E \equiv /0$ $\lambda\ A\ B$ >，B( )。根据引理 .8，由于，我们可以从大小为 的网格中选取 ( ; , )，使得该约束成立。 $4w^2 - 4w$

因此，所构造的秩一投影算子 Π 为：

- 非零
- 秩一
- 幂等元 • 多项式可计算 • 完全包含于矩阵词代数

结论

定义Φ 为以下各项的复合：

1. 行列式见证求逆，2. Cayley–Hamilton幂等元提取，3. 角伴随提取（引理 4.11）。

随后，Φ(*W*) 会产生一个秩一幂等元，其构造不需要除法，受明确的次数界，控制，并且可以通过有限多项式避零实现。这就完成了证明。■

**第 4 节的概念性总结**

我们已经确立了一个**确定性代数谱提取原理**：

- 矩阵表达力完备意味着存在可逆字元素 • 凯莱–哈密顿定理产生一个非零幂等元 • Amitsur–Levitzki 定理迫使秩坍缩 • 有限回避确保所有约束同时成立 • 无需除法或随机性即可提取出一个秩一投影算子

这个秩一投影算子将在下一节中充当**代数探针，使次数三角化和基于曲线的非消去成为可能**。

## 4.5 在字代数中传递秩一方向

令 Π ∈B(*χ*) 为定理 4.13 得到的秩一幂等元。

由于 B(*χ*) =Mat*w*(𝕂)，投影算子 Π 在全矩阵代数中刻画出一个一维子空间。现在我们将证明，这个一维方向可以通过完全代数化且次数受控的方式进行传递，从而生成一个由向量和余向量组成的张成系。

引理 *4.14*（秩一轨道张成引理）

存在矩阵字 $U_1, \dots, U_w, V_1, \dots, V_w \in \mathrm{B}(\chi)$，使得向量 $U_k \Pi e_w (1 \le k \le w)$ 构成 $\mathbb{K}^w$ 的一个张成集，且余向量 $e_1^\top \Pi V_k (1 \le k \le w)$ 构成对偶空间 $(\mathbb{K}^w)^*$ 的一个张成集。

证明

由于 Π 的秩为一，存在非零向量 $u$、$v \in \mathbb{K}^w$，使得 $\Pi = uv^\top$。

由于 $\mathrm{B}(\chi) = \mathrm{Mat}_w(\mathbb{K})$，对于每个标准基向量 $e_i$，都存在一个满足 $U_i u = e_i$ 的矩阵字 $U_i$ 。类似地，对于每个对偶基向量 $e_i^\top$，都存在一个满足 $v^\top V_i = e_i^\top$ 的矩阵字 $V_i$ 。

于是 $U_i \Pi e_w = U_i(uv^\top)e_w = (v^\top e_w)e_i$，并且由于 $v^\top e_w \neq 0$，向量 $\{U_i \Pi e_w\}$ 张成 $\mathbb{K}^w$。对偶的张成陈述 аналогously 成立。■

推论 *4.15*（矩阵单位生成）

存在矩阵字 $W_{ij} \in \mathrm{B}(\chi)$ 使得 $W_{ij} = e_i e_j^\top$，即字代数包含一个完整的矩阵单位系。

**证明**

定义 $W_{ij} := U_i \Pi V_j$。于是 $W_{ij} = (U_i u)(v^\top V_j) = e_i e_j^\top$，从而在 $\mathrm{B}(\chi)$ 内建立了显式的矩阵单位。■

推论 *4.16*（非退化双线性配对接口）

双线性型 $X, Y := e_1^\top X \Pi Y e_w$ 在 $\mathrm{Mat}_w(\mathbb{K})$ 上是非退化的。等价地，格拉姆矩阵 $G_{ij} := e_1^\top W_{ij} \Pi e_w$ 是可逆的。

**诠释**

投影算子 Π 现在充当一个秩一代数探针，它：

- 区分所有矩阵方向，• 通过标量配对实现系数提取，• 并确保后续行列式展开在结构上必然呈现非消去。

这构成了次数三角化所需的精确代数接口。

### 4.6 第 4 节的结构性输出

我们总结本节所构建的结构性工具。

定理 *4.17*（无特征值（有理）谱原语）

根据假设 $\mathrm{B}(\chi) = \mathrm{Mat}_w(\mathbb{K})$，我们仅使用多项式恒等式和有限避开论证构造了：

1. 一个用于证明可逆矩阵字存在的**行列式见证** 2. 一个不需要特征值除法的**Cayley–Hamilton 幂等元提取器** 3. 一个由显式多项式约束控制的**秩一投影算子提取**（引理 4.11，定理 4.13） 4. 一个从秩一投影算子生成完整矩阵单位的**传输系统** 5. 一个能够实现系数恢复的**非退化双线性配对**

所有步骤都能给出关于$w$的**显式多项式次数界**，因此仍与确定性有限回避特化兼容。

**概念性解读**

本节构造一个**无特征值（有理）谱原语**:
嵌入字代数中的秩一代数探针，完全由多项式恒等式推导而来，而非解析特征值理论。

这一基本构件将在证明余下部分充当刚性锚点。

**第5节的衔接（次数三角化）**

在第5节中，我们利用由 Π 诱导的矩阵单位基，对行列式展开施加次数层**级**。

推论 4.16 中的非退化双线性配对将确保恰有一个单项式项保留下来，从而防止代数曲线代入导致消去。

这就构造出了一个显式的确定性曲线型命中集，其中有限次数回避可用于证明代数构造的正确性。

### 4.7 模稳定性猜想与条件性全多项式时间黑盒多项式恒等性检验

**动机。**
第 3–7 节利用矩阵词代数的代数刚性、有限回避约束和曲线代入，构造了一种确定性黑盒多项式恒等式检验过程。要实现全多项式时间黑盒多项式恒等性检验（关于 $n$、 $w$、 $d$ 的多项式时间），剩下的障碍是命中集仍依赖于高次数的曲线分离。我们提出一种自然的“模哈希”改进方案，通过将曲线求值压缩到一个小的循环环中来消除此依赖。该改进方案的正确性由以下猜想刻画。

#### 4.7.1 定义（代入到循环商环中的模替换）

固定一个素数 $r$ 满足 $\gcd\ (r, \mathrm{char}(\mathbb{K})) = 1$，并定义循环商环 $R_r := \mathbb{K}[\lambda]/\langle \lambda^r - 1 \rangle$.

对于 $g \in \mathbb{Z}_r^*$，定义模替换 $\Gamma_g$ 为 $\Gamma_g: x_i \mapsto \lambda^{g^i} \in R_r$，其中指数按模 $r$解释，且 $\lambda^r = 1$ 在 $R_r$中。

对于 $C \in \mathbb{K}[x_1, \ldots,\ x_n]$，记 $C_g(\lambda) := C(\Gamma_g) \in R_r$。

#### 4.7.2 猜想（模稳定性／铰链猜想）

猜想 *4.7.2*（模稳定性）。

存在一个显式多项式 $R(w, d)$ 和一个绝对常数 $\varepsilon > 0$，使得对于每个由宽度为 $w$、次数为 $d$ 的只读代数分支程序计算的非零多项式 $C$，以及每个素数

$$r \geq R(w, d) \text{ (e.g., typically } r \geq (wd)^7),$$

坏集合

$$\mathcal{B}_r(C) := \{\, g \in \mathbb{Z}_r^* : C_g(\lambda) \equiv 0 \text{ in } \mathbb{K}[\lambda]/\langle \lambda^r - 1 \rangle \,\}$$

满足$|\mathrm{B}_r(C)| \leq r^{1-\varepsilon}$。

注（结构化例外与紧性）。

猜想 4.7.2 中界的形式在定性意义上是紧的，具体来说，对于任意固定参数 $g \in \mathrm{Z}_r^*$，都存在被循环哈希代换 $x_i \mapsto \lambda^{g^i}$消去的非零多项式 $C$ （例如，两个单项式之差）。这类障碍源于指数向量 $g^i mod\ \ r$之间的加性碰撞。

不过，目前已知的所有这类构造都具有高度结构化且代数退化的特征。具体而言，它们都可以由有效宽度极小（常数或对数级）的只读代数分支程序计算，而且其系数支撑呈现出极低的代数密度。这些例子表明，我们不能期望哈希映射对所有多项式和所有参数 $g$都具有一致的单射性。

猜想 4.7.2 讨论的是互补情形。它预先固定多项式 $C$ ，使其为宽度-$w$、次数-$d$ 的只读代数分支程序，并断言——除这类高度退化的情形外——发生完全模坍缩的参数 $g$ 集合是稀疏的。具体而言，针对特定选择的 $g$ 量身定制 $C$ 的对抗性构造并不与该猜想矛盾。

算术几何中的启发式结果，例如结构化指数和中的平方根消去现象，表明一般 ROABP 可能满足界 $|\mathrm{B}_r(C)| \leq r^{1/2+o(1)}$ 。然而，我们的主要算法结果（定理 7.5）只要求 $\varepsilon > 0$ 是一个固定的绝对常数（例如，$\varepsilon = 0.1$ 就足够了）。

澄清

猜想 4.7.2 对每个固定的多项式 $C$，界定了坏参数 $g$ 的数量。它并未声称对于固定的 $g$，哈希映射对所有多项式都一致地具有单射性，也不排除存在孤立的结构化反例。

**例 4.7.3（二单项式碰撞障碍）**。

固定一个素数 $r$和 $g \in \mathrm{Z}_r^{\backslash *}$。令 $v_i := g^i mod r$。若存在两个不同的子集 $S, S' \subseteq [n]$ ，使得

$$\sum_{i \in S} v_i \equiv \sum_{i \in S'} v_i \ (\mathrm{mod} r),$$

那么非零多项式

$$C(x_1, \ldots, x_n) := \prod_{i \in S} x_i \ - \prod_{i \in S'} x_i$$

在哈希代换 $x_i \mapsto \lambda^{v_i}$ 下，满足 $C_g(\lambda) \equiv 0$ in $\mathbb{K}[\lambda]/\lambda^r - 1$。特别地，对于这个 $C$ ，我们有 $g \in \mathrm{B}_r(C)$。

证明。 在 $x_i \mapsto \lambda^{v_i}$, $C_g(\lambda) = \lambda^{\Sigma_{i \in S} v_i} - \lambda^{\Sigma_{i \in S}\ v_{i'}} \equiv 0 \ \ (\mathrm{mod} \lambda^r - 1)$ 下，因为指数模 $r$ 同余。□

注。

这种障碍是将多项式哈希到循环商环所固有的：它表明，对于固定的 $g$，存在专门构造的非零多项式 $C$，会被该映射消去。猜想 4.7.2 关注的是互补情形：此时 $C$ 预先固定为宽度为 $w$、次数为 $d$ 的只读代数分支程序，并断言这类会被消去的参数 $g$ 构成稀疏集合。

命题 *4.7.3*（特殊情形）。

猜想 4.7.2 对宽度为 2 的对角只读代数分支程序成立。

证明：

在对角情形中，系数是标量之和。模约化对指数起哈希作用，因此适用标准的稀疏多项式结果。

### 4.7.3 启发式验证（刚性 + 结构化单射性）

记

$$C_g(\lambda) = \sum_{k=0}^{r-1} a_k(g)\,\lambda^k, a_k(g) \in \mathbb{K}.$$

对于固定的$g$，每个系数$a_k(g)$是通过聚合那些指数模式在该映射下模$r$发生碰撞的单项式$x^{\mathbf{e}}$ 而得到的

$$\mathbf{e} \mapsto \langle \mathbf{e}, v(g)\rangle := \sum_{i=1}^{n} e_i\, g^i (\mathrm{mod} r).$$

因此$g \in \mathrm{B}_r(C)$当且仅当结构化聚合产生同时消去 ：

$$a_k(g) = 0 \text{ for all } k \in \mathbb{Z}_r.$$

猜想 4.7.2断言，对于只读代数分支程序系数族——其内在线性代数复杂度是有界的（经由前缀上的求值维数/系数空间界，维数为$w^2$ $g$ $r$ ）——一旦

目标维数以多项式方式大于内在维数，这种完全湮灭就不能对过多参数发生。虽然$\Gamma_g$ 是一个高度结构化的族，而非均匀随机线性映射，但该猜想认为，只读代数分支程序刚性阻止了与该结构化压缩的核的对齐，除非在一个稀疏例外集上。

### 4.7.4 经由特征和的数论表述

令 $\omega$ 是某个适当扩域中的本原 $r$ 次单位根。对 $t \in \mathbb{Z}_r$，定义

$$S_t(g) := \sum_{\mathbf{e}} c_{\mathbf{e}}\ \omega^{\,t\langle \mathbf{e}, v(g)\rangle}.$$

傅里叶反演将系数 $a_k(g)$ 表示为 $\{S_t(g)\}^{t\in\mathbb{Z}_r}$ 的形式。特别地，条件 $C_g(\lambda) \equiv 0$ 属于 $R_r$ 等价于对所有 $t \in \mathrm{Z}r$，$S_t(g) = 0$ 同时为零。因此，对 $|\mathrm{B}r(C)|$ 的上界估计归结为：在系数向量 $(c_e)$ 来源于宽度为 $w$ 的只读代数分支程序（ROABP）的约束下，控制一族结构化指数和随 $g$ 遍历 $\mathrm{Z}_r^{\backslash *}$ 时同时为零的次数。

### 4.7.5 条件定理（完全多项式时间确定性黑盒多项式恒等式检验）

假设猜想 4.7.2 成立。令 $r = \mathrm{poly}(w, d)$ 为满足 $r \geq R(w, d)$ 的素数。枚举所有 $g \in \mathrm{Z}_r^{\backslash *}$，并在 $R_r$ 中计算 $C_g(\lambda)$。由于坏值至多有 $r^{1-\varepsilon}$ 个，只要 $C \equiv/0$，就至少有一个 $g$ 是好的；对于该 $g$，我们可以在 $R_r$ 中得到 $C_g(\lambda) \equiv/0$。

由于 $|\mathrm{Z}_r^{\backslash *}| = r - 1 = \mathrm{poly}(w, d)$，且在 $R_r$ 上进行运算的代价为 $\mathrm{poly}(r)$，因此可得到一个确定性黑盒恒等式检验算法，其运行时间为 $\mathrm{poly}(n, w, d)$。

### 4.7.6 实验证据

我们在大型素数域上对随机和结构化的只读代数分支程序测试了猜想 4.7.2，扫描 $g \in \mathrm{Z}_r^{\backslash *}$ 中不超过 $10^4$–$10^7$ 的素数 $r$。在这些测试中，除退化的混叠情况（例如 $g = 1$ 导致强碰撞）外，我们没有观察到其他非平凡的坏参数。这些实验支持了该猜想的预测：$\mathrm{B}r(C)$ 通常极其稀疏。

## 5. 次数三角化与非消去（TRI 核心）

本节为矩阵词贡献施加次数层级，以确保某个行列式项占主导，从而防止消去。这种机制称为次数三角化（TRI）。

### 5.1 目标

根据第 4 节，我们有：

- 一个秩一投影算子 $\Pi(\lambda) = \mathrm{adj}\ (\mu I - X(\lambda))$、- 词族 $U_1(\lambda), \ldots, U_w(\lambda), V_1(\lambda), \ldots, V_w(\lambda)$，使得配对矩阵 $G_{kl}(\lambda)$ $e_1^{\top} U_k\ \lambda\ \Pi\ \lambda\ V\ \lambda\ e_w$ ( ) ( ) ı( ) 非退化。

我们的目标是为这些字添加受控的多项式次数，使得该矩阵的行列式具有唯一的最高次数项。

### 5.2 代数曲线代入

固定互不相同的域元素 $\alpha_1, \ldots, \alpha_n \in \mathbb{K}$，并定义曲线代入 $x_i = (\lambda + \alpha_i)^B$，其中 $B$ 是一个待指定的大整数。

令 $M_i(\lambda) = A_i((\lambda + \alpha_i)^B)$ 表示由此得到的关于 $\lambda$ 的矩阵多项式。

### 5.3 次数权重赋值

赋予 $a_1 < a_2 < \cdots < a_w, b_1 < b_2 < \cdots < b_w$ 严格递增的整数权重，并定义次数装饰词 $\widetilde{U}_k(\lambda) = U_k(\lambda)\, M(\lambda)^{a_k}, \widetilde{V}_\ell(\lambda) = M(\lambda)^{b_\ell}\, V_\ell(\lambda)$，其中 $M(\lambda)$ 是从 ROABP 层中固定选取的矩阵多项式。

注。迹配对仅用于证明活跃块中基元素的线性无关性。只读代数分支程序的输出本身是一个向量–矩阵–向量收缩，可通过引理 5.5 的唯一首项论证直接处理。

### 5.4 对角次数剖面的支配性

引理 *5.1*（活动子空间轨道张成）

存在词族 $U_1, \ldots, U_{r^2}, V_1, \ldots, U_{r^2} \in \mathrm{B}(\chi)$，使得双线性形式 $U_i \Pi V_j \psi := \mathrm{Tr}\ (\psi(U_i \Pi V_j))$ 张成 $\mathrm{Mat}_r(\mathbb{K})$ 的整个对偶空间。

Equivalently, the matrix $G_{ij} := \mathrm{Tr}\ (\psi(U_i \Pi V_j))$ has rank $r^2$.

证明

根据第 4 节中的构造，$\psi(\Pi)$ 是 $\mathrm{Mat}_r(\mathbb{K})$ 中的非零秩一幂等元。因此，存在非零向量 $u$、$v \in \mathbb{K}^r$，使得 $\psi(\Pi) = uv^\top$。

由于 $\psi(\mathrm{B}(\chi)) = \mathrm{Mat}_r(\mathbb{K})$，对于每个矩阵单位 $E_{ab} \in \mathrm{Mat}_r(\mathbb{K})$，都存在字 $U_{ab}$、$V_{ab} \in \mathrm{B}(\chi)$，使得 $\psi(U_{ab})\, u = e_a$、$v^\top \psi(V_{ab}) = e_b^\top$，其中 $\{e_1, \ldots, e_r\}$ 是标准基。

Then $\psi(U_{ab} \Pi V_{ab}) = \psi(U_{ab})\, uv^\top \psi(V_{ab}) = e_a e_b^\top = E_{ab}$.

因此，集合 $\{\, \psi(U_{ab} \Pi V_{ab}) : 1 \le a, b \le r \,\}$ 张成所有矩阵单位，进而张成 $\mathrm{Mat}_r(\mathbb{K})$。

由迹配对可知，泛函 $X \mapsto \mathrm{Tr}\ (E_{ab} X)$ 构成 $\mathrm{Mat}_r(\mathbb{K})$ 的对偶空间的一组基。因此，双线性形式 $\mathrm{Tr}\ (\psi(U_i \Pi V_j))$ 张成整个对偶空间。

这就证明了该断言。■

### 5.5 ROABP 计算的唯一首项（新）

现在我们证明，曲线代入所施加的次数三角化能够防止 ROABP 计算本身内部发生消去，而不仅仅是防止行列式见证内部发生消去。

**定义（单项式预算）**。化简为 $m \le w^2$ 个单变量次数至多为 $d$ 的变量后，可能的单项式数量至多为 $M := (d+1)^m \le (d+1)^{w^2}$。所有次数分离界均以 $M$ 表示。

**定义（结构次数界）**。令 $D_{\mathrm{struct}}$ 表示第 6 节中引入的有限个约束多项式的最大 $\lambda$-次数。由于这些约束涉及元素次数至多为 $d$ 的矩阵的行列式，我们取保守界

$$D_{\text{struct}} := K \cdot w^3 d \quad \text{（对于某个绝对常数 } K \geq 8\text{）。}$$

我们明确选择分离基数 $B$，使其满足 $B > 2(D_{\text{struct}} + \deg\ C + 1) \cdot M$。

这确保权重向量的贡献严格大于所有低阶扰动。

引理 *5.4.2*（克罗内克代换的唯一性）

设 $\mathbf{e}, \mathbf{e}' \in \mathrm{N}^m$ 是多项式 $C$ 中出现的两个不同指数向量。若选择分离基数 $B > D_{\max}$，则映射

$$\Phi(\mathbf{e}) = \sum_{j=1}^{m} e_j\, B^{j-1}$$

是单射。

证明。 这是由整数的 $B$ 进制表示的唯一性得到的。

注。我们的构造使用平移曲线 $x_j = (\lambda + \alpha_j)^{B^j}$。由于首项为 $\lambda^{B^j}$，$\Phi$ 的单射性保证不同单项式的最高次项会映射为$\lambda$的不同次幂，从而确保次数分离不受低阶移位的影响。

引理 *5.5*（曲线代换与模代换下的首项保留）。

设 $C(x_1, \ldots, x_n)$ 是只读代数分支程序计算的多项式，并假设 $C \equiv/0$。

**（i）曲线代入（无条件）**。
在曲线代入 $x_j \mapsto \lambda^{B^j}$ 中，取基数 $B$，如第 5.3 节所述，则所得单变量多项式 $C(\lambda) := C(\lambda^{B^1}, \ldots, \lambda^{B^n})$ 在 $\lambda$ 中有唯一的首单项式。特别地，$C(\lambda) \equiv/0$ 在 $\mathbb{K}[\lambda]$ 中。

**(ii) 模约化（有条件）**。
此外，在模替换 $x_j \mapsto \lambda^{g^j}$ 到 $R_r := \mathbb{K}[\lambda]/\langle \lambda^r - 1 \rangle$ 下，若 $g \notin \mathrm{B}r(C)$（即猜想 4.7.2 中的坏集合），则像 $C_g(\lambda)$ 在 $R_r$ 中非零。

证明。

**第 (i) 部分**。
根据构造（第 3–4 节），词 $W_i$ 投影为活跃单块的一组基，且系数多项式并非全为零。

代入 $x_j \mapsto \lambda^{B^j}$ 所诱导的次数分离，加上选择 $B$ 使其大于矩阵乘法和投影算子提取所产生的所有结构次数，确保恰有一个加项达到最大的 $\lambda$ 次数。这个主导项不会抵消，因此 $C(\lambda) \equiv/0$。

**（二）部分**。
根据猜想 4.7.2，使模特化消去该多项式的参数集合 $g$ 是稀疏的。对于任意 $g \notin \mathrm{B}r(C)$，第 (i) 部分中的非零多项式 $C(\lambda)$ 在模 $\lambda^r - 1$ 约化后仍然非零，因此 $C_g(\lambda) \equiv/0$ 属于 $R_r$。□

### 5.6 行列式展开中的唯一最高次项

设 $H_{k\ell}(\lambda) = e_1^{\top} \widetilde{U}_k(\lambda)\, \Pi(\lambda)\, \tilde{V}_\ell(\lambda)\, e_w$，并定义行列式见证 $\Delta(\lambda) = \det\ (H(\lambda))$。

引理 *5.2*（唯一最高次项引理）

在引理 5.1 的条件下，$\Delta(\lambda)$ 的行列式展开中包含一个唯一的最高次数单项式，该单项式来自对角置换。

证明

根据引理 5.1，每个非对角置换在 $\lambda$ 中产生的总次数都严格较低。因此，最高次数项不可能发生消去，对角项得以唯一保留。■

### 5.7 首项系数的非零性

引理 *5.3*（最高次项系数非零性）

$\Delta(\lambda)$ 中最高次数单项式的系数非零。

证明

最高次项系数等于 $\det\ (G_{k\ell}(\lambda))$，其中 $G_{k\ell}(\lambda)$ 是第 4 节中的非退化配对矩阵。由于该矩阵可逆，其行列式非零，这意味着 $\Delta(\lambda)$ 的最高次项系数非零。■

### 5.8 推论：行列式见证在代入后仍然成立

推论 *5.4*

行列式见证 $\Delta(\lambda)$ 是关于 $\lambda$ 的非零单变量多项式。

因此，当且仅当 $\Delta(\lambda)\ \equiv/0$ 时，原 ROABP 多项式非零。

### 5.9 见证多项式的次数界

引理 *5.4.1*（活跃块首项保持）

设 $\Delta(\lambda) = \det\ (H(\lambda))$ 为第5.6节中构造的行列式见证。根据引理 5.1，矩阵元素 $H_{kl}(\lambda)$ 是基元素的迹配对，这些基元素张成活跃块 $\mathrm{Mat}_r(\mathbb{K})$。次数权重的选取旨在确保唯一的对角首项与这些基配对的乘积相对应。

由于基张成活跃块，配对矩阵 $G$ 在活跃块中是非退化的（推论 4.16），这意味着其行列式在 $\psi$ 下非零。

**结论：** $\Delta(\lambda)$ 的唯一首项系数为 $\det\ (G)$，它满足 $\psi(\det\ (G)) \neq 0$。因此，投影到活跃块后仍能保持次数分离。

引理 *5.6*（次数界）

$\Delta(\lambda)$ 的总次数满足 $\deg_\lambda \Delta(\lambda) \le 2d^2w^8$。

证明

$H(\lambda)$ 的每个元素都是至多 $O(w^2)$ 个次数至多为 $Bd$ 的矩阵多项式的乘积。$w \times w$ 矩阵的行列式将 $w$ 个此类元素相乘，从而得到所述次数界。■

### 5.10 第 5 节总结

我们已经证明：

1. 行列式见证在曲线代入后会获得唯一的最高次数项。2. 可以证明，最高次数项不可能发生消去。3. 由此得到的单变量多项式非零，且具有明确的次数界。

这完成了**TRI 机制**，通过次数分离确保代数**非消去**。

## 6. 选择引理与有限多项式避零（SEL）

本节通过证明存在一个参数值能够同时满足所有代数非退化约束，消除了构造中剩余的所有非确定性。这一步以显式的有限避开论证取代了概率泛性。

**一般非消失原理**。为确保命中集具有通用性，我们针对每个候选秩 $r \in \{1, \dots, w\}$，在一般矩阵代数 $\mathrm{Mat}_r(\mathbb{K}[X])$ 上以句法方式定义约束多项式 $F_r$，完全独立于输入 ROABP。通过在一般空间中展示一个单一的形式见证（例如对角矩阵），可以证明它们的非零性。最终的命中集避开通用乘积 $\prod_{r=1}^{w} F_r$，从而确保：如果输入 ROABP 非零（因此具有某个秩为 $r^*$ 的活跃块），则相应的约束 $F_{r^*}$ 得到满足。在 ROABP 恒等为零的平凡情形下，命中集构造仍然定义良好，并且算法在求值时正确返回零。

### 6.1 代数约束的性质

第 4 节和第 5 节中的构造要求多个性质同时成立，包括：

1. 矩阵族 $X(\lambda)$ 存在单特征值 2. 秩一伴随投影算子非零 3. 配对矩阵非退化 4. 满足次数三角化支配条件

每个这样的要求都可以表示为标量参数 $\lambda$ 的**多项式的非零性**。我们将这些约束多项式记为：$F_1(\lambda), \dots, F_R(\lambda) \in \mathbb{K}[\lambda]$。

### 6.2 显式多项式约束

我们简要回顾这些多项式的由来。

- 通过判别式来施加**单谱约束**：

$$F_{\text{disc}}(\lambda) = \text{Disc}_{\mu}(\det(\mu I - X(\lambda))).$$

- 投影算子非消失约束由一个结式强制实现：

$$F_{\text{proj}}(\lambda) = \text{Res}_{\mu}(\det(\mu I - X(\lambda)), m(\mu, \lambda)),$$

其中，$m(\mu, \lambda)$是$\mu I - X(\lambda)$的一个固定的$(w-1) \times (w-1)$子式。

- 通过一个行列式结式强制实现**配对非退化约束**：

$$F_{\text{pair}}(\lambda) = \text{Res}_{\mu}(\det(\mu I - X(\lambda)), \det G(\mu, \lambda)),$$

$G$ 是来自第 4 节的配对矩阵。

- 通过确保首项系数不为零来强制实现**次数三角化约束**，并将其编码为有限个标量行列式条件。

**见证**。取$M = \text{diag}(1, \dots, r)$可得$F_{\text{disc}} \equiv /0$。令$A = I, B = 0$ 可知配对约束非零。

如前几节所述，每个 $F_i(\lambda)$ 都是一个**非零单变量多项式**。

### 6.3 约束多项式的次数界

现在，我们来界定 $\lambda$ 中每个约束多项式的次数。

引理*6.1*（判别式约束的次数）

$$\deg_{\lambda} F_{\text{disc}}(\lambda) \le 2w^2.$$

引理*6.2*（投影结式约束的次数）

$$\deg_{\lambda} F_{\text{proj}}(\lambda) \le 2w^2.$$

引理*6.3*（配对行列式约束的次数）

$$\deg_{\lambda} F_{\text{pair}}(\lambda) \le 2w^3.$$

引理 *6.4*（*TRI* 首项系数约束的次数）

$$\deg_{\lambda} F_{\text{tri}}(\lambda) \le 2w^3.$$

证明（引理 *6.1–6.4*）

每个界都源于对判别式、结式和行列式的标准次数估计，并利用了以下事实：$X(\lambda)$、$U_k(\lambda)$ 和 $V_k(\lambda)$ 中的所有矩阵元素关于 $\lambda$ 都是仿射线性的。■

### 6.4 总次数界

令 $F(\lambda) = \prod_{i=1}^{R} F_i(\lambda)$ 表示所有约束多项式的乘积。

引理 *6.5*（总次数界）。

$$\deg_{\lambda} F(\lambda) \le 8w^3.$$

证明。

将引理 6.1.6.4 $2w^2 + 2w^2 + 2w^3 + 2w^3 = 4w^2 + 4w^3 \le$ . –. 中的次数界相加，可得（对于 $8w^3$ $w \ge 1$ ■
）。

### 6.5 选择引理（有限多项式避零）

现在陈述关键的选择原理。

引理 *6.6*（有限回避）。
设 $F(\lambda) \in \mathbb{K}[\lambda]$ 是一个次数至多为 $D$ 的非零单变量多项式。设 $L \subseteq \mathbb{K}$ 是任意满足 $|L| > D$ 的有限子集。

那么存在 $\lambda^{\star} \in L$ 使得 $F(\lambda^{\star}) \neq 0$。

证明。
次数至多为 $D$ 的非零单变量多项式在 $\mathbb{K}$ 中至多有 $D$ 个根。由于 $|L| > D$，至少有一个 $\lambda^{\star} \in L$不是 $F$ 的根，因此 $F(\lambda^{\star}) \neq 0$。■

在我们的应用中，多项式 $F(\lambda)$ 是以下约束多项式的乘积：这些约束分别来自（i）活跃块中的特征值分离，（ii）伴随矩阵子式非零，以及（iii）次数-三角化约束。根据引理 3.1.1，我们进一步将候选集 $L$ 与保持活跃块的特化的 Zariski 开稳定集 $\Omega$ 相交。由于 $\Omega$ 在任何足够大的有限网格中都是余有限的，同样的有限避零论证也适用于 $L \cap \Omega$。

推论 *6.7*（同时有限回避）。设 $F_1, \dots, F_m \in \mathbb{K}[\lambda]$ 为非零多项式，
且 $\sum \deg\left(\prod_{i=1}^{m} F_i\right) \le D$。

那么，对于任意满足 $|L| > D$ 的 $L \subseteq \mathbb{K}$，存在 $\lambda^{\star} \in L$，使得对于所有 $i = 1, \dots, m$，均有 $F_i(\lambda^{\star}) \neq 0$ 。

#### 6.5.1 通用并集策略（算法块独立性）

我们不会通过算法确定活跃块秩 $r$ 或同态 $\psi$，而是针对所有可能的秩 $r \in \{1, \dots, w\}$构造约束，并取它们的并集。

对于每个 $r$，定义一个形式化约束族 $F_r(\lambda; Z)$，其中 $Z$ 表示符号矩阵词项。该多项式是通过对一个一般的 $r \times r$ 矩阵代数应用投影算子提取过程（第 4 节）和次数分离构造（第5节）得到的。这些约束族是**语法上的**：它们不需要计算 $\mathrm{B}(\chi)$ 的韦德伯恩分解。

如果真实的活跃块的秩为 $r^\star$，那么在特化下，实例化多项式 $F_{r^\star}(\lambda)$ 与引理 4.11 和引理 5.5 中导出的真正非退化约束一致。

我们定义**通用避零多项式**

$$F_{\text{univ}}(\lambda) := G_{\text{stab}}(\lambda) \cdot \prod_{r=1}^{w} F_r(\lambda),$$

其中 $G_{\text{stab}}(\lambda)$ 是引理 3.1.1 中的稳定性多项式。由于每个因子 $F_r(\lambda)$ 的次数至多为 $8w^3$（引理 6.5），通用多项式的总次数满足 $\deg F_{\text{univ}} = \text{poly}(w)$。推论 *6.8*（确定性选择）。

设 $L \subseteq \mathbb{K}$ 是一个有限网格，且 $|L| > \deg(F_{\text{univ}})$。那么存在 $\lambda^* \in L$，使得 $F_{\text{univ}}(\lambda^*) \neq 0$。

此选择保证正确性，无需显式识别活跃块或计算同态 $\psi$。

### 6.6 同时有效参数的存在性

推论 *6.9*

若 $|L| > 5w^3$，则存在 $\lambda^\star \in L$，使得第 4 节和第 5 节所需的所有代数约束同时成立。

证明

将引理 6.6 应用于 $F(\lambda)$。■

### 6.7 确定性参数选择算法

现在我们得到一个明确的确定性规则：

1. 枚举取值 $\lambda \in L$2. 计算所有约束多项式 $F_i(\lambda)$ 3. 选择第一个使其均不为零的 $\lambda^\star$

这需要关于 $w$的多项式时间，并且完全确定性。

### 6.8 第 6 节总结

我们已经：

- 将所有必要的代数泛性要求编码为显式的非零多项式 • 证明了其总次数的多项式上界
- 利用有限根规避保证有效特化的存在 • 以显式有限消去取代随机性，完成了确定性 TRI 框架

这解决了确定性构造的最后一个障碍，并为最后一节中的**曲线击中论证**做好了准备。

## 7. 曲线击中与证明的完成

在最后一节中，我们将第4–6节构造的代数见证转化为**显式确定性击中集**，从而完成主定理的证明。

### 7.1 目标

根据第 5 节和第 6 节，我们构造出了一个**非零单变量多项式**$\Delta(\lambda) \in \mathbb{K}[\lambda]$，其非零性可证明原始只读代数分支程序计算的是一个非零多项式。我们的目标是确定性地选取一个值 $\lambda^{\star}$，使得 $\Delta(\lambda^{\star}) \neq 0$，然后将这一选择反向提升为原始只读代数分支程序变量的一个显式输入赋值。

### 7.2 见证多项式的次数界

回顾引理 5.5，$\deg_{\lambda} \Delta(\lambda) \leq 2d^2w^8$。

引理*7.1*（见证多项式的根数上界）

多项式 $\Delta(\lambda)$在 $\mathbb{K}$中至多有 $2d^2w^8$ 个根。

证明

这直接由代数学基本定理得出。■

### 7.3 曲线击中集的构造

定义求值集合 $L = \{0,1,2,\dots, M\}$，其中：$M = 9w^4 + 2d^2w^8 + 1$。（注意：$2d^2w^8$ 项来自行列式见证 Δ，因此为稳妥起见，我们将它们相加。）

引理*7.2*（曲线击中引理）

存在 $\lambda^{\star} \in L$，使得 $\Delta(\lambda^{\star}) \neq 0$。

证明

由于 $|L| = M + 1 > \deg_{\lambda} \Delta(\lambda)$，引理 6.6 保证了此类 $\lambda^{\star}$ 的存在。■

### 7.4 将参数提升为完整变量赋值

回顾第5节中定义的曲线代入：$x_i = (\lambda + \alpha_i)^B$，其中 $B$ 和 $\alpha_i$ 均为确定性选取。

定义**命中赋值** $x_i^{\star} = (\lambda^{\star} + \alpha_i)^B$，$i = 1$、……、$n$。

引理 *7.3*（命中集的正确性）

设 $C(x_1, \dots, x_n)$ 是由只读代数分支程序计算得到的多项式，并假设 $C \equiv /0$。

设 $x_j \mapsto \lambda^{w_j}$ 为第5节中定义的代数曲线代入，其权重满足第 5.3 节的分离条件。

Th因此，存在一个有限例外集 $\mathrm{E} \subset \mathbb{K}$，使得对于所有 $\lambda^* \in \mathbb{K} \setminus \mathrm{E}$，$C(\lambda^*) \neq 0$。

证明

根据引理 5.5（ROABP 计算的唯一首项），限制多项式 $C(\lambda)$:
$C\ \lambda^{w_1} \quad \lambda^{w_n}$ $\lambda$ $C\ \lambda$ = ( , ..., ) 在 中有唯一的首单项式。特别地，( ) 是一个非零单变量多项式。

令 $L(\lambda)$ 表示首单项式的系数。由于 $L(\lambda)$ 是一个系数属于$\mathbb{K}$的非零多项式，它仅在有限多个点上取零。定义 E 为这个有限零点集。

对于任意 $\lambda^* \notin \mathrm{E}$，$C(\lambda^*)$ 的首项均不为零，且不会被低次数项抵消。因此，$C(\lambda^*) \neq 0$。■

关于认证的注。

引理 5.5 确立了曲线编码的 ROABP 多项式 $C(\lambda)$ 的次数结构。其非零性由行列式见证 $\Delta(\lambda) := \det(H(\lambda))$ 认证，其中 $H(\lambda)$ 是对计算进行编码的带标记配对矩阵。根据引理 5.4.1，次数三角化确保 $\Delta(\lambda)$ 有唯一的首项，因此 $\Delta(\lambda) \equiv/0$。根据可靠性链（推论 3.3），这证明原始 ROABP计算 $C(x)$ 不恒为零。

### 7.5 显式命中集大小

命中集由 $\lambda \in L$ 所诱导的所有曲线点组成。

定理*7.4*（命中集大小界（无条件））。
由此得到的确定性命中集大小为 $|H| \leq n \cdot (wd)^{O(w^2)}$，其构造时间关于 $n$ 为多项式级，关于 $w$、$d$ 为准多项式级。此处 $m \leq w^2$ 表示约化后的有效变量数量（推论 3.6）；命中集是在完成该约化后构造的。

证明。

我们使用移位幂曲线 $x_j = (\lambda + \alpha_j)^B$ 实现 Kronecker 式变量分离。按照第 5.5 节的方式选取分离基数 $B$（相对于有效单项式数量，是关于 $w$、$d$ 的多项式），可得到一个次数至多为 $B \cdot M = (wd)^{O(w^2)}$ 的单变量多项式，其中 $M$ 是约化后单项式空间的上界。这决定了命中集大小。关于 $n$ 的线性依赖来自计算变量约化映射。■

### 7.6 主定理的完成

现在我们将所有结果结合起来。

定理 *7.5*（多项式时间黑盒多项式恒等性检验）。
假设模稳定性猜想 (4.7.2) 成立，则存在一个大小为 $\mathrm{poly}(n, w, d)$ 的显式确定性命中集。

证明。

这可由算法 1 中对 $g \in \mathbb{Z}_r^*$ 的枚举得出，相关分析见第 7.8 节。具体而言，命中集大小对应于素数模数 $r$，其选取满足：对于一个显式常数（例如 $c = 7$），有 $r = O((wd)^c)$；该常数由要求 $r$ 严格大于定义在 $w^2$ 维矩阵代数上的代数约束的次数而得。□

### 7.7 算法

现在我们在假设猜想 4.7 成立的前提下，给出模哈希算法。无条件的基于曲线的算法已包含在该框架中，为简洁起见不再赘述。

算法 定理 1：只读代数分支程序的确定性黑盒多项式恒等式检验（条件是模稳定性 y)

**输入**。
对由域 $\mathbb{K}$ 上宽度为 $w$、个别次数为 $\leq d$ 的只读代数分支程序计算出的多项式 $C(x_1, \ldots, x_n)$ 进行黑盒访问。

**输出**。
若 $C \equiv 0$，则输出**零**；否则输出**非零**。

步骤 ***1***：选择一个模哈希环

$r =$ $w$ $r$ $=$
选择一个素数 $\mathbb{K}[\lambda]$ $\lambda^r - 1$ 多项式

$(, d)$ ，满足 最大公约数 $(,$ 特征 $(\mathbb{K})) = 1$，并定义循环商环 $R_r$: /。

步骤 ***2***：枚举哈希参数并构造单变量特化

对于每个 $g \in \mathbb{Z}_r^{\backslash *}$，定义模替换 $\Gamma_g$: $x_i \mapsto \lambda^{g^i} \in R_r$，其中指数按模 $r$计算，并且 $\lambda^r = 1$属于 $R_r$。
定义所得的单变量特化 $C_g(\lambda)$: $= C(\Gamma_g) \in R_r$。

步骤 ***3***：环求值（黑盒）

对于每个 $g \in \mathbb{Z}_r^{\backslash *}$，使用对 $C$ 的黑盒访问，按如下方式计算 $C_g(\lambda) \in R_r$：

1. 固定 $\mathbb{K}$-基 $\{1, \lambda, \ldots, \lambda^{r-1}\}$，用于表示 $R_r$。 2. 在输入赋值 $x_i = \lambda^{g^i}$ 处对 $C$ 求值，其中输入位于 $R_r$ 内（即将每个 $x_i$ 解释为环元素$\lambda^{g^i}$）。 3. 获得输出元素 $C_g(\lambda) \in R_r$ ，并将其写成系数形式 $\sum_{k=0}^{r-1} a_k \lambda^k$。

If f或者，对于任意 $g$ ，所得元素满足 $C_g(\lambda) \neq 0$ 在 $R_r$ 中，则输出 **非零** 并停止 .

步骤 ***4***：判定

如果对于所有 $g \in \mathbb{Z}_r^*$，$C_g(\lambda) = 0$ 在 $R_r$ 中，则输出 **零**。

正确性（以猜想 4.7.2 为条件）

- **（可靠性）**若 $C \equiv 0$，则每个特化 $C_g(\lambda)$ 在 $R_r$ 中恒等于零。因此，算法输出 **零**。• **（完备性）**若 $C \equiv/0$，则根据模稳定性猜想（猜想 4.7.2），对于任意素数 $r \geq R(w,d)$，至多有 $|B_r(C)$ 个 $|\leq r^{1-\varepsilon}$ 参数 $g \in Z_{r\setminus *}$满足 $C_g(\lambda)$ 在 $R_r$ 中为 $\equiv 0$。由于 $|Z_{r\setminus *}| = r-1$，至少存在一个 $g \in Z_{r\setminus *} \setminus B_r(C)$，使得 $C_g(\lambda)$ 在 $R_r$ 中为 $\neq 0$。算法通过枚举找到这样的一个 $g$，并输出 **非零**。

注

1. 该算法是黑盒且顺序无关的：它不使用也不需要 ROABP 变量顺序。2. 在猜想 4.7.2 成立的条件下，对 $g \in \mathbb{Z}_r^*$ 进行枚举，且 $r = \text{poly}(w,d)$，可在参数 $(n,w,d)$ 上实现全多项式时间确定性多项式恒等式检验。3. 模哈希算法不使用曲线代入、秩集中、隔离引理或有限避零网格。

可靠性。
若 $C \equiv/0$，则根据推论 3.3 和引理 5.5，诱导出的单变量多项式 $C(\lambda)$非零。由于命中集 $L$避开了它的所有根（根据引理 6.6），存在 $\lambda \in L$，使得 $C(\lambda) \neq 0$，且算法输出 **非零**。

完备性。
若 $C \equiv 0$，则对 $C$的任意特化求值结果均为零。特别地，对所有 $\lambda \in L$，都有 $C(\lambda) = 0$，且算法正确地输出 **零**。

通用并集为何重要。
该算法从不识别当前起作用的韦德伯恩块。$\Phi_{\text{univ}}$ 的构造保证，无论哪个块起作用，至少有一个因子能够对其进行认证。

运行时间。
总体运行时间可由第 7.8 节中的分析得出。

### 7.8 复杂度分析（条件多项式时间黑盒多项式恒等性测试）

令 $n$ 为变量数，$w$ 为只读代数分支程序的宽度，$d$ 为单变量次数的上界。我们分析基于模哈希的确定性黑盒恒等性测试算法的运行时间。该算法在第 [模稳定性小节], 中有描述，并假设猜想 4.7.2（模稳定性）成立。

**（1）有效变量约简**

固定只读代数分支程序表示

$$C(x_1,\dots,x_n) \;=\; e_1^\top\Big(\prod_{i=1}^{n} A_i\,(x_i)\Big)e_w, A_i(x_i) = \sum_{t=0}^{d} A_{i,t}\;x_i^t.$$

定义前缀系数空间 fi i t

$$\mathcal{V}_k := \text{span}\,\{A_1(x_1)\cdots A_k(x_k)\colon x_1,\dots,x_k \text{ range over monomials}\} \subseteq \text{Mat}_{\,w}(\mathbb{K}).$$

每个空间 $\mathcal{V}_k$ 的维数至多为 $w^2$。因此，整个计算至多由环境矩阵空间中的 $m := w^2$ 个独立方向控制。

具体而言，为一个饱和前缀空间固定一组基 $B_1$，…， $B_m$ 。每个前缀乘积都可以唯一地展开为

$$A_1(x_1)\cdots A_k(x_k) = \sum_{j=1}^{m} \beta_{k,j}\,(x_1,\dots,x_k)\,B_j,$$

其中，系数 $\beta_{k,j}$ 是标量多项式。这是只读代数分支程序的标准求值维数压缩。

定义变量约简映射 $\rho\ \mathbb{K}^n \to \mathbb{K}^m$ $G \in :$ ,

$y_j = \sum_{i=1}^{n} G_{j,i}\,x_i$，对应一个显式生成矩阵。

构造这些线性形式需要 $O$（$w^2n$）次域运算。

生成矩阵 $G$ 可以在黑盒模型中通过提取系数空间的一个基来构造。按照 Forbes、Saptharishi 和 Shpilka（ 2014 $m \le$ ）的方法，我们通过在多项式规模网格上对取值进行高斯消元，使用（ ）次黑盒查询恢复有效线性形式的张成空间。

**关键点**。 后续所有代入都应用于大小为 $m = w^2$ 的约化变量集，而不是原始的 $n$ 个变量。

**（2）通过模稳定性确定哈希域大小**

固定一个满足 $r = \text{poly}(w,d)$ 且 gcd $(r,\text{char}(\mathbb{K})) = 1$的素数 $r$ ，并定义循环环 $R_r$： $=$ $\mathbb{K}[\lambda]$ $\lambda^r - 1$ $g \in$ $_r^{\backslash *}$ $\Gamma_g$ $x_i \mapsto \lambda^{g^i} \in R_r$ $C_g$ $\lambda$ $=/$ 。对于每个 Z ，考虑模 $C$ 替换：，并记（）：（$\Gamma_g$） $\in R_r$。

根据猜想 4.7.2（模稳定性），对于 $r \ge R(w,d)$，坏参数集 $\text{B}_r(C) = \{\, g \in \text{Z}_r^{\backslash *}\colon C_g(\lambda) \equiv 0 \text{ in } R_r \,\}$ 的大小至多为 $r^{1-\varepsilon}$。因此，在 $r-1$ 个可能的 $g$ 值中，至少有一个是好的。枚举所有 $g \in \text{Z}_r^{\backslash *}$ ，即可保证检测到非零性。

因此，求值次数为 $|\,\text{Z}_r^{\backslash *}\,| = r - 1 = \text{poly}(w,d)$。

**(3) $R_r$中的每次求值成本**

在代入 $\Gamma_g$ 后，$A_i(x_i)$ 的每个元素都变为关于 $\lambda$ 的多项式，其次数为 $<r$。计算 $C_g(\lambda)$ 相当于在环 $R_r$ 上将 $n$ 个 $w \times w$ 矩阵相乘。使用朴素矩阵乘法和多项式运算，每次求值需要进行 $O(n\,w^3\,r^2)$ 次域运算。使用基于 FFT 的多项式乘法，可将其降至 $\tilde{O}(n\,w^3\,r)$，其中 $\tilde{O}(\cdot)$ 隐去了 $r$ 中的多对数因子。

**(4) 总运行时间**

变量约化步骤需要 $O(w^2 n)$ 次域运算。随后，我们枚举所有满足 $r = \text{poly}($ $w\ d$ $g$ $T\ n\ w\ d\ = O\ w^2 n\ +\ r -,)$ 的 $g \in \mathbb{Z}_r^*$，并对每个 执行一 $1 \cdot \tilde{O}\ n w^3\ r\ =$ $n\ w\ d$ $4\ 7\ 2$ 次环求值。因此，假设猜想 成立，总运行时间为 $(,,)\ (\ )\ (\ )\ (\ )\ \text{poly}(,,)$。

**结论**

假设模稳定性猜想成立，上述分析得出了一个针对只读代数分支程序的确定性黑盒多项式恒等式测试，其运行时间关于变量数量 $n$、宽度 $w$ 和单变量次数 $d$ 均为多项式级。基于曲线的构造中存在的所有超多项式复杂度均已消除，复杂度完全关于自然输入参数呈多项式级。

**域大小说明**

如果$|\ \mathbb{K}\ |$ 是有限的，我们假设$|\ \mathbb{K}\ | > |\ H\ |$（或在大小超过$|\ H\ |$的扩域上工作），以便避开和根计数论证可以原样适用。

**7.9 概念性贡献总结**

至此，我们构建了一个基于以下内容的新型确定性多项式恒等式测试框架：

- **矩阵词代数刚性** • **无特征值（有理）投影算子提取** • **凯莱–哈密顿和阿米楚尔–莱维茨基多项式恒等式** • **次数三角化以防止消去** • **以有限多项式避零取代随机性** • **使用显式多项式大小的求值集进行曲线击中**

由此产生的 结构以完全代数化的刚性论证取代了概率多项式恒等式测试 .

与以往工作的比较。Forbes 和 Shpilka 为只读代数分支程序构造了大小为 $n^{O(\log w)}$ 的准多项式命中集。将问题约化为 $w^2$ 个有效变量后，我们的构造得到大小为 $\text{poly}(w, d) \cdot B^{O(w^2)}$ 的命中集。虽然我们对宽度的依赖是指数级而非准多项式级，但对变量个数的依赖严格为多项式级，而且该构造基于一种根本不同的代数刚性机制，而非组合基隔离。

**表 7.9.1：与先前的只读代数分支程序确定性黑盒多项式恒等性测试的比较 s**

| 算法 | 顺序无关-性? | 黑盒-Box? | 时间 / 击中集大小 | 注释 |
|---|---|---|---|---|
| 本文工作（无条件） | Yes | Yes | $n \cdot (wd)^{O(w^2)}$ | $n$ 中的多项式；$w$ 中的超多项式 |
| 本文工作（条件性） †。 | Yes | Yes | $\mathrm{poly}(n, w, d)$ | 完全多项式时间假设模 稳定性 |
| Forbes–Shpilka [9] | No | Yes | $(nwd)^{O(\log n)}$ | 需要已知变量顺序 |
| Agrawal–Gurjar–Korwar–Saxena [11] | Yes | Yes | $(nwd)^{O(\log n)}$ | 未知顺序 只读代数分支程序 |

注意：与以往的 $(nwd)^{O(\log n)}$ 结果不同，[9,14], 我们的无条件结果关于 $n$ 是线性的，但关于 $w$ 是指数级的。

## 8. 结论与展望

我们基于针对矩阵词代数的一种新型刚性理论，构建了一个用于只读一次无关代数分支程序的确定性多项式恒等式检验框架。证明以代数结构取代随机性，将凯莱–哈密顿控制、阿米楚尔–列维茨基恒等式、秩一投影算子提取、次数三角化和有限多项式避零整合为一个连贯的机制。

从概念上说，该论证不同于以往依赖组合秩集中特性或显式单项式分离的多项式恒等式检验方法。相反，它将只读代数分支程序视为受约束非交换代数中的元素，并证明非平凡计算必然会生成全矩阵代数。一旦确立了这种刚性，在结构化曲线代入下便不可能发生消去，而非零性则可通过确定性行列式见证加以认证。

该框架引入了若干本身也颇具价值的工具。无特征值（有理）投影算子构造提供了一种新方法，仅利用多项式恒等式，就能在矩阵代数中分离出秩一方向。次数三角化原理为在行列式展开中确保主导项唯一提供了一种通用机制。有限避零引理给出了概率泛性的一种确定性替代方案，或可应用于其他代数复杂性领域。更广泛地说，矩阵词刚性的视角提供了一种系统方法，可将非交换代数结构转化为确定性算法保证。

### 8.1 展望与开放问题

本文发展的技术引出了若干自然的问题。

**拓展至只读代数分支程序之外。**
一个核心挑战是，能否将矩阵词刚性扩展到更一般的代数模型，包括一般代数分支程序、公式或电路。弄清哪些

计算模型会迫使生成全矩阵代数，或许能为实现更广泛的确定性多项式恒等式测试开辟一条新的统一途径。

**代数刚性界的紧致性。**

命中集，但未优化参数依赖性。确定基于刚性的多项式恒等式测试对宽度和次数依赖性的最优形式，仍是一个开放问题，并可能揭示有界宽度计算内部更精细的结构现象。

**与非交换不变量理论的联系。**

有界宽度生成元所生成的全矩阵代数的出现，表明它与不变量理论、中心多项式理论以及字代数的表示论结构存在关联。探索这些联系或能为代数计算模型带来更深入的分类结果。

**无特征值（有理）谱提取的推广。**

以及除法。代数复杂性理论的系统理论，可能应用于去随机化、符号线性代数和算法不变理论。

**更广泛的去随机化计划。**

最后，整体证明策略呼应了确定性素性测试背后的理念：用内在的代数刚性取代随机性。对于去随机化中的其他路的多项式恒等式检验、多项式因式分解，以及符号行列式恒等式测试。

**参考文献**


[1] R. A. DeMillo 和 R. J. Lipton，“关于代数程序测试的一个概率性注”，*Information Processing Letters*，7(4):193–195，1978。

[2] J. T. Schwartz，“用于验证多项式恒等式的快速概率算法”，*Journal of the ACM*，27(4):701–717，1980年。

[3] R. Zippel，“稀疏多项式的概率算法”，载于*EUROSAM 1979*，LNCS 72，Springer，1979年。

[4] V. Kabanets 和 R. Impagliazzo，“多项式恒等式测试去随机化意味着证明电路下界”，*Computational Complexity*，13(1–2):1–46，2004年。

[5] S. Aaronson，“从去随机化得到电路下界”，*Theory of Computing*，7(12)，2011年。

[6] A. Shpilka 和 A. Yehudayoff，“算术电路：近期成果与开放问题综述”，*Foundations and Trends in Theoretical Computer Science*，5(3–4):207–388，2010年。

[7] N. Saxena，《多项式恒等式测试进展》，综述笔记（及其更新版本），2013 年及以后。

[8] A. Shpilka，《只读一次多项式恒等式测试》，*Computational Complexity*，2015 年（及更早版本）。

[9] M. A. Forbes 和 A. Shpilka，《非交换只读一次无序代数分支程序的准多项式时间恒等式测试》，*FOCS 2013*；完整版本见 ECCC/TR 和 arXiv:1209.2408。

[10] M. A. Forbes、R. Saptharishi 和 A. Shpilka，《任意顺序的多线性只读一次代数分支程序的命中集》，*STOC 2014*。

[11] M. Agrawal、R. Gurjar、A. Korwar 和 N. Saxena，《ROABP 和集合多线性电路之和的击中集》，*SIAM Journal on Computing*，44(3):669–697，2015 年（arXiv:1406.7535）。

[12] R. Gurjar、A. Korwar、N. Saxena 和 T. Thierauf，“只读一次无关代数分支程序之和的确定性恒等式检验”，*CCC 2015*（及其完整版）。

[13] R. Gurjar、A. Korwar 和 N. Saxena，“常宽度及任意变量顺序的只读一次无关算术分支程序的恒等式测试”，arXiv:1601.08031，2016年。

[14] Z. Guo，“只读代数分支程序的改进显式命中集”，*APPROX/RANDOM 2020*（及其完整版）。

[15] V. Bhargava 等，“只读代数分支程序轨道的改进命中集”，2021年（不同版本／发表渠道）。

[16] C. Saha 等（合作者），“电路类轨道和多项式族的命中集”，ECCC 2021年／APPROX-RANDOM 2021 版本。

[17] D. Medini 等人，《VPe 中稠密轨道的命中集与重构……》，*CCC 2021*（包含常宽度只读代数分支程序轨道结果的轨道击中框架）。

[18] P. Chatterjee、D. Kush、S. Saraf 和 A. Shpilka，《只读一次代数分支程序之和的指数下界》，ECCC，2023年12月25日。

[19] C. Ramya 和 P. Shastri，《只读代数分支程序的阶数查找与等价性测试的困难性》，*FSTTCS 2025*。

[20] S. A. Amitsur 和 J. Levitzki，《代数的最小恒等式》，美国数学会会刊，1:449–463，1950年。（Amitsur–Levitzki 定理的标准参考文献。）

[21] A. R. Shemesh（以及标准线性代数参考文献），矩阵的 Cayley–Hamilton 定理；参见任何标准代数教材（并广泛用于多项式恒等式检验/代数分支程序代数论证）。

[22] 160 2 781 793, M. Agrawal、N. Kayal 和 N. Saxena, 2004
《PRIMES 属于 P》，数学年刊，0): – 。（AKS 素性判定框架启发了有限代数检验。）

## APPENDIX A. 演算示例（模哈希特化）

这个例子展示了无条件代数框架；模哈希变体也同样适用。

考虑有理数域上计算 $C(x_1, x_2) = x_1 x_2$ 的宽度为 2 的只读代数分支程序，

With $A_1(x_1) = \begin{pmatrix} x_1 & 0 \\ 0 & 1 \end{pmatrix}, A_2(x_2) = \begin{pmatrix} 1 & 0 \\ 0 & x_2 \end{pmatrix}$.

则 $C(x_1, x_2) = e_1^\top A_1(x_1) A_2(x_2) e_2$。

**模哈希环**

固定一个素数 $r$，使得最大公约数 $(r, \text{char}(\text{有理数域})) = 1$（此处为空），并在 $R_r :=$ 有理数域$[\lambda]/\lambda^r - 1$ 中运算。

**模替换**

对于每个 $g \in \mathbb{Z}_r^*$，定义 $\Gamma_g$ 为 $x_i \longmapsto \lambda^{g^i} \in R_r$，

其中指数按模 $r$ 解释。特化多项式为 $C_g(\lambda) := C(\Gamma_g) = \lambda^{g^1} \cdot \lambda^{g^2} = \lambda^{g+g^2} \in R_r$。

**哈希下的非零性**

由于对于每个 $k \in \mathbb{Z}r$，$\lambda^k \neq 0$ 都属于 $R_r$，因此对于每个 $g \in \mathbb{Z}_r^*$，我们有 $C_g(\lambda) \neq 0$ 。

Equivalently, the bad set $\mathcal{B}_r(C) = \{ g : C_g(\lambda) \equiv 0 \text{ in } R_r \}$

在这个例子中为空。

**算法行为**

算法 1 枚举 $g \in \mathbb{Z}_r^*$，在 $R_r$ 下使用 $\Gamma_g$对只读代数分支程序求值，并在找到 $C_g(\lambda) \neq 0$时立即停止。在此示例中，每个 $g$ 都能成功，因此算法立即输出 **非零**。

## 附录 B. 模稳定性的实证验证

**模稳定性的实验证据**

我们进行了大量计算实验，测试模稳定性猜想在广泛参数范围内的表现，其中包括具有对抗性结构的只读代数分支程序。所有实验均采用精确算术：将循环环 $R_r = \mathbb{K}[\lambda]/(\lambda^r - 1)$ 嵌入含有一个本原 $r$ 次单位根的有限域中，从而消除数值或概率伪影。

我们测试了变量数最多为 $n = 20$ 、宽度最多为 $w = 10$、单变量次数为 $d = 2$ 的只读代数分支程序，所用素数 $r$ 的范围从 $10^3$ 到超过 $10^9$。对于每个实例，我们在模替换 $x_i \mapsto \lambda^{g^i}$ 下，对数百个不同的参数 $g \in \mathbb{Z}_r^*$ 进行了求值。我们纳入了随机构造和对抗性构造，例如通过路径控制的只读代数分支程序，以及旨在尽量减少代数混合并促进消去的上三角只读代数分支程序。

在所有测试实例中，均未观察到非平凡的坏参数：每种情况下，对于所有测试的 $g$，特化多项式 $C_g(\lambda)$ 始终非零。尤其是，我们没有观察到坏参数密度随宽度或模数增加而上升。

尽管这些实验并不能构成证明，但它们有力地表明，坏集合 $\mathrm{B}r(C)$ 在实践中极其稀疏，甚至往往为空，即使是在远超猜想所要求范围的条件下也是如此。这种实测现象与猜想的界 $|\mathrm{B}r(C)| \leq r^{1-\varepsilon}$ 相符，实际上还暗示着一种强得多的现象。

**大规模实验验证**。

我们进一步在大得多的参数规模下检验了模稳定性猜想。具体而言，我们使用素数模数 $r = 1,000,000,007$，对具有 $n = 20$、宽度为 $w = 10$、单变量次数为 $d = 5$ 的对抗性结构只读代数分支程序进行了评估。对于每个实例，我们在模替换 $x_i \mapsto \lambda^{g^i}$ 下测试了 6,000 个不同的参数 $g \in \mathbb{Z}_r^*$，并通过嵌入到包含一个本原 $r$ 次单位根的有限域中进行精确算术计算。

在所有测试的实例和参数中，我们均未观察到错误值：每个特化 $C_g(\lambda)$ 在环 $R_r = \mathbb{K}[\lambda]/(\lambda^r - 1)$ 中都非零。即使对于旨在将代数混合降至最低的对抗性构造，这一现象仍然成立。这些实验有力地表明，坏集合 $\mathrm{B}r(C)$ 在实践中极其稀疏，而且往往为空，即使是在远超猜想所要求范围的情形下也是如此。

| **N** | **n** | **d** | **w** | **参数** | **错误值** |
|---|---|---|---|---|---|
| $\mathbf{1,000,000,007}$ | 20 | 2 | 10 | 600 | 0 |
| $\mathbf{1,000,000,007}$ | 20 | 5 | 10 | 6,000 | 0 |
| $\mathbf{1,000,000,007}$ | 20 | 5 | 20 | 600 | 0 |
| $\mathbf{1,000,000,007}$ | 40 | 5 | 10 | 600 | 0 |
| $\mathbf{10,000,000,019}$ | 20 | 5 | 10 | 600 | 0 |
| $\mathbf{1,000,000,007}$ | 20 | 5 | 10 | 60,000 | 0 |
| $\mathbf{100,000,007}$ | 20 | 5 | 8 | 1,000,000 | 0 |