arXiv:2602.17904v1 [cs.CC] 20 Feb 2026

希尔伯特零点定理属于计数层级 y

Robert Andrews* Abhibhav Garg† Éric Schost‡

摘要

我们证明，希尔伯特零点定理——判定一个多元多项式方程组在底域的代数闭包中是否有解的问题——属于计数层级。更一般地，我们证明，可以通过计数层级预言机访问，在多项式时间内计算方程组的解的数量。我们的结果特别适用于系数属于有理数域或有限域的多项式。此前，这些问题已知的最佳复杂度上界分别为 PSPACE 和 FPSPACE。我们的主要技术贡献是构造了一个一致的常数深度算术电路族，用于计算多元结式。

目录

1 引言 **1**
1.1 背景 .1 1.2 我们的结果 .2 1.3 证明概述 .5 1.4 组织结构 .9

2 预备知识 **9**
2.1 符号与约定 .9 2.2 布尔电路族和算术电路族的一致性 .10 2.3 整数、有理数和有限域算术. 14

3 算术电路基本操作的一致性 **16**

4 多元结式 **22**
4.1 多元结式 .22 4.2 仿射系统的可满足性 .24 4.3 零维系统中的解计数 .28

5 常数依赖 用于结式的 th 电路 **31**
5.1 记号与证明概述 .31 5.2 初始方程组 .32 5.3 定义同伦的方程组的结式 .35

*彻里顿计算机科学学院，滑铁卢大学。本研究的部分工作得到了西蒙斯计算理论研究所的支持，并且是在作者访问该研究所期间完成的。电子邮件：randrews@uwaterloo.ca。

†滑铁卢大学彻里顿计算机科学学院。电子邮箱：abhibhav.garg@uwaterloo.ca。

‡滑铁卢大学彻里顿计算机科学学院。电子邮箱：eschost@uwaterloo.ca。

6 在计数层级中判定零点定理 416.1 从一致算术电路到计数层级 .416.2 计算结式并判定零点定理 .486.3 计数零维方程组中的解 .51

7 零点定理的应用 55

1 引言

1.1 背景

多项式方程在数学和科学领域无处不在。它们描述了有用的几何和物理关系，例如勾股定理，或抛体的高度随时间的变化，因此数百年来一直是研究的对象。求根公式、高斯消元法和欧几里得算法都是求解方程的重要工具，古代文明便已知晓它们，也是流传至今最古老的算法之一。文艺复兴时期的数学家后来发现了求解三次方程和四次方程的公式。在阿贝尔证明五次方程求根公式并不存在之前，人们曾为寻找这一公式付出巨大努力。数值方法也在同期发展起来，例如牛顿法，即使没有显式的方程解公式，也能求解高次数方程；此后，这些方法已成为现代计算科学不可或缺的一部分。

人们对求解多项式方程的兴趣历久不衰。随着计算机科学的发展，数学家自然而然地开始探讨求解方程的可计算性与复杂性问题。早在 20th 计算机时代到来之前的世纪之交，希尔伯特 [希尔02]提出了二十三个问题，希望借此指引数学的发展。求解方程组是他的第十个问题。用现代术语来说，希尔伯特提出的问题是：是否存在一种算法，以多项式 $f_1, \ldots, f_m \in \mathbb{Z}[x_1, \ldots, x_n]$ 作为输入，并判断方程组 $f_1 = \cdots = f_m = 0$ 是否有整数解。马季亚谢维奇 [马特70], 在戴维斯、普特南和罗宾逊 [DPR61], 的研究基础上证明了这个问题不可判定。然而，如果我们转而寻求其他数域中的解，例如实数或复数，这个问题便成为可判定问题，并呈现出另一番图景。

在复数域中——更一般地说，在代数闭域中——求解多项式方程的出发点是希尔伯特零点定理。给定多项式f_1，……， $f_m \in \mathbb{C}[x_1, \ldots, x_n]$，零点定理指出，方程组 $f_1 = \cdots = f_m = 0$在 $\mathbb{C}^n$ 中无解，当且仅当存在多项式 g_1，……， $g_m \in \mathbb{C}[x_1, \ldots, x_n]$ 使得

$$f_1(\mathbf{x})g_1(\mathbf{x}) + f_2(\mathbf{x})g_2(\mathbf{x}) + \cdots + f_m(\mathbf{x})g_m(\mathbf{x}) = 1.$$

因此，我们可以通过转而寻找满足 $\sum_{i=1}^{m} f_i g_i = 1$的多项式 g_1，……， g_m，来判断方程组 $f_1 = \cdots = f_m = 0$ 是否有解。由于零点定理在判定方程组可解性方面发挥着关键作用，判定一个多项式方程组是否有解这一计算问题也称为希尔伯特零点定理，简称 HN。

零点定理将我们原来的非线性问题化为一个线性问题：考察方程 $\sum_{i=1}^{m} f_i g_i = 1$ 两边单项式$\mathbf{x}^{\mathbf{a}}$的系数，便得到关于多项式 g_1，……， g_m的未知系数的一个线性方程。要将其转化为算法，若多项式 g_1，……， g_m存在，我们需要给出它们的次数界。Hermann [Her26] 率先做到了这一点。她证明，若 f_i 的次数以 d 为界且没有公共解，则可以找到次数至多为$(2d)^{n2^n}$的 g_i 。[1] 这一次数界将判定 $f_1 = \cdots = f_m = 0$ 的可解性这一任务归结为求解一个双指数规模的线性方程组，而该任务可在双指数时间内完成。此后，大量工作证明了关于 g_i的次数（及高度）的更强界，从而得到形如 $\deg(g_i) \leq d^n$[Bro87; CGH88; Kol88; FG90; Som99; KPS01; Jel05]的界。自然，这些单指数次数界意味着，相对于输入规模，希尔伯特零点定理可在指数时间内判定，而非双指数时间。

[1]证明见 Hermann 的原始论文并不完整，其中的疏漏后来由 Seidenberg 补上 [Sei74]。

尽管形如$\deg(g_i) \leq d^n$的次数界对零点定理而言基本上是紧的，但其复杂性仍有更多可说之处，因为线性方程可以用出人意料的高效方式求解。1976年，Csanky [Csa76]设计了一种精巧的并行算法，可在$O(\log^2 n)$时间内计算一个$n \times n$矩阵的行列式。随后十年中，人们为线性代数中的许多问题设计了并行算法，其中包括Borodin、von zur Gathen与Hopcroft [BvH82]的算法，该算法能在$O(\log^2 n)$并行时间内求解线性方程组。结合Borodin [Bor77]的一个观察，即并行算法可用小空间模拟，由此得到一种仅使用$O(\log^2 n)$空间即可求解线性方程组的算法。[2] 将其推广到零点定理中出现的指数规模方程组（其中矩阵的规模为$d^{\mathrm{poly}(n)}$），便得到一个PSPACE算法，用以在代数闭域上判定希尔伯特零点定理，这是该问题目前的最佳结果。

关于求解方程组的计算困难性，我们所知甚少。通过将可满足性问题算术化，很容易看出，希尔伯特零点定理 是NP困难的，而计算方程组解的数量（若保证该数量有限）则是#P类困难的。这些是该问题已知的最强下界，原因也很充分。Koiran [Koi96]证明了，假设广义黎曼猜想成立，希尔伯特零点定理 在复数域上的问题属于复杂性类AM。在合理的困难性假设下，Miltersen 和 Vinodchandran [MV05] 证明了 AM =NP，因此 Koiran 的工作确立了希尔伯特零点定理 在NP意义下是完备的 $\mathbb{C}$。鉴于此，任何强于NP困难性的希尔伯特零点定理 下界，都意味着复杂性类出现出人意料的坍缩，或者 Koiran 的NP算法所依据的两个猜想之一是错误的。

在其他域上，希尔伯特零点定理 的复杂性则不太明了。上述次数界对任意域都成立，因此，只要输入属于一个能够高效进行算术运算的子域，就可以在任意代数闭域上以PSPACE 判定零点定理。Koiran 的算法近期由 Ait El Manssour、Balaji、Nosan、Shirmohammadi 和 Worrell [ABNSW25] 扩展，从而可以在 $\mathbb{C}(y_1, \ldots, y_k)$ 上以AM判定零点定理，同样以广义黎曼猜想成立为前提。在正特征域上的情况则更为棘手。例如，在有限域上，我们只知道希尔伯特零点定理 是NP困难的，并且可以在PSPACE内判定。即使在条件假设下，也没有已知的更强下界或更好的算法。

希尔伯特零点定理除了本身是一个具有内在意义的问题之外，在代数复杂性中也起着核心作用，类似于布尔可满足性在经典复杂性理论中所处的地位。在交换环 R上，问题希尔伯特零点定理$_R$——即判定 R 上的多项式方程组在 R中是否有解——对NP$_R$是完备的，而该NP是Blum–Shub–Smale 计算模型中NP的类似物 [BSS89；BCSS98]。希尔伯特零点定理$_R$的计数变体记为#希尔伯特零点定理$_R$，其中必须计数环 R上一个方程组的解的个数，它在计数问题理论中同样重要。Bürgisser和Cucker [BC06]定义了复杂性类#P$_{\mathbb{R}}$ 和#P$_{\mathbb{C}}$，分别是NP$_{\mathbb{R}}$ 和NP$_{\mathbb{C}}$的计数版本，并证明#希尔伯特零点定理$_{\mathbb{R}}$ 和#希尔伯特零点定理$_{\mathbb{C}}$ 对其各自的类是完备的。零点定理在计算代数几何中也是一个有用的算法原语：许多受关注的问题，例如计算代数闭域上一个代数簇的维数 [Koi97]，都将零点定理用作必不可少的子程序。

1.2 我们的结果

我们证明了，与求解多项式方程组相关的各种问题——其中首要的是零点定理——都可以在计数层级（CH）中判定。我们采用图灵

[2] Csanky 的算法 [Csa76] 以及 Borodin、von zur Gathen 和 Hopcroft 的算法 [BvH82] 被表述为算术算法，没有考虑位复杂度，但在计算位复杂度的情况下，它们同样可以在 $O(\log^2 n)$ 并行时间内实现。

机模型，以系数的二进制编码表示多项式。全文中，我们考虑系数属于有理数域、数域、有限域或这类域上的多项式环的方程组；所有这些对象都可以高效地进行二进制编码，并且我们关注它们在系数域的代数闭包上的可解性。

我们采用多项式的稠密表示，即列出所有单项式及其系数，包括系数为零的单项式。也可以考虑表达能力更强的多变量多项式编码：要么只写出多项式中非零的单项式（稀疏表示），要么描述一个用于计算该多项式的算术电路（直线程序表示）。通过添加多项式数量的扩展变量，稀疏表示和直线程序表示都可以转换为稠密表示。这种转换会保留原方程组的可满足性以及解的数量（如果该数量有限）。

我们的主要结果是，希尔伯特零点定理——也就是说，判定域 $\mathbb{F}$ 上的方程组是否在代数闭包 $\overline{\mathbb{F}}$中有解——可以在 CH复杂性类中求解。

定理 1.1 (见 定理 6.9)。 设 $\mathbb{F}$ 是以下域之一： $\mathbb{Q}$， $\mathbb{Q}(y_1, \ldots\ldots, y_k)$、数域 $\mathbb{K}$，$\mathbb{K}(y_1, \ldots\ldots, y_k)$、有限域 $\mathbb{F}_q$，或 $\mathbb{F}_q(y_1, \ldots\ldots, y_k)$。那么， $\mathbb{F}$ 上的希尔伯特零点定理可以在 CH复杂性类中求解。

在继续介绍其他结果之前，我们先简要回顾计数层级。计数层级 CH 最初由 Wagner 提出 [Wag86] ，用于刻画组合计数问题的复杂性。其 k^{th} 第 CH 层记作 $\mathsf{C}_k\mathsf{P}$，其定义如下：

$$\begin{aligned}\mathsf{C}_0\mathsf{P} &:= \mathsf{P}\\ \mathsf{C}_1\mathsf{P} &:= \mathsf{PP}\\ \mathsf{C}_k\mathsf{P} &:= \mathsf{PP}^{\mathsf{C}_{k-1}}.\end{aligned}$$

计数层级是这些复杂性类的并集，即 $\mathsf{CH} := \bigcup_{k\geq 0}\mathsf{C}_k\mathsf{P}$。或者，也可以将 CH 定义为这样一类语言：它们可由多项式时间图灵机判定，且机器使用常数个多项式有界的多数数量词；这类似于 PH 对语言的刻画：语言可由多项式时间图灵机判定，而机器可以使用常数个多项式有界的存在量词和全称量词。

计数层级在复杂性类的版图中处于什么位置？Toda 的结果指出$\mathsf{PH} \subseteq \mathsf{P}^{\mathsf{PP}}$ [Tod91] ，多项式时间层级包含于 CH 的第二层，因此有包含关系 $\mathsf{PH} \subseteq \mathsf{CH}$。此外，很容易看出 $\mathsf{CH} \subseteq \mathsf{PSPACE}$ ，这是$\mathsf{PP} \subseteq \mathsf{PSPACE}$ 的推论。顾名思义，计数层级刻画了计数的复杂性：根据定义，若 $\mathsf{FP} = \#\mathsf{P}$ （即矩阵永久式可在多项式时间内计算），则有坍缩 $\mathsf{P} = \mathsf{CH}$。关于计数层级的更多细节，请参阅 Allender 和 Wagner [AW90] 以及 Torán [Tor91]。

回到我们的结果，希尔伯特零点定理表明，多项式方程组$f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$ 不可满足，当且仅当常数多项式 1 属于由 $f_1, \ldots, f_m$生成的理想的根基 $\mathrm{rad}(f_1, \ldots, f_m)$。更一般地，零点定理指出，多项式 $h \in \mathbb{F}[x_1, \ldots, x_n]$ 在 $f_1, \ldots, f_m$的公共零点上取零，当且仅当 $h \in \mathrm{rad}(f_1, \ldots, f_m)$。这些公共零点称为$f_1$代数簇 f_m，记作 $\mathrm{V}(f_1, \ldots, f_m)$。判定 $h \in \mathrm{rad}(f_1, \ldots, f_m)$ 是否成立的问题称为根理想成员问题，是计算代数几何中的另一个基本问题。前面提到的零点定理次数界也适用于根理想成员问题，但需额外乘以一个因子，以计入多项式 h的次数。这些次数界表明，根理想成员问题与希尔伯特零点定理一样，可以在

PSPACE 中求解。通过将我们的主定理与 Rabinowitsch技巧结合起来，我们改进了这一界，证明根理想成员问题可以在 CH复杂性类中判定。

定理 1.2 （见推论 7.1）。 设 $\mathbb{F}$ 为以下域之一： $\mathbb{Q}$， $\mathbb{Q}(y_1,\ldots,y_k)$、数域 $\mathbb{K}$，$\mathbb{K}(y_1,\ldots,y_k)$、有限域 $\mathbb{F}_q$，或 $\mathbb{F}_q(y_1,\ldots,y_k)$。则$\mathbb{F}$上的根理想成员问题可在 CH复杂性类中判定。

相比之下，Mayr 与 Meyer [MM82] 证明了一般理想成员问题是 EXPSPACE-完全的。因此，理想成员问题复杂性的类似改进将适用于 EXPSPACE 类本身。

一旦我们知道方程组 $f_1,\ldots,f_m \in \mathbb{F}[x_1,\ldots,x_n]$ 有一个解，自然的下一步便是了解该方程组有多少个解。使这一问题精确化的一种方式，是求代数簇 $V(f_1,\ldots,f_m)$ 的维数，它是解集规模的一种粗略度量。对我们主要定理的直接应用，使我们能够在 FP^{CH} 中计算该维数。

定理 *1.3*（见推论 *7.2*）。设 $\mathbb{F}$ 是以下域之一： $\mathbb{Q}$、 $\mathbb{Q}(y_1, \ldots, y_k)$、数域 $\mathbb{K}$、 $\mathbb{K}(y_1, \ldots, y_k)$、有限域 $\mathbb{F}_q$ 或 $\mathbb{F}_q(y_1, \ldots, y_k)$。给定 $\mathbb{F}[x_1,\ldots,x_n]$ 中的多项式集合 $f_1, \ldots, f_m$，可以在 FP^{CH} 中计算代数簇 $V(f_1, \ldots, f_m)$ 的维数。

当代数簇 $V(f_1, \ldots, f_m)$ 为零维时，它由一个有限点集组成，因此询问方程组 $f_1 = \cdots = f_m = 0$ 的解的数量是有意义的。与我们主定理的前两个应用不同，后两者可通过简单归约到希尔伯特零点定理得到；而对于将代数簇上的点计数归约到希尔伯特零点定理，我们尚不知道一种简单的归约方法。尽管如此，我们的技术可以轻松扩展到这一问题，从而在 FP^{CH} 中计算代数簇上的点数。

定理 *1.4*（见定理 *6.16*）。设 $\mathbb{F}$ 是域 $\mathbb{Q}$、 $\mathbb{Q}(y_1, \ldots, y_k)$、数域 $\mathbb{K}$、 $\mathbb{K}(y_1, \ldots, y_k)$、有限域 $\mathbb{F}_q$ 或 $\mathbb{F}_q(y_1, \ldots, y_k)$ 中的一个。给定 $\mathbb{F}[x_1,\ldots,x_n]$ 中的多项式集合 $f_1, \ldots, f_m$，可以在 FP^{CH} 中计算代数簇 $V(f_1, \ldots, f_m)$ 的基数。

代数簇上的点计数是计数复杂性中的一个基本问题，其精确分类尚未得到充分理解。Bürgisser 和 Cucker [BC06] 引入了几何计数复杂问题的复杂性类 GCC，并证明复代数簇上的点计数对于 GCC 是完全的。[3] GCC 类及其函数类对应物 FP^{GCC} 包含代数几何中的自然计数问题，包括计算代数簇的几何次数 [BC06], 、代数簇的欧拉示性数 [BCL05], 以及光滑等维代数簇的希尔伯特多项式 [BL07]。通过将 #SAT 算术化，可以很容易地看出，代数簇上的点计数至少与计算布尔公式的可满足赋值数量一样困难，因此 #P ⊆ GCC。在我们的工作之前，GCC 已知的最佳上界是 GCC ⊆FPSPACE [BC06]。定理 1.4 将其改进为 GCC ⊆FP^{CH}。

定理 1.4 解释了为什么我们的方法只能证明 CH复杂性类 是希尔伯特零点定理复杂性的一个上界，而不能将 希尔伯特零点定理 置于多项式时间层级中。定理 1.1 和 1.4的证明也采用了相同的方法。由于 定理 1.4 讨论的是一个 #P-困难问题，因此，除非复杂性类出现出人意料的塌缩，否则我们用这些方法所能证明的最佳上界是 #P。

最后，我们提及定理 1.1 在计算张量秩方面的一个直接应用；张量秩是代数复杂性中的一个重要问题，与确定矩阵乘法指数有关。通过对希尔伯特零点定理的直接归约，我们可以在FP^{CH}中计算给定张量的秩。

[3] Bürgisser 和 Cucker [BC06] 还引入了计数复杂性类 $\#P_{\mathbb{C}}$ 和 $\#P_{\mathbb{R}}$，作为 Blum–Shub–Smale 计算模型中 #P类的对应类。他们还证明，在复代数簇或实代数簇上进行点计数，分别是 $\#P_{\mathbb{C}}$ 和 $\#P_{\mathbb{R}}$的完全问题。

定理 *1.5*（参见推论 *7.3*）。设 $\mathbb{F}$ 为以下之一：域 $\mathbb{Q}$、 $\mathbb{Q}$（y_1，……，y_k）、数域 $\mathbb{K}$、$\mathbb{K}$（y_1，……，y_k）、有限域 $\mathbb{F}_q$，或 $\mathbb{F}_q$（y_1，……，y_k）。给定张量 $T \in \mathbb{F}^{d_1} \otimes \cdots \otimes \mathbb{F}^{d_k}$，可以在$FP^{\mathsf{CH}}$中计算 T 在 $\mathbb{F}$上的张量秩。

1.3 证明概述

如我们所见，要判断多项式组 $f_1, \ldots, f_m \in \mathbb{C}[x_1, \ldots, x_n]$ 的次数至多为 d时是否有解，可以通过判断以下线性方程组是否可解

$$f_1(\mathbf{x})g_1(\mathbf{x}) + f_2(\mathbf{x})g_2(\mathbf{x}) + \cdots + f_m(\mathbf{x})g_m(\mathbf{x}) = 1.$$

其中未知数是次数至多为 d^n的多项式 $g_1, \ldots, g_m \in \mathbb{C}[x_1, \ldots, x_n]$ 的系数，由此得到一个规模为 $d^{\mathrm{poly}(n)}$的方程组。为了降低希尔伯特零点定理的复杂性，我们将利用这样一个事实：这些线性方程组并非任意的，而是具有高度结构性。

1.3.1 结式

要了解像 $\sum_{i=1}^{m} f_i g_i = 1$ 这样的线性方程组有何特殊之处，我们来考虑这样一个问题：判断关于一个变量的两个方程 $f_1, f_2 \in \mathbb{C}[x]$ 组成的方程组是否有解。线性方程组 $f_1(x)g_1(x) + f_2(x)g_2(x) = 1$ 的行列式是一个关于 f_1 和f_2 的系数的著名函数，称为它们的结式，记作 Res(f_1, f_2)。结式具有一个显著性质：当且仅当方程组 $f_1(x) = f_2(x) = 0$ 有解时，Res(f_1, f_2) $= 0$ 。根据定义，结式是一个规模为多项式级的矩阵的行列式，因此可以使用 Csanky 算法 [Csa76] 在多对数空间内计算。这对应于希尔伯特零点定理 PSPACE 算法的一个缩减版。

尽管结式被定义为一个行列式，但计算结式比计算行列式本身更高效。Andrews 和 Wigderson [AW24]证明，两个多项式的结式可以用常数深度、多项式规模的算术电路计算，而行列式则已被证明不可能做到这一点 [LST25]。由于有理数的迭代加法和乘法可以由常数深度、多项式规模的阈值电路计算，即属于 TC^0 [HAM02], 类，这意味着当输入以二进制表示时，结式也可以在 TC^0 中计算。正如我们很快将看到的，TC^0 类对应于缩小版的计数层级 CH，因此，这个算法表明，改进希尔伯特零点定理的复杂性或许是可能的。结式的改进算法依赖于泊松公式，它用 f_1 和 f_2 的复根来表示 Res(f_1, f_2)。假设 f_1 和 f_2 是首一多项式，且 f_1 在 $\mathbb{C}$ 上可分解为 $f_1(x) = \prod_{i=1}^{d}(x - \alpha_i)$。在这种情况下，泊松公式将 f_1 和 f_2 的结式表示为

$$\mathrm{Res}(f_1, f_2) = \prod_{i=1}^{d} f_2(\alpha_i).$$

尽管这一点并非显而易见，但这个恒等式可用于在常数深度下计算结式，因为 f_1 的系数提供了关于其根 α_1、……、α_d 的有用信息。

结式可以推广到若干变量中的多个多项式，而设计计算它的算法对我们的工作至关重要。假设 $F_0, \ldots, F_N \in \mathbb{C}[x_0, \ldots, x_n]$ 是次数分别为 $d_0, \ldots, d_n$ 的齐次多项式。存在一个关于它们系数的多项式函数，同样称为结式，记作 Res($F_0, \ldots, F_n$)，使得 Res($F_0, \ldots, F_n$) $= 0$

当且仅当方程组 $F_0(\mathbf{x}) = \cdots = F_n(\mathbf{x}) = 0$ 有非零解。[4] 因此，如果我们能高效计算结式，就也能判定 希尔伯特零点定理，至少对于多项式个数与变量个数相同的齐次方程组是如此。多元结式可以表示为一个结构化矩阵的两个子式之商，该矩阵的规模为 $\binom{d_0+\cdots+d_n}{n}$，称为 麦考莱矩阵，对应于$F_0, \ldots, F_n$。最坏情况下，该矩阵相较于 $\sum_{i=0}^{n}\binom{n+d_i}{n}$（即多项式 $F_0, \ldots, F_n$ 的系数个数）呈指数级增长，因此其任一子式均可在 PSPACE 中计算。设计一种能在 $\mathsf{FP}^{\mathsf{CH}}$ 中计算多元结式的改进算法，将是证明 希尔伯特零点定理 $\in$CH复杂性类 的主要步骤。

1.3.2 计数层级

在介绍如何计算 $\mathsf{Fp}^{\mathsf{CH}}$ 中的结式之前，我们先来看看CH复杂性类所具有的算法能力。正如多项式时间层级PH 与由与门、或门和非门构成的有界深度布尔电路 [FSS84], 相关联一样，计数层级与由阈值门和否定门构成的有界深度布尔电路相关联。对我们来说，按照多项式有界多数量词的刻画来理解CH 会很有用：语言 $L \subseteq \{0,1\}^*$属于 CH，当且仅当存在一个多项式有界函数 p 和一个多项式时间图灵机 M，使得

$$x \in L \iff \operatorname{Maj} y_1 \in \{0,1\}^{p(|x|)} \cdots \operatorname{Maj} y_k \in \{0,1\}^{p(|x|)} M(x, y_1, \ldots, y_k) \text{ accepts},$$

其中，多数量词 $\operatorname{Maj} y$ 规定：后续公式对变量 y的大多数取值都为真。借助一个多数量词，只要这个指数规模位串集合中的任意单个位都能在多项式时间内计算出来，我们就能计算该集合上多数函数（更一般地说，任意阈值函数）的值。重复应用这一观察，我们就能在 CH复杂性类中求值一个指数规模的常数深度阈值电路，前提是该电路的连通性性质可由多项式时间图灵机判定。更准确地说，如果布尔函数 $f\colon \{0,1\}^* \to \{0,1\}$ 可由一个常数深度、指数规模的阈值电路多对数时间一致族计算，那么 $f \in$CH。

有界深度阈值电路的能力出奇地强。对有理数进行基本运算，例如迭代加法、迭代乘法和带余除法，都可以由对数时间一致族的 TC^0 电路 [HAM02]计算。这意味着，阈值电路能够模拟算术电路，同时深度只增加一个常数因子，规模只增加一个多项式因子。特别是，在 CH复杂性类中，我们可以模拟一个多对数时间一致的有界深度、指数规模算术电路族。这是我们在算法中利用 CH 的主要性质。

1.3.3 常数深度计算结式

现在我们回到在 $\mathsf{FP}^{\mathsf{CH}}$ 中计算多元结式这一任务。根据我们对 CH 复杂性类能力的讨论，只需构造一个多对数时间一致的常数深度、指数规模算术电路族来计算结式，这正是我们将采用的方法。

与两个多项式的情形一样，多元结式可以表示为将其中一个多项式代入其他多项式的公共根所得的值。为设定记号，令

$$\overline{F}_i(\mathbf{x}) \coloneqq F_i(x_0, \ldots, x_{n-1}, 0)$$
$$f_i(\mathbf{x}) \coloneqq f_i(x_0, \ldots, x_{n-1}, 1).$$

[4] 由于多项式 F_0、.....， F_n 是齐次的，因此全零点始终是方程组 $F_0 = \cdots = F_m = 0$的一个解。结式可以检测该方程组是否有非平凡解，或者等价地，是否存在一个位于射影空间 $\mathbb{P}^n$中的解。

然后，假设较小的结式 Res(F_0、……、 F_{n-1}) 非零，泊松公式 表明结式可因式分解为

$$\mathrm{Res}(F_0,\dots,F_n) = \mathrm{Res}(\overline{F}_0,\dots,\overline{F}_{n-1})^{d_{n-1}} \prod_{\boldsymbol{\alpha}\in \mathrm{V}(f_0,\dots,f_{n-1})} f_n(\boldsymbol{\alpha})^{m(\boldsymbol{\alpha})},$$

其中，V($f_0,\dots,f_{n-1}$) $\subseteq \mathbb{C}^n$ 是 $f_0,\dots,f_{n-1}$ 的公共根集合（根据较小结式的假设，该集合必为有限集），而 $m(\boldsymbol{\alpha})$ 是 $\boldsymbol{\alpha}$ 作为方程组 $f_0 = \cdots = f_{n-1} = 0$ 的解时的重数。通过对较小结式 Res(F_0, …, E_{n-1}) 递归地应用泊松公式，我们看到，所要计算的原始结式 Res($F_0,\dots,F_n$) 可以表示为形如 $\prod_{\boldsymbol{\alpha}\in \mathrm{V}(f_0,\dots,f_{n-1})} f_n(\boldsymbol{\alpha})^{m(\boldsymbol{\alpha})}$ 的项的乘积。如果我们能用有界深度算术电路计算这样的一项，那么并行计算所有这些项并将其相乘，就能得到一个用于计算结式本身的有界深度算术电路。

为了计算形如 $\prod_{\boldsymbol{\alpha}\in \mathrm{V}(f_0,\dots,f_{n-1})} f_n(\boldsymbol{\alpha})^{m(\boldsymbol{\alpha})}$ 的乘积，我们似乎需要求解方程组 $f_0 = \cdots = f_{n-1} = 0$。在 $n = 1$ 的情形下，可以用 Girard–Newton 恒等式 [AW24] 避免这一点。在 $n \geq 2$ 的情形下也有类似的恒等式（见 [AiK81] 及其中的参考文献），但这些恒等式更为复杂，而且尚不清楚能否在常数深度内实现。为此，我们将使用隐函数定理的一个计算上显式的版本，把 $f_0 = \cdots = f_{n-1} = 0$ 的解表示为 $f_0,\dots,f_{n-1}$ 的系数的幂级数，其中这些幂级数的初始片段可以由常数深度电路计算。Bhattacharjee、Kumar、Rai、Ramanathan、Saptharishi 和 Saraf 最近的工作中也出现了类似的思路 [BKR+25a], ，他们使用拉格朗日反演证明低深度算术电路在因式分解下封闭。他们的工作，尤其是对隐函数定理显式版本的运用，是本文结果的重要灵感来源。

隐函数定理要求 (f_0，……， f_{n-1}) 的雅可比矩阵在 $\boldsymbol{\alpha}$ 处可逆，而这对给定的方程组未必成立。为解决这一问题，我们采用同伦延拓的方法，通过求解另一个相关但不同的方程组，来求出 $f_0 = \cdots = f_{n-1} = 0$ 的根。我们将选择另一个齐次方程组 G_0，……， $G_n \in \mathbb{C}[x_0,\dots,x_n]$，它与 F_i 无关；该方程组的解可以预先明确得知，且在这些解处雅可比矩阵可逆。令 t 为一个新的变量，然后考虑方程组 $H_0 = \cdots = H_n = 0$，其中 H_i 定义为

$$H_i(t,\mathbf{x}) \coloneqq (1-t)\cdot G_i(\mathbf{x}) + t\cdot F_i(\mathbf{x}).$$

在 $t = 0$ 处，这个方程组很容易求解，因为它会化简为 $G_0 = \cdots = G_n = 0$，而其解我们已知。在 $t = 1$ 处，我们就得到原本要解的方程组。特别是，如果我们能够改为计算结式 Res(H_0，……， H_n)，那么在 $t = 1$ 处求值就能得到 Res(F_0，……， F_n)。

Let

$$g_i(\mathbf{x}) \coloneqq G_i(x_0,\dots,x_{n-1},1)$$
$$h_i(t,\mathbf{x}) \coloneqq H(t,x_0,\dots,x_{n-1},1).$$

对于方程组 $g_0 = \cdots = g_{n-1} = 0$ 的每个解 $\boldsymbol{\alpha} \in \mathbb{C}^n$，都存在一个对应的幂级数解 $\boldsymbol{\varphi}_{\boldsymbol{\alpha}}(t) \in \mathbb{C}[\![t]\!]^n$，它属于 $h_0 = \cdots = h_{n-1} = 0$；而 $h_0 = \cdots = h_{n-1} = 0$ 的所有解都以这种方式得到。幂级数解 $\boldsymbol{\varphi}_{\boldsymbol{\alpha}}(t)$ 的系数是原方程组 $f_0,\dots,f_{n-1}$ 的系数的多项式函数。重要的是，这些幂级数的前 $(n+1)d^n$ 个系数可以由 $f_0,\dots,f_{n-1}$ 的系数通过一个常数深度、规模不超过 $d^{\mathrm{poly}(n)}$ 的算术电路计算得到，其中 $d = \max(d_0,\dots,d_{n-1})$。这使我们能够

计算一个近似解 $\widetilde{\boldsymbol{\varphi}_{\boldsymbol{\alpha}}}(t) \in \mathbb{C}[t]^n$，使其与 $\boldsymbol{\varphi}_{\boldsymbol{\alpha}}(t)$ 在次数 $(n+1)d^n$ 以内一致。将 h_n 代入每个近似解 $\widetilde{\boldsymbol{\varphi}_{\boldsymbol{\alpha}}}(t)$，并使用泊松公式，我们$\widetilde{\quad}$计算出一个多项式 $\mathrm{Res}(H_0,\ldots,H_n)$，它与结式 $\mathrm{Res}(H_0,\ldots,H_n)$ 模 $t^{(n+1)d^n}$ 同余。由于结式的次数至多为 $(n+1)d^n$，我们可以使用插值$\widetilde{\quad}$，恢复 $\mathrm{Res}(H_0,\ldots,H_n)$ 中关于 t 的次数至多为 $(n+1)d^n$ 的项，而这些项必然等于结式 $\mathrm{Res}(H_0,\ldots,H_n)$。

这种方法得到一个常数深度、指数规模的算术电路族，用于计算结式。要得出结式可以在 $\mathsf{FP}^{\mathsf{CH}}$ 中计算这一结论，我们需要确保这个电路族具有足够的一致性。很容易证明，该算法的大部分部分都是一致的。唯一不能立即看出一致性的部分，是我们使用求值插值，根据多项式的取值计算其系数。为此，需要构造一个一致的常数深度算术电路族来计算范德蒙矩阵的逆矩阵；我们通过范德蒙矩阵在点 1、2、.....、N处的逆矩阵的显式描述，用斯特林数来实现这一点。

到目前为止，我们已经看到，如何在 $\mathbb{Q}$ 上用 $\mathsf{FP}^{\mathsf{CH}}$ 计算多项式的结式。同一算法同样可以生成用于计算任意域上结式的常数深度算术电路，但在有限域上，一致性这一算术电路概念会更难处理。具体而言，我们的电路需要使用来自某个扩域的常数，而且必须以某种方式界定这些常数的一致性。相比之下，在 $\mathbb{Q}$ 上，无常数电路足以满足我们的需求，因此只需界定电路结构的一致性。要计算其他域上的结式，例如有限域 $\mathbb{F}_p$ 上的结式，我们利用结式在所有域上本质上都是同一个多项式这一事实。具体而言，对于多项式 ˆF_0、.....、$F_n \in \mathbb{F}_p[x_0,\ldots,x_n]$，如果将 F_i 提升为多项式 $F_i \in \mathbb{Z}[x_0,\ldots,x_n]$，那么结式满足

$$\mathrm{Res}(F_0,\ldots,F_n) = \mathrm{Res}(\hat{F}_0,\ldots,\hat{F}_n) \bmod p.$$

因此，要在 $\mathbb{F}_p$ 有限域 $\mathsf{FP}^{\mathsf{CH}}$ 上计算结式，我们先将输入提升到整数环上，在整数环上计算结式，然后将所得值模 p 化简。

1.3.4 从齐次系统到仿射系统

在 $\mathsf{FP}^{\mathsf{CH}}$ 中计算结式，使我们能够判定由 n 个关于 n 个变量的齐次方程组成的方程组是否有非零解；换言之，就是判定它在射影空间 $\mathbb{P}^{n-1}$ 中是否有解。不难将其扩展为一种可处理非方形射影方程组的算法：若给定 n 个变量上的 m 个方程 $F_1 = \cdots = F_m = 0$，其中 $m > n$，可以证明，将每个 G_i 取为 F_j 的随机线性组合所得到的方程组 $G_1 = \cdots = G_n = 0$，以高概率具有相同的解集。判定非齐次方程的可解性则更加困难。自然的做法是将给定的非齐次方程组齐次化，但这不一定能保持方程组的可解性。例如，方程组 $x+y-1 = x+y-2 = 0$ 无解，但其齐次化 $x+y-z = x+y-2z = 0$ 有非零解 $(1,\ -1,\ 0)$。

幸运的是，这个问题已经得到了解决。*Canny* 的广义特征多项式 [可90], Ierardi 后来扩展了它 [Ier89a], 通过对给定方程组施加微小扰动后计算结式，便可判断一个非齐次方程组是否有解。对广义特征多项式的构造稍作调整，就能得到一个一元多项式；假设给定方程组的解的数目有限，该多项式的根与方程组的解一一对应。这样一来，计算多元方程组解的数目，就转化为计算一个一元

次数呈指数级、但系数可在$\mathsf{FP}^{\mathsf{CH}}$中计算的多项式。若要在$\mathsf{FP}^{\mathsf{CH}}$中完成这项工作，我们改造 Andrews 和 Wigderson 的无平方因子分解算法 [AW24]；该算法利用常数深度、多项式规模的算术电路，计算一元多项式的无平方因子分解。将其推广到指数级次数的多项式后，便得到一个$\mathsf{FP}^{\mathsf{CH}}$ 算法，用于计算给定多项式不同根的数目。

1.4 组织结构

本文其余部分安排如下。第2节介绍记号，并介绍我们用于布尔和算术电路族的一致性概念，也涵盖计算代数方面的预备知识。在第 3 节中，我们证明包括多项式插值在内的基本运算可以由一致的常数深度算术电路族完成。第4节介绍多元结式，汇集结式的众所周知的性质，并说明如何利用结式判定零点定理以及计算零维方程组的解的数量。在第5节中，我们构造一个用于计算多元结式的一致常数深度算术电路族。第6节将这一电路族转换到布尔设置中，从而得到CH复杂性类算法，用于计算多元结式，并由此处理零点定理。最后，我们在第7节介绍我们用于零点定理的算法的一些直接应用，以此作为结尾。

2 预备知识

2.1 符号与约定

在全文中，我们用 $\mathbb{F}$ 表示一个域。我们使用和给出的各种结果对域 $\mathbb{F}$ 有不同的要求（例如，有些结果要求域足够大）。每条陈述都会明确说明对域 $\mathbb{F}$的要求。如果某个结果的陈述中没有这类限定，那么该结果对任意域都成立。我们用 $\mathbb{F}$ 表示 $\mathbb{F}$的代数闭包。

域 $\mathbb{F}$ 的系数子域 是 $\mathbb{F}$ 的素域在$\mathbb{F}$中的最大代数扩张。例如，如果 $\mathbb{F}=\mathbb{Q}(y)$，那么 $\mathbb{F}$ 的系数子域是 $\mathbb{Q}$；如果 $\mathbb{F}=\mathbb{F}_{p^a}$，那么 $\mathbb{F}$ 就是其自身的系数子域。

我们分别用 $\mathbb{F}[x_1,\ldots,x_n]$ 和 $\mathbb{F}(x_1,\ldots,x_n)$表示变量 $x_1,\ldots,x_n$ 的多项式环和有理函数域，系数取自 $\mathbb{F}$。向量简记为$\mathbf{x}=(x_1,\ldots,x_n)$。对于一个 $\in\mathbb{N}^n$，我们用$\mathbf{x^a}$ 表示单项式 $x_1^{a_1}\cdots x_n^{a_n}$。我们用 $|\mathbf{a}|$ 表示和$\sum_{i=1}^n a_i$。

次数为 d的型，指的是 $\mathbb{F}[x_1,\ldots,x_n]$ 中次数为 d的齐次元素。我们用大写字母表示型，用小写字母表示非齐次多项式。我们经常会处理一对多项式，其中一个是另一个的齐次化或去齐次化。在这种情况下，我们用同一字母的大写和小写形式作为提示，以表明它们之间的关系。例如，如果 $F\in\mathbb{F}[x_0,x_1,\ldots,x_n]$ 是一个型，我们用 $f(x_1,\ldots,x_n)$ 表示其去齐次化 $F(1,x_1,\ldots,x_n)$。同样，如果 $f\in\mathbb{F}[x_1,\ldots,x_n]$ 是次数为 d的非齐次多项式，我们用F表示其齐次化 $x_0^d f(x_1/x_0,\ldots,x_n/x_0)$。在某些情形下，我们可能会选择用不同的变量进行齐次化和去齐次化，具体会在上下文中说明。

对于多项式 f_1、……、 $f_m\in\mathbb{F}[x_1,\ldots,x_n]$，我们用 $\mathrm{V}(f_1$、……、 $f_m)$ 表示 f_1、……、 f_m 在 $\mathbb{F}^n$ 中的公共零点集。处理形式 F_1、……、 $F_m\in\mathbb{F}[x_0,\ldots,x_n]$时，我们则考虑它们在射影空间 $\mathbb{P}^n_{\mathbb{F}}$ 中的零点集 $\mathrm{V}(F_1$、……、 $F_m)$。通常我们会省略此记号对域的依赖，直接将 n维射影空间记作 $\mathbb{P}^n$ 。

我们用 Vand(x_1、……、 x_n) 表示使用 x_1、……、 x_n定义的范德蒙矩阵。具体而言，上述矩阵中位置 i、 j处的元素为 x_i^{j-1}。

我们经常需要讨论多项式相对于某个变量的尾项和尾部。为方便起见，我们定义以下记号。

定义 2.1。 设 $f \in \mathbb{F}[t, y_1, \ldots, y_m]$是一个非零多项式。 f相对于 t的尾项记为 $\mathrm{TT}_t\, f(y_1, \ldots\ldots, y_m)$，它是将 f视为关于 t的多项式时最低次数项的系数。具体而言，若 $f = t^i f_i(y_1, \ldots\ldots, y_m) + t^{i+1} f_{i+1}(y_1, \ldots\ldots, y_m) + \cdots + t^d f_d(y_1, \ldots\ldots, y_m)$，其中 $f_i(\mathbf{y}) \neq 0$，则 $\mathrm{TT}_t\, f = f_i$。

f相对于 t的尾部记作 $\mathrm{TP}_t\, f$，它是将 f中 t的最高次幂因式分解出来后得到的多项式。在上述设定中，我们有 $\mathrm{TP}_t\, f = f_i + t f_{i+1} + \cdots + t^{d-i} f_d$。B

约定 i用法,h长 ili项和 d th长 ili部分 f th零多项式lynomial 为零。 ◊

我们采用这样的约定：代数簇是代数闭域上某个多项式方程组的所有解构成的集合。特别地，代数簇不一定是不可约的。我们还采用这样的约定：可约射影簇或仿射簇的次数（记作 $\deg V$）是其所有不可约分支的次数之和。域 $\mathbb{F}$ 中任意两个一元多项式的最大公因式总取首一形式。

2.2 布尔电路族与算术电路族的一致性

本小节讨论布尔电路族与算术电路族的一致性概念，首先从布尔情形说起。我们将讨论范围限定为布尔阈值电路族。

衡量布尔电路一致性的方法有很多种 [Vol99]。在我们的工作中，我们通过布尔电路的直接连接语言的复杂性来衡量其一致性，定义如下。这一概念特别适用于非常弱的电路类，例如常深度电路。我们的表述遵循 Vollmer [Vol99], ，但有一项重要修改：大多数关于一致性的研究针对由单个参数索引的电路族$n \in \mathbb{N}$，而我们将研究由任意多个参数索引的电路族 n_1、……、 $n_k \in \mathbb{N}$，因此我们将直接连接语言的概念调整到这一情形。在定义直接连接语言之前，我们必须先定义电路的容许编码这一概念。

定义 2.2 ([第99卷，定义 2.14])。 设 $\mathcal{C} = (C_{k,\ n_1,\ \ldots\ldots,\ n_k})_{k,\ n_1,\ \ldots\ldots,\ n_k \in \mathbb{N}}$ 是一个规模为 $s := s(k,\ n_1,\ \ldots\ldots,\ n_k)$ 的布尔电路族。 $\mathcal{C}$的容许编码是指对该电路族中每个电路 $C = C_{k,\ n_1,\ \ldots\ldots,\ n_k}$ 的门进行编号，并满足以下性质。

1. 如果 C有 m 个输入门，则它们的编号为 $0, \ldots\ldots, m-1$。2. 如果 C有 m' 个输出门，则它们的编号为 $m, \ldots\ldots, m+m'-1$。3. 存在一个常数 c，仅取决于该电路族，使得 C 中任意门的编号的二进制表示长度至多为 $c \cdot \log(s)$。◊

对于具有容许编码的阈值电路族，我们定义其直接连接语言如下。

定义 2.3 （直接连接语言）。 设 $\mathcal{C} = (C_{k,n_1,\ldots,n_k})_{k,n_1,\ldots,n_k \in \mathbb{N}}$ 是一个带有容许编码的阈值电路族。假设门类型（与、或、非、多数、0、1）的编号已固定。 $\mathcal{C}$ 的直接连接语言记作 $L_{DC}(\mathcal{C})$，它由以下元组的二进制编码组成：$(k, n_1, \ldots, n_k, a, p, b)$，其中

1. a 是$C_{k、\ n_1、\ \ldots\ldots n_k}$中一个门的编号。2. 如果 $p \neq \epsilon$，那么 b 是$C_{k、\ n_1、\ \ldots\ldots n_k}$ 中一个门的编号，且该门是 a的直接前驱。

3. 如果 $p = \epsilon$，那么 b 编码了 a 的门类型（使用固定的门类型编号） . ◊

通过修改允许的门类型，上述定义也可以扩展到其他类型的布尔电路族；不过，本文只研究阈值电路。电路族的一致性可以通过直接连接语言的复杂性来衡量，具体如下。

定义 2.4. 设 $\mathcal{C} = (C_{k,n_1,\ldots,n_k})_{k,n_1,\ldots,n_k \in \mathbb{N}}$ 是一个规模为 $s := s(k, n_1, \ldots, n_k)$、具有容许编码的阈值电路族。若该电路族 $\mathcal{C}$ 满足以下条件，则称其为多对数时间一致：

1. 其直接连接语言 $L_{DC}\,\mathcal{C}$ $s + k +$ $\sum_{i=1}^{k}$ ( ) 可在关于 log( ) log( ) log( ) n_i 的多项式时间内判定；2. $C_{k,n_1,\ldots,n_k}$的输入和输出数量，以及其规模 s 的一个上界，均可在关于 $\log(s) + \log(k) + \sum_{i=1}^{k} \log(n_i)$ 的多项式时间内计算，其中输入为 $(k, n_1, \ldots, n_k)$。

我们称电路族 $\mathcal{C}$ 是对数时间一致的，如果这两项任务都能在与 $\log(s) + \log(k) + \sum_{i=1}^{k} \log(n_i)$ 成线性的时间内完成。◊

对于由单个参数索引的电路族，上述定义要求图灵机能够在关于电路规模以及该电路族内索引的多重对数时间内判定直接连接语言。我们指出，上述第二项通常并不属于标准定义。我们将其纳入，是为了更便于一致地组合电路。

在前述定义中，第一个索引是其余索引个数的计数。在我们设计的电路中，我们将对此稍作推广，并允许索引个数是第一个索引的函数。该函数始终非常简单；在所有应用中，索引个数都将是第一个索引的线性函数，例如第一个索引的两倍加二。在索引个数仅为常数的情形中，例如由单个参数索引的族，我们并不把第一个索引用作索引个数的计数。例如，单索引电路族就写成 $(C_n)_n$，而不是如上述记号所可能暗示的 $(C_{1,n})_n$ 。我们还用向量记号作为多重索引族的简写。例如，我们用 $(C_{\mathbf{n}})_{\mathbf{n}}$ 表示由 $k, n_1, \ldots, n_k$ 索引的族，并用 $C_{\mathbf{n}}$ 表示该族中的某个具体电路。在所有情形中，索引的确切个数始终可从上下文清楚看出。

注 2.5. 容许编码的定义让我们在选择门的编号方式时拥有很大的自由度。除了输入门和输出门之外，只要满足长度限制，我们可以任意给门编号。这种自由度使我们能够用 1 到 s 以外的整数来给门编号：我们可以将整数元组解释为门名称，下面将对此进行说明。接下来，为避免混淆，当我们用自然数以外的对象为门编号时，将称其为门的名称，而不称其为编号。

例如，我们可以这样设计门名称为自然数对的电路。存在高效的方案，可以将自然数对编码为单个自然数；若逆映射存在，这些编码方案也可以高效求逆。固定这样一种方案后，我们可以使用诸如 $(i,\ j)$ 这样的自然数对作为名称，并约定门的实际编号是将自然数对 $(i,\ j)$ 编码为单个自然数所得的结果。

必须注意遵守输入输出编号的条件：我们必须确保编码方案能将这些门映射到 0，……，$m - 1$ 与m，……，$m + m' - 1$。在所有依赖此类命名约定的情形中，给定一个输入门或输出门的名称（由一对或一个元组的整数表示），我们总能

在限定时间内判定它是输入还是输出，并确定其索引；反过来也同样成立。对于输入和输出之外的门，我们将使用上述方案，把一对（或一个元组的）整数映射为一个大于 $m + m' - 1$的单个整数，反之亦然（回顾一下，输入和输出的数量可以在多对数时间内计算）。◊

注 2.6. 假设我们处理的是一个多对数时间一致电路族。我们可以利用电路的索引和门名称，高效地确定门的类型，具体方法如下。给定电路的索引 $(k,\ n_1,\ \ldots\ldots,\ n_k)$ 以及电路中某个门的名称 a，我们遍历所有门类型 b，并检查元组 $(k,\ n_1,\ \ldots\ldots,\ n_k,\ a,\ \epsilon,\ b)$ 是否属于直接连接语言。由于门类型的数量是一个常数，因此给定门的名称后，我们就能计算出该门的类型。

给定输入 $(k, n_1, \ldots, n_k, a)$，我们还可以在关于 $\log(s) + \log(k) + \sum_{i=1}^{k} \log(n_i)$ 的多项式时间内，判断候选门名称 a 是否有效。我们首先计算 s 的一个上界 s'；根据定义，这可以在限定的时间内完成；然后，我们检查 a 的长度是否至多为 $c\log(s')$，其中 c 是定义 2.2 中的常数。由于 $\log(s')$ 本身关于 $\log(s) + \log(k) + \sum_{i=1}^{k} \log(n_i)$ 是多项式的，因此这也符合我们的时间界。如果不符合，则拒绝。否则，我们按上述方法继续，为所有门类型 b 构造字符串 $(k, n_1, \ldots, n_k, a, \epsilon, b)$，并检查它们是否属于直接连接语言。

同样，我们总能判断给定的门是否为输入门或输出门，因为我们可以确定特定电路的输入和输出数量。◊

注记 2.7. 在我们的电路中，我们还会仔细安排输入和输出的顺序，以便简化其他计算。例如，如果电路的输出表示矩阵的元素，我们可以选择按行优先顺序排列输出。如果电路的输出表示多项式的系数，我们会固定一种单项式顺序，并据此排列输出。◊

现在我们来定义一致算术电路族。首先给出算术电路的定义。

定义 2.8. 设 $\mathbb{F}$ 是一个域，$\mathbb{F}(\mathbf{x})$是变量$x_1, \ldots, x_n$上的有理函数域，其中系数取自 $\mathbb{F}$。一个在上的算术电路是一个有向无环图。该图中入度为零的顶点称为输入门，并标记为一个变量 x_i；或者称为常数门，并标记为一个域元素 $\alpha \in \mathbb{F}$。入度为正的顶点称为内部门，并标记为 $\{+, \times, \div\}$中的一个运算。出度为零的顶点称为输出门。假设电路中没有发生除以零的情况（这是我们的要求），则电路中的每个门都会自然地计算 $\mathbb{F}(\mathbf{x})$中的一个元素。若 $\{f_1, \ldots, f_m\}$ 是电路输出门所计算的函数，则称该电路计算函数 $f_1, \ldots, f_m$。电路的规模是电路中连线的数量。电路的深度是电路中从输入到输出的最长路径的长度。

如果电路输入门上的唯一标记常数是 0、$+1$ 和 -1，则称该电路为无常数电路。对于固定变量 x_i，如果电路中每个除法门的分母所对应的子树都不包含与 x_i 对应的输入门，则称该电路关于 x_i 无除法。如果 X' 是变量的一个子集，且该电路关于 X'中的每个变量都无除法，则称该电路关于 X' 无除法。如果该电路关于所有变量都无除法，则称该电路为弱无除法电路。◊

处理算术电路族时，一致性还必须考虑构造电路中所用域元素的复杂性（这些元素见 α 定义 2.8）。文献 [Gat86]讨论了若干将域元素纳入考量的一致性定义。本文将仅研究无常数电路。电路中需要使用的任何域元素，都必须通过 $+1$ 与 -1来构造。这样便避开了以下问题：

必须为电路族中所用的域元素定义一致性概念。因此，我们可以采用一种针对算术电路族的一致性概念，使其与针对布尔电路族的一致性概念非常相似。

之后我们将尝试用布尔阈值电路来模拟算术电路。我们将以便于实现这种模拟的方式定义一致性概念。在布尔情形中，直接连接语言只能回答如下形式的查询：门 b 的类型是否为 以及 门 b 是否是门 a 的前驱节点？为了实现模拟，我们对算术电路族的一致性提出稍严格的要求。给定一个具有 k 个前驱节点的门 a，我们希望能够回答如下形式的查询：门 b 是否是门 i^{th} 的前驱节点？为此，我们当然要求对电路中每个门的所有前驱节点进行排序。这将作为算术电路容许编码定义的一部分。

定义 2.9（容许编码）。设 $\mathbb{F}$ 是一个域，且 $\mathcal{C} = (C_{k,\ n_1,\ \ldots\ldots,\ n_k})_{k,\ n_1,\ \ldots\ldots,\ n_k \in \mathbb{N}}$ 是一个定义在 $\mathbb{F}$ 上、规模为 $s := s(k,\ n_1,\ \ldots\ldots,\ n_k)$ 的无常数算术电路族。$\mathcal{C}$ 的容许编码是指对该族中每个电路 $C = C_{k,\ n_1,\ \ldots\ldots,\ n_k}$ 的门进行编号，并满足以下性质。

1. 如果 C 有 m 个输入门，则它们的编号为 0，……，$m-1$。2. 如果 C 有 m' 个输出门，则它们的编号为 m，……，$m+m'-1$。3. 存在一个仅取决于电路族的常数 c，使得 C 中任意门的编号的二进制表示长度至多为 $c \cdot \log(s)$。

此外，对于每个门 $a \in C$，我们都为 a 在 C中的直接前驱集合指定编号。我们要求这些前驱的编号连续，即从 1 开始，到 a的元数为止。我们不要求前驱的编号遵循门本身的编号：如果 b_1 和 b_2 是 a 的两个前驱，且在 C 的门编号中 b_1 排在 b_2 之前，我们不要求 b_1 在 a 的前驱编号中排在 b_2 之前。对于除法门，我们要求分子在前驱编号中排在分母之前。◊

定义 2.10。设 $\mathbb{F}$ 是一个域，且 $\mathcal{C} = (C_{k,n_1,\ldots,n_k})_{k,n_1,\ldots,n_k \in \mathbb{N}}$ 是一个在 $\mathbb{F}$ 上、采用容许编码的无常数算术电路族。假设门类型 $(+, -, \times, \div, +1, 0, -1)$ 的编号已固定。$\mathcal{C}$ 的直接连接语言记作 $L_{DC}(\mathcal{C})$，它由元组 $(k, n_1, \ldots, n_k, a, p, b)$ 的二进制编码组成，其中

1. a 是 $C_{k,n_1,\ldots,n_k}$ 中某个门的编号。2. 如果 $p \neq \epsilon$，那么 b 是 a 在 $C_{k,n_1,\ldots,n_k}$ 中的第 p^{th} 个前驱门的编号。3. 如果 $p = \epsilon$，那么 b 对 a 的门类型进行编码（使用固定的门类型编号）。

◊

与布尔情形一样，我们用电路族 $\mathcal{C} = (C_{k,n_1,\ldots,n_k})_{k,n_1,\ldots,n_k \in \mathbb{N}}$ 的直接连接语言 $L_{DC}(\mathcal{C})$ 的复杂性来度量其一致性。

定义 2.11。设 $\mathbb{F}$ 是一个域，并设 $\mathcal{C} = (C_{k,\ n_1,\ \ldots\ldots,\ n_k})_{k,\ n_1,\ \ldots\ldots,\ n_k \in \mathbb{N}}$ 是一个规模为 $s := s(k,\ n_1,\ \ldots\ldots,\ n_k)$ 的无常数算术电路族，其定义在具有容许编码的 $\mathbb{F}$ 上。我们称电路族 $\mathcal{C}$ 是多对数时间一致的，当且仅当

1. 其直接连接语言 L_{DC} $\mathcal{C}$ s + k + $\sum_{i=1}^{k}$ n_i ( ) 可在关于 log( ) log( ) log( ) 的多项式时间内判定；2. 给定 $(k, n_1, \ldots, n_k)$ 作为输入，可在关于 $\log(s) + \log(k) + \sum_{i=1}^{k} \log(n_i)$ 的多项式时间内计算 $C_{k,n_1,\ldots,n_k}$ 的输入和输出数量，以及规模 s 的一个上界。

3. 给定 $(k, n_1, \ldots, n_k)$ 和门名称作为输入，可在关于 $\log(s)+\log(k)+\sum_{i=1}^{k}\log(n_i)$ 的多项式时间内计算门的元数。

我们称电路族 $\mathcal{C}$ 是对数时间一致的，如果这些任务可以在与 $\log(s)+\log(k)+\sum_{i=1}^{k}\log(n_i)$ 成线性关系的时间内完成。◊

注 2.5 至2.7 可原样应用于算术情形。

2.3 整数、有理数与有限域算术

本节讨论图灵机和布尔电路如何表示不同域中的元素。我们还概述一些基本的整数和有理数算术运算，这些运算属于 TC^0。

$\mathbb{Z}$ 中的元素将以二进制表示，并附加一个符号位。对于整数 $a \in \mathbb{Z}$，a 的高度定义为 $\lceil \log_2(|a|) \rceil$，因此，高度为 h 的整数使用 $h+1$ 位表示（计入符号位）。系数属于 $\mathbb{Z}$ 的多项式的高度定义为其系数高度的最大值。在这种表示下，有如下结论。

定理 2.12. 下列函数属于对数时间一致的 TC^0。

1. 迭代整数加法：给定 n 个整数 a_1，……，a_n 作为输入，每个至多包含 n 比特，计算和 $a_1+\cdots+a_n$。
2. 迭代整数乘法：给定 n 个整数 a_1，……，a_n 作为输入，每个由至多 n 比特组成，计算乘积 $a_1 \cdots a_n$。
3. 整数除法：给定整数 a 和 b 作为输入，计算 $\lfloor a/b \rfloor$。
4. 带余多项式除法：给定整数 a_0，……，a_n 和 b_0，……，b_m 作为输入，其中 $b_m \neq 0$ 和 $n \geq m$，计算 $d := b_m^{n-m+1}$ 以及整数 q_0，……，q_{n-m}，r_0，……，r_{m-1}，使得对于

$$f(x) := a_n x^n + \cdots + a_1 x + a_0 \qquad q(x) := q_{n-m}x^{n-m} + \cdots + q_1 x + q_0$$
$$g(x) := b_m x^m + \cdots + b_1 x + b_0 \qquad r(x) := r_{m-1}x^{m-1} + \cdots + r_1 x + r_0,$$

我们有 $d \cdot f(x) = q(x)g(x) + r(x)$。

5. 迭代多项式乘法：给定作为输入的整数 $a_{1,0}, \ldots, a_{m,n}$，计算整数 $b_0, \ldots, b_{mn}$，使得

$$b_{mn}x^{mn} + b_{mn-1}x^{mn-1} + \cdots + b_1 x + b_0 = \prod_{i=1}^{m}(a_{i,n}x^n + a_{i,n-1}x^{n-1} + \cdots + a_{i,1}x + a_{i,0}).$$

证明。第 1 项是经典结果，参见 [RT92]。第 2 项和第 3 项是 [HAM02] 的主要结果。第 4 项和第 5 项来自 [HAM02，推论 6。5]。对于上述所有各项，输入位数和输出位数都可以根据相应族中电路的索引轻松计算。□

第 4 项执行的操作是伪除法。上述记号中的多项式 q 和 r 分别称为 f 和 g 的伪商 和伪余式 。

多元多项式将以稠密表示的方式表示。换言之，每个次数不超过指定次数的单项式（包括系数为零的单项式）的系数都会被

列出。为了将 $\mathbb{Z}[y_1, \ldots, y_k]$中的多项式相乘，我们使用克罗内克代换将问题归约到单变量情形。若要将 m 个次数为 d的这类多项式相乘，那么我们对每个$z^{(md+1)^i}$ 代入 y_i。这样便得到 m 个次数为 $(md)^{O(k)}$的多项式，我们可以使用定理 2.12所提供的单变量乘法电路进行相乘。乘积中$\mathbf{y}$ 单项式的系数，可以从上述代换后乘积中 z 的系数读出。

$q \in \mathbb{Q}$ 的一个元素将由一对整数 a, b 表示，并有 $b \neq 0$ 使得 $q = a/b$，其中 a, b可以有公因子。我们允许 a, b有公因子，是因为计算整数最大公约数尚不知是否属于TC^0,，因此我们所使用的电路无法把一个分数化为最简形式。一对整数 a, b 的高度就是 a 和 b的高度的最大值。

上述表示下有理数的迭代乘法与加法可由多对数时间一致TC^0 电路完成，方法如下。对于迭代乘法，我们利用迭代整数乘法的电路分别将分子与分母相乘（定理 2.12）。这直接给出乘积的一种表示。对于迭代加法，我们首先将所有元素化为公分母。该公分母是输入各分母的乘积，因此每个输入在此公分母下的表示可利用来自定理 2.12的迭代整数乘法电路计算得到。一旦得到该表示，我们便可利用迭代整数加法电路将分子相加，该电路同样来自定理 2.12。

根据本原元定理，每个数域 $\mathbb{K}$ 都具有如下形式：$\mathbb{Q}[\alpha] \cong \mathbb{Q}[z]/(g(z))$，其中$\alpha$ 是一个代数数，其最小多项式为 $g(z)$。因此，数域 $\mathbb{K}$ 中的元素将用 $\mathbb{Q}[z]$ 中的次数小于 $\deg g$的多项式表示。每当我们处理这样的数域时，都假设 $g(z)$作为输入的一部分给出。

$\mathbb{F}_p$中的元素（其中 p是素数）将用介于 0 和 $p-1$（含）之间的整数表示。$\mathbb{F}_p$ 中元素的高度 定义为 $\log(p)$。

有限域 $\mathbb{F}_{p^a}$ 同构于某个不可约多项式 $g(z) \in \mathbb{F}_p[z]$ 的商域 $\mathbb{F}_p[z]/(g(z))$，其次数为 a。因此，域 $\mathbb{F}_{p^a}$ 中的元素将用 $\mathbb{F}_p[z]$ 中的次数小于 a的多项式表示。每当我们处理这样的有限域时，都假设 $g(z)$作为输入的一部分给出，且 $g(z)$是首一的。$\mathbb{F}_{p^a}$ 中元素的高度 定义为 $a\log(p)$。对于上文讨论的每个环 R，系数属于 R 的多项式的高度是其各系数高度的最大值。

我们的算法有时要求所使用的域具有大于某个界限 B的系数子域。如果输入位于系数子域为 $\mathbb{F}_{p^a}$、且 p^a 小于 B的域中，那么我们会改为扩张到一个足够大的域，并在该域上进行运算。下面的引理表明，图灵机可以高效地完成这一过程。

引理 2.13. 给定由不可约多项式 $g(y) \in \mathbb{F}_p[y]$ 定义的有限域 $\mathbb{F}_{p^a}$，该多项式的次数为 a，以及一个界限 B，存在一种拉斯维加斯算法，可以显式构造有限域 $\mathbb{F}_{p^b}$，使得 $p^b \geq B$，且 $\mathbb{F}_{p^a}$ 是 $\mathbb{F}_{p^b}$ 的子域。该算法还会构造一个 $\mathbb{F}_p$-线性映射 ϕ （以关于 y 的幂基表示的矩阵形式给出），将 $\mathbb{F}_{p^a}$ 映射到 $\mathbb{F}_{p^b}$的一个同构子域。该算法的期望运行时间关于 a对数 p 和 对数 $|B|$是多项式级的。

证明。回顾一下，$\mathbb{F}_{p^n}$ 是 $\mathbb{F}_{p^m}$ 的子域，当且仅当 m 是 n的倍数。因此，我们选取 b 为大于 $\log |B|/\log p$的 a 的最小倍数。要构造次数为 b的不可约多项式，我们只需在 $\mathbb{F}_p[y]$ 上随机抽取一个次数为 b 的随机多项式，并检验其是否不可约。根据[GG13，推论 14.39],，期望而言，这可以通过在 $\mathbb{F}_p$ 中进行 $\widetilde{O}\left(b^3 + b^2 \log p\right)$ 次运算来完成。记这个不可约多项式为 $h(y)$。

要构造 $\mathbb{F}_{p^a}$ 与 $\mathbb{F}_{p^b}$之间的映射，我们只需在 $\mathbb{F}_{p^b}$中找到 g 的一个根。根据费马小定理以及多项式分解的结构，这样的根确实存在。

关于有限域中的情形，参见例如 [GG13, Theorem 14.2]。根据 [GG13, 推论 14.16], ，找到这个 ˜根，期望需要 $O(ab\log\ p)$ 次 $\mathbb{F}_{p^b}$ 运算。如果 α 是这样的一个根，那么将 $\mathbb{F}_p[y]/(g(y))$ 中的 y 映射到 α 的映射ϕ，是 $\mathbb{F}_{p^a}$ 与 $\mathbb{F}_{p^b}$的一个子域之间的同构。 □

我们指出，上述方法远非构造相容域扩张的最优方法。不过，这已足以满足我们的应用需求。

3 算术电路基本运算的一致性

本节将证明，算术电路上的基本运算可以用保持一致性的方式实现。特别地，我们将证明，多项式插值——一种用于构造低深度算术电路的标准工具——可以一致实现。由此，我们得到了一致算术电路族，用于计算初等对称多项式以及符号范德蒙矩阵的逆。

这些构造所用的主要技术工具，是一个以第一类斯特林数表示范德蒙矩阵 Vand(1，...， n) 的逆矩阵元素的显式公式。结合斯特林数的一个显式公式，我们得到一个电路族，用于计算 Vand(1，...， n) 的逆矩阵的元素。提醒读者，下面的证明会详尽到近乎繁琐，这只是因为这是第一个运用了上述一致性概念的证明。

引理 3.1。 存在一个多对数时间一致的无常数、常深度电路族$\mathcal{C} = (C_n)_{n\in\mathbb{N}}$，其定义在 $\mathbb{Q}$ 上，其中 C_n 没有输入， n^2 个输出，规模为 poly(n)，并计算范德蒙德矩阵 $\mathrm{Vand}(1，\ldots，\ n)$ 的逆矩阵的元素。

证明。 Macon 和 Spitzbart 给出了 $\mathrm{Vand}^{-1}(1，\ldots，\ n)$ 的元素的显式公式[MS58], ，以下陈述来自 [EFP98，引理 4]。令 V_n 表示 $\mathrm{Vand}(1，\ldots，\ n)$，则有

$$\left(V_n^{-1}\right)_{j,i} = (-1)^{i+j} \sum_{k=\max(i,j)}^{n} \frac{1}{(k-1)!}\binom{k-1}{i-1} s(k,j), \tag{1}$$

其中 $s(\cdot，\ \cdot)$ 表示第一类斯特林数。这些斯特林数可以使用以下公式计算：

$$s(a,b) = \sum_{j=a}^{2a-b}\binom{j-1}{b-1}\binom{2a-b}{j}\sum_{m=0}^{j-a}\frac{(-1)^{m+a-b}m^{j-b}}{m!(j-a-m)!}, \tag{2}$$

该公式由第二类斯特林数的显式公式与联系两类斯特林数的对称公式结合而得（参见 [Cha02，公式 8。21]）。

我们使用这些公式实现电路 C_n。我们的门名称将是数字元组。

1. 我们从常数 $+1$ 和 -1 开始，各复制 $2n$ 份。对于每个 $i \in [2n]$，名称为 $(0, i)$ 和 $(1, i)$ 的门分别是标记为常数 $+1$ 和 -1 的常数门。

2. 接下来，我们计算从 1 到 $2n$ 的每个数的 $2n$ 份副本。对于每个 $i, j \in [2n]$，名称为 $(2, i, j)$ 的门是一个 $+$ 门，其输入是名称为 $(0, k)$ 的门（对应 $k \le i$）。门 $(2, i, j)$ 计算 i。$(2, i, j)$ 的 p^{th} 前驱是 $(0, p)$。

3. 接下来计算阶乘。对于每个 $i \in [2n]$，名称为 $(3，\ i)$ 的门是一个 $\times$ 门，其输入是名称为 $(1，\ j)$（对应 $j \le i$）的各个门。门 $(3，\ i)$ 计算 $i!$。 $(3，\ i)$ 的 p^{th} 前驱是 $(1，\ p)$。

4. 现在计算二项式系数。对于每个 $i \in [2n]$ 和 $j \le i$，我们有名称为 (4, 1, i, j) 和 (4, 2, i, j) 的门。门 (4, 1, i, j) 是一个 $\times$ 门，其输入依次为门 (3, j) 和 (3, $i-j$)。门 (4, 2, i, j) 是一个 $\div$ 门，其分子为 (3, i)，分母为 (4, 1, i, j)。由于 (3, i) 计算 $i!$，且 (4, 1, i, j) 计算 $(i-j)! \cdot j!$，因此门 (4, 2, i, j) 计算 $\binom{i}{j}$。

5. 接下来，我们计算形如 i^j 的数，其中 i 和 j 在 $[2n]$ 上变化。特别地，对于每个$i,\ j \in [2n]$，门 (5，i，j) 是一个 $\times$ 门，其输入为 (2，i，k)，对每个 $k \le j$ 都如此（前驱节点也将按此顺序编号）。这样，门 (5，i，j) 就计算出 i^j。

6. 现在我们使用 公式 (2) 计算斯特林数。对于每个 a，$b \in [n]$，其中 $b \le a$，我们按如下方式计算双重求和中的 $(j,\ m)$ 项，其中 $j \in \{a, \ldots, 2a-b\}$ 且 $m \in \{0, \ldots, j-a\}$。

(a) 门 (6, a, b, j, m, 1) 是一个 $\times$ 门，其输入为 (3, m) 和 (3, $j-a-m$)。该门计算阶乘的乘积 $m! \cdot (j-a-m)!$。(b) 门 (6, a, b, j, m, 2) 是一个 $\times$ 门，其第一个输入为 (5, $m, j-b$)，第二个输入则根据 $m+a-b$ 的奇偶性，取 (0, 1) 或 (1, 1)。该门计算 $(-1)^{m+a-b} m^{j-b}$。(c) 门 (6, a, b, j, m, 3) 是一个 $\div$ 门，其分子为 (6, a, b, j, m, 2)，分母为 (6, a, b, j, m, 1)。该门计算 $(-1)^{m+a-b} m^{j-b} / (j-a-m)!$。(d) 最后，门 (6, a, b, j, m, 4) 是一个 $\times$ 门，其输入为 (6, a, b, j, m, 3)、(4, 2, $2a-b, j$) 和 (4, 2, $j-1, b-1$)。该门计算 $\binom{j-1}{b-1}\binom{2a-b}{j}(-1)^{m+a-b}/(j-a-m)!$，这恰好就是用于计算斯特林数 $s(a, b)$ 的双重求和中出现的 (j, m) 项。

对于上面每个门，其前驱节点按我们介绍它们的顺序编号。为计算斯特林数 $s(a,\ b)$，我们添加一个 $+$ 门 (7，a，b)，其输入为 (6，a，b，j，m，4)，其中所有 $j \in \{a, \ldots, 2a-b\}$ 和 $m \in \{0, \ldots, j-a\}$ 均满足条件。(7，a，b) 的前驱节点根据 (j，m) 按字典序编号。给定二进制表示的 a、b 和 p，可以在多项式时间内计算出满足该约束的数对中字典序第 p^{th} 个元素。

7. 最后，我们使用 公式 (1)计算范德蒙德矩阵的逆矩阵的元素。对于 $i,\ j \in [n]$，我们计算求和中的第 k^{th} 项，其中 $k \in \{\max(i,\ j)\ldots\ldots,\ n\}$，具体如下。

(a) 门 (8, i, j, k, 1) 是一个 $\div$ 门，其分子为 (0, 1)，分母为 (3, $k-1$)。此门计算 $^1 (k-1)!$ (b) 门 (8, i, j, k, 2) 是一个~~$\times$~~门，其输入为 (8, i, j, k, 1)、(4, 2, $k-1, i-1$) 和 (7, k, j)。此门计算 $^1 (k-1)! \binom{k-1}{i-1} s(k, j)$。

为了计算 V_n^{-1} 的 (i, j) 项，我们添加一个 $+$ 门 (9, i, j)，其输入为所有 $k \in \{\max(i, j) \ldots, n\}$ 对应的 (8, i, j, k, 2)。我们添加一个最终的 $\times$ 门 (10, i, j)，其输入为 (9, i, j)，以及 (0, 1) 或 (1, 1)，具体取决于 $i+j$ 的奇偶性。根据式 (1)，门 (10, i, j) 正确计算出 V_n^{-1} 的 (j, i) 项。

最后，对于上述每一个门，其前驱节点均按我们给出它们的顺序编号。

根据前述计算 V_n^{-1}的电路描述，显然该电路的规模是 n 的多项式，且深度由一个通用常数所界定。上述描述也可用于界定该电路族的一致性。存在固定数量的规则来确定一个门的类型及其前驱节点。这些规则可直接转化为一台图灵机的构造：该图灵机能够在$\log(n)$的多项式时间内确定一个门的类型，或判定一个门是否为另一个门的前驱。唯一具有多于常数个前驱节点的门，是那些计算各种常数的门，以及名称为$(7, i, j)$和$(9, i, j)$的门。对于这些门中的每一个，电路描述说明了如何在门名称的二进制长度以及电路索引的多项式时间内计算出 a 的第 p^{th} 个前驱。因此，我们可以计算出 a 的第p^{th} 个前驱，并检查其是否与 b 相符，从而判定直接连接语言。电路构造明确陈述了每个门的元数，因此这也可以高效地计算。最后，电路的规模也可从上述构造中明显看出，因此所需的规模上界同样可以高效地计算。

□

插值的一致性将由上述引理推出。我们首先说明如何对单个变量的系数进行插值，然后处理一般情形。

引理 3.2。 设 $\mathcal{C} =(C_{\mathbf{n}})_{\mathbf{n}}$ 是一个在 $\mathbb{Q}$ 上的多对数时间一致算术电路族，其规模为 $s_{\mathbf{n}}$，深度有常数 Δ作为上界，并且只有一个输出。设 $f_{\mathbf{n}}$ 是由 $C_{\mathbf{n}}$计算的有理函数，设 y 是一个指定变量，并假设每个 $C_{\mathbf{n}}$ 相对于 y都是无除法的，因此 $f_{\mathbf{n}} \in \mathbb{Q}(\mathbf{x})[y]$。

设 $d_{\mathbf{n}}$是 $f_{\mathbf{n}}$在 y中的次数上界，并设 $f_{\mathbf{n},\,0}$、…、$f_{\mathbf{n},\,d_{\mathbf{n}}} \in \mathbb{Q}(\mathbf{x})$ 满足

$$f_{\mathbf{n}}(\mathbf{x}, y) = \sum_{i=0}^{d_{\mathbf{n}}} f_{\mathbf{n},i}(\mathbf{x}) y^i.$$

最后，假设可以从$\mathbf{n}$ 的二进制表示出发，在关于$\mathbf{n}$ 的二进制长度和 $\log(d_{\mathbf{n}})$上多项式时间内计算出 $d_{\mathbf{n}}$ 的二进制表示。那么存在一个多对数时间一致算术电路族 $\mathcal{D} = (D_{\mathbf{n}})_{\mathbf{n}}$，它在 $\mathbb{Q}$ 上，规模为 $\text{poly}(s_{\mathbf{n}}, d_{\mathbf{n}})$，深度至多为 $\Delta + O(1)$，使得 $D_{\mathbf{n}}$ 计算 $f_{\mathbf{n},\,0}$、…、$f_{\mathbf{n},\,d_{\mathbf{n}}}$。

证明。 固定 $C = C_{\mathbf{n}}$、 $f = f_{\mathbf{n}}$ 和 $d = d_{\mathbf{n}}$。我们来描述电路 $D = D_{\mathbf{n}}$。

电路 D 首先计算数字 $1, \ldots, d+1$。与引理 3.1 的证明一样，我们有一组标记为常数 1 的门，并使用加法门由这些常数计算出 $1, \ldots, d+1$。常数门对 $i \in [d+1]$ 分别命名为 $(1, i)$，而计算 $1, \ldots, d+1$ 的门对 $i \in [d+1]$ 分别命名为 $(2, i)$。对于这些加法门，只要满足 $p \le i$，$(2, i)$ 的 p^{th} 前驱就是 $(1, p)$。

接着，电路 D 包含 $d+1$ 个 C 的副本。在第 i^{th} 个副本中，输入门 y 被转换为只有一个输入的求和门，该输入就是计算数字 i 的门 $(2,\ i)$。 C 的其他输入门也被转换为求和门，其唯一输入是 D 的输入门，且该输入门标记为相同的变量。因此，这些 C 的副本计算部分求值 $f(\mathbf{x},\ 1), \ldots, f(\mathbf{x}\ d+1)$。条件 y 不出现在 C 的任何分母中，确保电路不会除以零。这些 C 副本中的门按如下方式命名：若 v 是 C 中某个门的名称，那么在 D 中 C 的第 i^{th} 个副本里，对应的门命名为 $(3,\ i,\ v)$。

该电路 D 还包含一个副本，该副本是根据引理 3.1 中构造的、用于计算范德蒙德矩阵的逆矩阵$\text{Vand}(1, \ldots, d+1)$的电路。我们将此电路记为 V。对于每个名称为v 且属于 V的门，其在 D 中的对应副本命名为$(4, v)$。

多项式$f_{\mathbf{n},\,i}(\mathbf{x})$是范德蒙德矩阵的逆矩阵的一列与 C各副本输出的内积。这些输出通过 $d+1$ 个乘积门和一个

求和门各自计算得出。对于每个 $i,\ j \in [d+1]$，门 $(5,\ i,\ j)$ 是一个 $\times$ 门，与j^{th} 副本的输出以及范德蒙德矩阵的逆矩阵的 $(j,\ i)$ 项相连，其前驱节点按此顺序编号。对于每个 $i \in [d+1]$，门 $(6,\ i)$ 是一个 $+$门，其输入为所有$j \in [d+1]$对应的 $(5,\ i,\ j)$。$(6,\ i)$ 的 p^{th} 个前驱节点是 $(5,\ i,\ p)$。门 $(6,\ i)$ 计算多项式 $f_{\mathbf{n},\ i}(\mathbf{x})$。

关于电路族 $\mathcal{D}$ 的规模与深度的断言，由上述描述以及对 D的子电路的相应界得出。我们现在通过描述如何判定直接连接语言，来论证 $\mathcal{D}$ 是一个多对数时间一致族。

设 T_C 与 T_V 分别表示判定 C 与V的直接连接语言的图灵机。我们将设计一台判定D的直接连接语言的图灵机 T_D 。设$(\mathbf{n}\ a, p, b)$为 T_D的一个输入。由门名称 a的第一项，我们可以确定该门在 D 中所处的位置：它是计算常数的一部分、C某一副本中的一个门、计算范德蒙德矩阵的逆矩阵的电路的一部分，还是内积计算的一部分。若 a 属于计算常数的子电路，则判定该输入是否为是实例是直接的。

假设 a 是 C的 i^{th} 副本的一部分。由 a，我们可以提取C 中那个门的名称 v_a ，而 a 是该门的一个副本。该机器确认 $i \leq d+1$ （回顾： $d = d_{\mathbf{n}}$ 可在$\mathbf{n}$与 $d_{\mathbf{n}}$的二进制长度的多项式时间内计算），否则拒绝。若 v_a 对应于输入变量 y，则当 $p = \epsilon$ 且 b 表示类型 $+$时，或当 $p = 1$ 且 b 是计算常数 i 的门时， T_D 接受；所有其他输入均被拒绝。若 v_a 对应于任何其他输入门，则类似地，当 $p = \epsilon$ 且 b 表示 $+$时，或当 $p = 1$ 且 b 是 D中由同一变量标记的输入门时，我们接受。若 v_a 不是输入门且 $p = \epsilon$，则机器 T_D 在输入$(\mathbf{n}\ v_a, p, b)$上模拟T_C，并相应地接受或拒绝。若 $p \neq \epsilon$，则 T_D 检查 b 是否也是 C的 i^{th} 副本中的一个门。若否，则机器拒绝。否则，机器 T_D 在$(\mathbf{n}\ v_a, p, v_b)$上模拟 T_C ，其中 v_b 是 C 中对应于 b的门的名称。

如果 a 反而是电路 V 的一部分，那么我们将改为在适当的输入上模拟 T_V ，以判断 $(\mathbf{n}\ a,\ p,\ b)$ 是否属于 D 的直接连接语言。这同样需要从 a 中提取电路 V 内门的名称；如果 $p \neq \epsilon$，还可能需要对 b 做同样的处理。要求 $d_{\mathbf{n}}$ 的二进制表示能够在关于$\mathbf{n}$ 的二进制表示的多项式时间内写出，这保证了 T_V 的输入可由 T_D 在规定时间内计算出来。

最后，如果 a 是内积子电路的一部分，那么它要么连接到 C 和 V 的副本的输出（对应于标记为 $(5,\ i,\ j)$ 的门），要么连接到内积子电路中的其他门（对应于标记为 $(6,\ i)$ 的门）。在第一种情况下，要判断 b 是否为 a 的前驱，我们可以检查 b 是否是正确子电路的输出门。如果 $a = (5,\ i,\ j)$，那么根据 $p = 1$ 是 2 还是其他值， b 要么是 j^{th} 个 C 副本的输出，要么是范德蒙德矩阵的逆矩阵中的 $(j,\ i)$ 项。后一种情况的处理方式类似。上述描述明确给出了每个门的元数，因此也可以高效地计算出来（如有必要，可通过预言机调用来确定 C 中门的元数）。如果 $C_{\mathbf{n}}$ 有 m 个输入，那么 $D_{\mathbf{n}}$ 有 $m-1$ 个输入，而 $D_{\mathbf{n}}$ 始终有 $d_{\mathbf{n}}+1$ 个输出。最后， $D_{\mathbf{n}}$ 的规模上界可由 $C_{\mathbf{n}}$ 的规模上界、参数 $d_{\mathbf{n}}$ 以及范德蒙德矩阵逆矩阵电路的规模推得，因此很容易计算出这样的上界。 □

我们关于一致性的证明通常会与上面的证明类似：我们将使用先前构造的一致子电路以及一些其他简单机制来构造电路。在所有情况下，直接连接语言都将通过模拟判定这些子电路的直接连接语言的图灵机来判定。因此，后续的证明不会像上面两个关于一致性的证明那样深入底层。

多变量插值的一致性可由引理 3.2 通过克罗内克代换得出。

引理 3.3。 设 $\mathcal{C}=(C_{\mathbf{n}})_{\mathbf{n}}$ 是一个关于 $\mathbb{Q}$ 的多对数时间一致算术电路族，其规模为 $s_{\mathbf{n}}$，深度有常数 Δ上界，且只有一个输出。设 $f_{\mathbf{n}}$ 是由 $C_{\mathbf{n}}$计算出的有理函数，$\mathbf{y}$ 是一个由 $m_{\mathbf{n}}$ 个变量组成的指定集合，并假设每个 $C_{\mathbf{n}}$ 关于$\mathbf{y}$都是无除法的，因此 $f_{\mathbf{n}} \in \mathbb{Q}(\mathbf{x})[\mathbf{y}]$。

设 $d_{\mathbf{n}}$ 是 $f_{\mathbf{n}}$ 关于$\mathbf{y}$的次数上界；对于每个满足 $|\boldsymbol{\alpha}| \le d_{\mathbf{n}}$ 的 $\boldsymbol{\alpha} \in \mathbb{N}^{m_{\mathbf{n}}}$，令$f_{\mathbf{n},\boldsymbol{\alpha}} \in \mathbb{Q}(\mathbf{x})$ 表示 $f_{\mathbf{n}}$ 中$\mathbf{y}^{\boldsymbol{\alpha}}$ 的系数。最后，假设可以在关于$\mathbf{n}$的二进制长度和$\log(d_{\mathbf{n}})$的多项式时间内，根据$\mathbf{n}$ 的二进制表示计算出 $d_{\mathbf{n}}$ 和 $m_{\mathbf{n}}$ 的二进制表示。

那么，存在一个多对数时间一致族 $\mathcal{D}=(D_{\mathbf{n}})_{\mathbf{n}}$，由规模为$\mathrm{poly}(s_{\mathbf{n}}(d_{\mathbf{n}}+1)^{m_{\mathbf{n}}})$、深度至多为 $\Delta + O(1)$ 的、在 $\mathbb{Q}$ 上的算术电路组成，使得 $D_{\mathbf{n}}$ 对所有满足$|\boldsymbol{\alpha}| \le d_{\mathbf{n}}$ 的 $\boldsymbol{\alpha} \in \mathbb{N}^{m_{\mathbf{n}}}$ 都计算 $f_{\mathbf{n},\boldsymbol{\alpha}}$。

证明。 我们使用克罗内克代换。定义 $g_{\mathbf{n}}$ 为

$$g_{\mathbf{n}}(\mathbf{x}, z) := f_{\mathbf{n}}\left(\mathbf{x}, z, z^{d_{\mathbf{n}}+1}, z^{(d_{\mathbf{n}}+1)^2}, \ldots, z^{(d_{\mathbf{n}}+1)^{m_{\mathbf{n}}-1}}\right).$$

多项式 $g_{\mathbf{n}}$ 的次数至多为 $d_{\mathbf{n}} \cdot (d_{\mathbf{n}}+1)^{m_{\mathbf{n}}}$，并且可以由一个规模为 $\mathrm{poly}(s_{\mathbf{n}}, (d_{\mathbf{n}}+1)^{m_{\mathbf{n}}})$、深度为 $\Delta + O(1)$ 的无常数电路计算，方法如下。我们构造一个输入为$\mathbf{x}$ z的电路。使用 $+$ 个门复制 z，以及 $\times$ 个门，我们可以创建计算幂 $z^{(d_{\mathbf{n}}+1)^i}$ 的门，对所有$i \in [m_{\mathbf{n}}-1]$均如此。前驱门的编号将采用自然顺序，与我们在先前的证明中计算幂和阶乘时的方式类似。

接下来，我们复制一份计算 $f_{\mathbf{n}}$ 的电路，将所有输入门改为 $+$ 门，并将它们连接到输入 $\mathbf{x}$ 以及这些 z 的幂。门的命名方式与前面的证明相同：门名称表示该门参与计算 z 的哪个幂，或者表示该门属于计算 $f_{\mathbf{n}}$ 的电路；在后一种情况下，门名称中会包含其在计算 $f_{\mathbf{n}}$ 的电路中对应门的名称。这个计算 $\{g_{\mathbf{n}}\}_{\mathbf{n}}$ 的电路族是多对数时间一致的。对于计算 $f_{\mathbf{n}}$ 的子电路中的门，只需模拟该电路族 $\mathcal{C}$ 对应的图灵机，即可判定直接连接语言。

现在，我们将 引理 3.2 应用于这个电路族（该电路族关于 z 无除法，并且我们可以在关于 $\mathbf{n}$ 和 $m_{\mathbf{n}}\log(d_{\mathbf{n}})$ 的二进制长度的多项式时间内，计算 $d_{\mathbf{n}} \cdot (d_{\mathbf{n}}+1)^{m_{\mathbf{n}}}$ 的二进制表示）。由此得到一个计算 $g_{\mathbf{n}}$ 关于 z 的多项式系数的电路族，这些系数与 $f_{\mathbf{n},\boldsymbol{\alpha}}$ 的系数一一对应。计算 $g_{\mathbf{n}}$ 的系数的电路中的门名称编码了正在计算其系数的 z 的幂。由此很容易计算出每个门正在计算其系数的单项式 $\boldsymbol{\alpha}$：只需将一个数转换为 $d_{\mathbf{n}}+1$ 进制并列出各位数字即可。

□

引理 3.3 使我们能够提取指定变量中每个单项式的系数。在某些应用中，我们需要在将给定多项式视为关于多个不同指定变量的一元多项式时，求出它的系数 y。以下引理表明，这项任务可以一致地完成。

引理 3.4. 设 $\mathcal{C}=(C_{\mathbf{n}})_{\mathbf{n}}$ 是一个规模为 $s_{\mathbf{n}}$、深度有常数 Δ界的、定义在 $\mathbb{Q}$ 上的多对数时间一致算术电路族。设 $C_{\mathbf{n}}$计算的有理函数为 $f_{\mathbf{n}}^{(k)}$，其中 $k \in [m'_{\mathbf{n}}]$，令 $\mathbf{y}$ 为一个由 $m_{\mathbf{n}}$ 个变量组成的指定集合，并假设每个 $C_{\mathbf{n}}$ 关于$\mathbf{y}$都是无除法的，因此每个 $f_{\mathbf{n}}^{(k)}$都属于 $\mathbb{Q}(\mathbf{x})[\mathbf{y}]$。

令 $d_{\mathbf{n}}$ 为 $\mathbf{y}$ 中所有 $f_{\mathbf{n}}^{(k)}$ 的次数上界，并且对于每个 $0 \le i \le d_{\mathbf{n}}$、$j \in [m_{\mathbf{n}}]$ 和 $k \in [m'_{\mathbf{n}}]$，令 $f^{(k)}{}_{\mathbf{n},j,i} \in \mathbb{Q}(\mathbf{x})[y_1, \ldots, y_{j-1}, y_{j+1}, \ldots, y_{m_{\mathbf{n}}}]$，使得

$$f_{\mathbf{n}}^{(k)} = \sum_{i=0}^{d_{\mathbf{n}}} f_{\mathbf{n},j,i}^{(k)} y_j^i.$$

最后，假设可以根据$\mathbf{n}$ 的二进制表示，在关于$\mathbf{n}$的二进制长度和log（$d_{\mathbf{n}}$）的多项式时间内，计算出 $d_{\mathbf{n}}$ 和 $m_{\mathbf{n}}$ 的二进制表示。

于是存在一个多对数时间一致族 $\mathcal{D}=(D_{\mathbf{n}})_{\mathbf{n}}$，由 $\mathbb{Q}$ 上规模为$\mathrm{poly}(s_{\mathbf{n}}, m_{\mathbf{n}}, d_{\mathbf{n}})$、深度为 $\Delta+O(1)$ 的算术电路组成，使得 $D_{\mathbf{n}}$ 计算 $f^{(k)}{}_{\mathbf{n},j,i}$，对所有 $0\le i\le d_{\mathbf{n}}$、 $j\in[m_{\mathbf{n}}]$ 和$k\in[m'_{\mathbf{n}}]$。

证明。 本证明类似于引理 3.2的证明。固定 $C=C_{\mathbf{n}}$， $f=f_{\mathbf{n}}$和 $d=d_{\mathbf{n}}$。我们描述电路 $D=D_{\mathbf{n}}$。

电路 D 有一组名为(1， i)的门，它们是标以常数1的常数门，以及一组 $+$ 个门(2， i)，对 $i\in[d]$ 而言，这些门计算数1，...， $d+1$。前驱节点按显然的方式编号。电路 D 随后有 $m_{\mathbf{n}}$($d_{\mathbf{n}}+1$)个 C的副本，每一对(i， j)（满足 $0\le i\le d_{\mathbf{n}}$ 和 $1\le j\le m_{\mathbf{n}}$）各对应一个。(i， j)th 副本中的门被命名为(3， i， j， v)，其中 v 是 C中相应门的名称。在(i， j)th 这一 C的副本中，标有y_j 的输入门被替换为一个一元求和门，其子节点是门(2， i)，该门计算整数 i。

电路 D 随后包含一个电路 V，它来自 引理 3.1，用于计算范德蒙德矩阵的逆矩阵 $\mathrm{Vand}(1,\ldots,d_{\mathbf{n}}+1)$。这些门命名为 $(4,v)$，其中 v是 V中对应门的名称。接下来，电路 D 包含门 $(5,k,*)$ 和 $(6,k,*)$，用于计算求值结果与矩阵逆的所有必需乘积。同样，前驱节点的编号方式与引理 3.2 的证明中完全相同。引理 3.2。

由上述描述可知， D 的规模和深度满足所声称的界。接下来要说明如何判定 D的直接连接语言。设 (n a,p,b) 是判定该直接连接语言的机器的一个输入。如果 a 的形式为 $(t,*)$，且满足 $t\neq 3$，那么判定它是否为是实例的方法与引理 3.2 的证明完全相同。如果 a 的形式为 $(3,i,j,v)$，且 v 是 C 中的输入门，我们可以利用索引 i,j 确保输入被连接到正确的常数或变量（我们首先检查 $0\le i\le d_{\mathbf{n}}$ 和 $1\le j\le m_{\mathbf{n}}$；根据假设，这一步所需时间关于 n 的二进制长度为多项式）。具体而言，如果输入是 x_t且满足 $t\neq j$，那么该门必须连接到 x_t 本身；否则，如果 $t=j$，输入就连接到计算常数 i 的门。其余计算也与引理 3.2 的证明完全相同。

□

上述插值结果的一个推论是，存在一个计算初等对称多项式的一致电路族。

引理 3.5。 存在一个多对数时间一致族，由定义在 $\mathbb{Q}$ 上的无常数、弱无除法、常数深度算术电路 $\mathcal{C}=(C_n)_n$ 构成，使得 C_n 的规模为 $\mathrm{poly}(n)$，并计算初等对称多项式 $e_1,\ldots,e_n$，其变量为 n。

证明。我们使用 Ben-Or 设计的用于计算初等对称多项式的常数深度电路。存在一个多对数时间一致族 $\mathcal{D}=(D_n)_n$，由定义在 $\mathbb{Q}$ 上的无常数、多项式规模、常数深度电路构成，使得 D_n 有 $n+1$ 个输入 $x_1,\ldots,x_n,t$，并计算 $\prod_{i=1}^{n}(x_i+t)$。事实上， D_n 只需使用 n 个求和门和一个乘积门即可计算这个多项式。 D_n 的次数恰好为 n，且 $\mathcal{D}$ 无除法。因此， $\mathcal{D}$ 满足引理 3.2 中的所有假设，我们可以应用引理 3.2 得到 $\mathcal{C}$。 □

利用 引理 3.5，我们还可以构造一个计算一般 Vandermondematrix 逆的一致电路族。

引理 3.6. 存在一个多对数时间一致族的无常数、常数深度算术电路 $\mathcal{C}=(C_n)_n$，其定义在 $\mathbb{Q}$ 上，使得 C_n 的规模为 $\mathrm{poly}(n)$，并计算矩阵 $\mathrm{Vand}(x_1,\ldots,x_n)$ 的逆矩阵元素。

证明. 该电路使用以下两个事实： $V := \mathrm{Vand}(x_1, \ldots, x_n)$ 的行列式为$\prod_{i<j}(x_i - x_j)$，且该矩阵的逆矩阵元素可以写为

$$V^{-1}_{i,j} = \frac{(-1)^{n-i} e_{n-i}(x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_n)}{\prod_{k \neq j}(x_j - x_k)}.$$

我们现在描述电路 C_n。该电路包含 n 份由引理 3.5构造的、关于 $n-1$ 个变量的初等对称多项式电路。提供给第 j^{th} 份的输入为 x_1，……，x_{j-1}，x_{j+1}，……，x_n。该电路还有 n 个子电路，其中第 j^{th} 个计算$\prod_{k \neq j}(x_j - x_k)$。最后，该电路将这些组合起来，以计算逆的元素。根据上述描述，关于规模和深度的断言是直接的。关于一致性，论证本质上与引理 3.2的证明中的论证相同：必须判定 $\mathcal{C}$ 的直接连接语言的图灵机可以模拟那些判定各组成子电路的直接连接语言的图灵机。注意，计算逆中位置(i, j)处元素的输出门将在其名称中编码(i, j)。

□

4 多元结式

本节讨论结式理论。我们首先介绍多元结式，它是通常结式的推广，适用于多个多变量多项式，用来判断齐次多项式方程组何时有解。随后，我们将讨论如何利用多元结式判断非齐次方程组何时有解。最后，我们将讨论如何利用多元结式计算零维系统的解的个数。

关于多元结式的通俗入门介绍，可参阅 Cox、Little 和 O'Shea [CLO05，第 3]章。关于结式的全面论述，可见 Gelfand、Kapranov 和 Zelevinsky 的著作 [GKZ94]，、Ierardi 和 Kozen 的综述 [IK93]，，或 Jouanolou 的研究 [Jou91]。

4.1 多元结式

两个一元多项式 f，g 的结式是关于 f 和 g 的系数的一个多项式，当且仅当 f 和 g 在基域 $\mathbb{F}$的代数闭包 $\mathbb{F}$ 中有一个公共解时，该多项式才为零。多元结式将这一概念推广开来，并能检测齐次方程组是否有射影解。

本节中，我们固定一个自然数 $n \in \mathbb{N}$ 以及一组自然数$d_0, \ldots, d_n \in \mathbb{N}$。对于 $d \in \mathbb{N}$，我们用 $M_{n,d}$ 表示由$n+1$ 个变量 $x_0, \ldots, x_n$构成的齐次d 次单项式集合。我们令$\mathbf{u} = \{u_{i,\boldsymbol{\alpha}} \mid i \in \{0, \ldots, n\}, \boldsymbol{\alpha} \in M_{n,d}\}$ 为一组变量，它们分别对应于 $n+1$个次数为 $d_0, \ldots, d_n$的齐次多项式的系数。

有了这个记号，我们现在定义多元结式。

定义 4.1（例如参见 [Jou91，命题 2.3]）。 设 $\mathbb{F}$ 为任意一个域。结式 $\mathrm{Res}_{d_0,\ldots,d_n} \in \mathbb{F}[\mathbf{u}]$ 是满足以下条件的唯一多项式。

1. 若 $F_0, \ldots, F_n \in \mathbb{F}[x_0, \ldots, x_n]$ 分别是次数为 $d_0, \ldots, d_n$的齐次多项式，则 $\mathrm{Res}_{d_0,\ldots,d_n}(F_0, \ldots, F_n) = 0$ 当且仅当方程组 $F_0(\mathbf{x}) = \cdots = F_n(\mathbf{x}) = 0$ 在 $\mathbb{P}^n_{\mathbb{F}}$ 中有解。$\mathrm{Res}_{d_0,\ldots,d_n}(F_0, \ldots, F_n)$ 表示 $\mathrm{Res}_{d_0,\ldots,d_n}$ 的取值，其中令$u_{i,\boldsymbol{\alpha}}$ 等于 F_i中单项式 $\mathbf{x}^{\boldsymbol{\alpha}}$ 的系数。

2. 结式$_{d_0,\ldots,d_n}(x_0^{d_0},\ldots,x_n^{d_n}) = 1$.

3. 多项式 $\mathrm{Res}_{d_0,\ldots,d_n}$ 在 $\mathbb{F}[\mathbf{u}]$中不可约。

此外，若分别用 $\mathbb{Q}$ 和 $\mathbb{F}$ 上的结式表示为 $\mathrm{Res}^{\mathbb{Q}}_{d_0,\ldots,d_n}$ 和 $\mathrm{Res}^{\mathbb{F}}_{d_0,\ldots,d_n}$，则前者的系数为整数，而 $\mathrm{Res}^{\mathbb{F}}_{d_0,\ldots,d_n}$ 是 $\mathrm{Res}^{\mathbb{Q}}_{d_0,\ldots,d_n}$ 在自然环同态 $\mathbb{Z}[\mathbf{u}] \to \mathbb{F}[\mathbf{u}]$ 下的像。$\Diamond$

当 n 以及次数 $d_0,\ldots,d_n$ 可由上下文明确得知时，我们将省略下标，并用结式 表示结式 $\mathrm{Res}_{d_0,\ldots,d_n}$。满足定义 4.1 的多项式是否存在并非显而易见。对于关心结式存在性问题的读者，可参阅 Jouanolou [Jou91]。证明中至关重要的是定义 4.1的最后一条陈述：任意域上的结式都是整数上的结式的像。

多元结式是行列式的推广。考虑一组齐次线性形式 $L_0,\ldots,L_n \in \mathbb{F}[x_0,\ldots,x_n]$，由 $L_i(\mathbf{x}) = \sum_{j=0}^n a_{i,j}x_j$ 给出。方程组$L_0(\mathbf{x}) = \cdots = L_n(\mathbf{x}) = 0$ 有非零解，当且仅当

$$\det\begin{pmatrix} a_{0,0} & a_{0,1} & \cdots & a_{0,n} \\ a_{1,0} & a_{1,1} & \cdots & a_{1,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,0} & a_{n,1} & \cdots & a_{n,n} \end{pmatrix} = 0.$$

同样，根据定义 4.1，我们知道，当且仅当 $\mathrm{Res}_{1,\ldots,1}(L_0,\ldots,L_n) = 0$时，该方程组有非零解。这并非巧合：多项式 $\mathrm{Res}_{1,\ldots,1}(\mathbf{u})$ 和 $\det_{n+1}(\mathbf{u})$ 是相同的！

从结式的定义可以清楚地看出，它是关于 $\sum_{i=0}^n \binom{n+d_i}{d_i}$ 个变量的多项式。不那么显而易见的是它的次数，以下引理给出了这一结果。

引理 4.2 (参见，例如， [CLO05，第 3 章，定理 3。1])。 结式 $\mathrm{Res}_{d_0,\ldots,d_n}(\mathbf{u})$ 关于变量 $\{u_{i,\boldsymbol{\alpha}} \mid \boldsymbol{\alpha} \in M_{n,d_i}\}$ 是 $d_0\cdots d_{i-1}d_{i+1}\cdots d_n$ 次齐次的，总次数为 $\sum_{i=0}^n d_0\cdots d_{i-1}d_{i+1}\cdots d_n$。

我们的工作将聚焦于设计计算结式的有界深度、规模为 $d^{\mathrm{poly}(n)}$ 的一致电路。为了设计这类电路，我们将使用结式的非行列式表述，因为已有证明表明，使用有界深度电路计算行列式需要超多项式规模 [LST21；对于24] ，人们猜想无法用准多项式规模的有界深度电路计算。具体而言，我们将使用以下恒等式，即泊松公式。它将结式 $\mathrm{Res}_{d_0,\ldots,d_n}$ 表示为两个项的乘积：一个是较小的结式 $\mathrm{Res}_{d_0,\ldots,d_{n-1}}$，另一个则与 F_n 在 $F_0,\ldots,F_{n-1}$的公共零点处取值有关。泊松公式中对应于 $n=1$ 的特殊情形曾用于设计计算二元结式的常数深度电路 [AW24; BKR+25b]；其多元推广已由 Jeronimo 和 Sabia 使用 [JS07], ，也将是设计多元结式低深度电路的关键。

定理 4.3 （例如，参见 [CLO05，第 3 章，第 3 节，习题 8]）。 设 $F_0,\ldots,F_n \in \mathbb{F}[\mathbf{x}]$ 是次数分别为 $d_0,\ldots,d_n$ 的齐次多项式。对于 $i \in \{0,1,\ldots,n\}$，令

$$\overline{F}_i(\mathbf{x}) \coloneqq F_i(x_0,\ldots,x_{n-1},0)$$
$$f_i(\mathbf{x}) \coloneqq F_i(x_0,\ldots,x_{n-1},1).$$

设 结式$_{d_0,\ldots,d_{n-1}}(F_0,\ldots,\overline{F_{n-1}}) \neq 0$。那么，结式 结式$_{d_0,\ldots,d_n}(F_0,\ldots,F_n)$ 满足恒等式

$$\mathrm{Res}_{d_0,\ldots,d_n}(F_0,\ldots,F_n) = \mathrm{Res}_{d_0,\ldots,d_{n-1}}(\overline{F}_0,\ldots,\overline{F}_{n-1})^{d_n} \cdot \prod_{\boldsymbol{\alpha}\in \mathrm{V}(f_0,\ldots,f_{n-1})} f_n(\boldsymbol{\alpha})^{m(\boldsymbol{\alpha})},$$

其中$\mathrm{V}(f_0,\ldots,f_{n-1}) \subseteq \overline{\mathbb{F}^n}$是 $f_0,\ldots,f_{n-1}$ 在代数闭包$\mathbb{F}^n$ 中的公共零点构成的有限集，而 $m(\boldsymbol{\alpha}) \in \mathbb{N}$ 是 $\boldsymbol{\alpha}$ 在$\mathrm{V}(f_0,\ldots,f_{n-1})$中的重数。

4.2 仿射方程组的可满足性

结式自然地引出一种算法，用于判定系数域的代数闭包中齐次方程组的可满足性。此类方程组包含 $n+1$个方程和 $n+1$个变量，称为方阵系统。给定方程 $F_0(\mathbf{x}) = F_1(\mathbf{x}) = \cdots = F_n(\mathbf{x}) = 0$，我们只需计算结式 Res($F_0,\ldots,F_n$)，并在且仅在 Res($F_0,\ldots,F_n$) $=0$时报告该方程组可满足。对于包含 $F_0 = \cdots = F_m = 0$ 个齐次方程的规模更大的方程组，可以通过对 F_i作 $n+1$ 随机线性组合，将问题化归为方阵情形。以较高概率，所得方阵系统将与原方程组等可满足，因此，计算结式的算法使我们能够判定任意规模的齐次方程组的可满足性。非齐次方程组又该如何处理呢?

求解非齐次方程组的一种自然策略是将该方程组齐次化，并尝试使用结式。该策略对某些仿射系统有效，但并非对所有仿射系统都有效，这取决于齐次化方程的无穷远处行为。利用多元结式研究仿射系统的一种经典方法是广义特征多项式方法，由 Canny [Can90]提出。在此，并非仅仅对仿射系统进行齐次化，而是额外使用扰动以消除无穷远处的退化行为。利用该方法，Ierardi [Ier89a] 得到了从检验仿射系统可满足性到计算系数属于小型多项式环的多项式多元结式的一个干净归约。在本小节中，我们回顾 Ierardi 的归约。我们建议读者参阅 Ierardi 的博士论文（[Ier89b]），以了解支撑该归约及相关构造的相当优美的几何思想。

我们现在引述 Ierardi 从检验仿射系统可满足性到计算多元结式的归约。在下述结果以及本节其余部分中，我们作如下假设:

(A) 域 $\mathbb{F}$ 是 $\mathbb{Q}$、$\mathbb{F}_{p^a}$、$\mathbb{Q}(y_1,\ldots,y_k)$ 或 $\mathbb{F}_{p^a}(y_1,\ldots,y_k)$ 之一

(B) 在后两种情况下，我们的算法所处理的输入，其系数是关于 $\mathbf{y}$ 的多项式。

特别 地，如第2.3节中所述，此类输入的高度始终定义良好 .

命题 4.4 ([Ier89a])。 假设 *(A)* 和 *(B)* 成立，并设 $f_1,\ldots,f_m \in \mathbb{F}[x_1,\ldots,x_n]$ 是次数至多为 d、高度至多为 h 的多项式。假设 $\mathbb{F}$ 的系数子域至少含有 $15nd^n$ 个元素。存在一个多项式时间蒙特卡洛算法，其成功概率为 $2/3$；该算法以 $f_1,\ldots,f_m$ 为输入，并生成一个多项式集合 $G_{i,j} \in \mathbb{F}[t,w,u,x_0,\ldots,x_n]$，满足 $0 \le i \le n$，且 $1 \le j \le n$ 具有以下性质。

- 每个$G_{i,j}$在 $x_0,\ldots,x_n$ 中都是齐次的，次数至多为 d。
- 每个$G_{i,j}$ 的次数在 w 中至多为 n，在 t 和 u中至多为 *1*。
- 每个$G_{i,j}$的高度均至多为 $h\cdot(n\log d)^c$，其中 c为某个通用常数。

- 代数簇$\mathrm{V}(f_1,\ldots,f_m)$非空，当且仅当存在一个 j 使得

$$(\mathrm{TT}_w \,\mathrm{TT}_t \,\mathrm{Res}(G_{0,j},\ldots,G_{n,j}))(0)=0,$$

其中，结式 $\mathrm{Res}(G_{0,j},\ldots,G_{n,j})$ 是通过将 $G_{i,j}$ 视为关于 $\mathbf{x}$的多项式来计算的，其系数属于 $\mathbb{F}(t,w,u)$。

上述归约的证明基本上就是 [Ier89a, §§2–3]的内容。下面我们概述证明，尽管我们会引用一条关于多元结式的技术性结论而不加证明（引理 4.7）。在说明如何利用结式对零维系统中的解进行计数时，这条技术引理也会派上用场。

我们首先定义射影簇的极限集这一概念。

定义 4.5。设 $G_1,\ldots,G_n\in\mathbb{F}[x_0,\ldots,x_n]$ 分别为次数为 $d_1,\ldots,d_n$ 的型。设$V_0:=\mathrm{V}(G_1,\ldots,G_n)$ 为由 $G_1,\ldots,G_n$定义的代数簇。 V_0 的极限集是通过以下过程得到的 V_0 的子簇 V_0^*。

令 t 为一个新变量。定义 $\widehat{G_i}:=G_i+t\cdot x_i^{d_i}$并令 $V:=\mathrm{V}\left(\widehat{G_1},\ldots,\widehat{G_n}\right)\subseteq\mathbb{P}^n\times\mathbb{A}$。令$V^*$ 表示 V 中那些不包含在任意 $\tau\in\mathbb{F}$对应的 $\mathrm{V}(t-\tau)$ 型子空间内的分支的并集。等价地，这些是 V中投影到 $\mathbb{A}$ 后满射的分支。定义 $V_0^*:=V^*\cap\mathrm{V}(t=0)$，并将其视为 $\mathbb{P}^n$中的代数簇。$\diamondsuit$

引理 4.6。对于次数为 $d_1,\ldots,d_n$的任意形式 $G_1,\ldots,G_n\in\mathbb{F}[x_0,\ldots,x_n]$，极限集 V_0^*是 $\mathrm{V}(G_1,\ldots,G_n)$ 的有限子集，且包含其所有孤立点。集合 V_0^* 的规模至多为 $\prod_{i=1}^n d_i$。

证明。第一条陈述的内容见 [Ier89a，引理 2。3]第二条陈述由以下结论推出：$\widehat{\quad}$ $\widehat{\quad}$贝祖不等式（[BCS97，定理 8。28]），将其应用于 G_1、……、G_n：由于 V_0^*是有限集，其基数$\widehat{\quad}$ $\widehat{\quad}$不超过 G_1、……、G_n 视为关于 $\mathbb{F}(t)[x_0,\ldots,x_n]$的多项式时的贝祖数。 □

现在我们引用 Ierardi 的技术引理 [Ier89a]，该引理构造出一个多项式 R_0^*，其因子是与极限集中的点相对应的线性多项式 V_0^*。

引理 4.7 ([Ier89a，引理 2。6])。设 G_1、……、$G_n\in\mathbb{F}[x_0,\ldots,x_n]$ 是次数分别为 d_1、……、d_n的型。设 F_1、……、$F_m\in\mathbb{F}[x_0,\ldots,x_n]$ 是次数为 d的额外齐次形式。定义 $\widehat{G_i}:=G_i+tx_i^{d_i}$。定义 $L\in\mathbb{F}[x_0,\ldots,x_n,u_0,\ldots,u_n,v_1,\ldots,v_m,t]$ 为 $L:=\sum_{i=0}^n u_i x_i^d+\sum_{j=1}^m v_j F_j$。定义

$$R_0^*:=\mathrm{TT}_t\,\mathrm{Res}\left(\widehat{G_1},\ldots,\widehat{G_n},L\right),$$

其中，结式$\mathrm{Res}\left(\widehat{G_1},\ldots,\widehat{G_n},L\right)$ 的计算方法是将 G_i和 L 视为以 $\mathbb{F}(\mathbf{u},\mathbf{v}\ t)$为系数的$\mathbf{x}$多项式。

那么，多项式 $R_0^*\in\mathbb{F}[\mathbf{u},\mathbf{v}]$ 可在 $\mathbb{F}$上分解为线性形式的乘积。对于$\mathrm{V}(G_1,\ldots,G_n)$的极限集中的每个点 $\boldsymbol{\alpha}\in V_0^*$，线性多项式 $\sum_{i=0}^n u_i\alpha_i^d+\sum_{j=1}^m v_j F_j(\boldsymbol{\alpha})$ 都是 R_0^*的一个因子。此外， R_0^* 的每个因子都具有这种结构，其中某个 $\boldsymbol{\alpha}\in V_0^*$对应于它。

上述引理将 U-结式的方法推广到了零维射影系统。根据 引理 4.7，我们可以利用结式来检测仿射方程组的孤立点。

引理 4.8。设 $B \subseteq \mathbb{F} \setminus \{0\}$ 是 $\mathbb{F}$ 的系数子域的一个子集。设 $g_1, \ldots, g_n, f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$ 是次数至多为 d 的多项式。设 $\gamma_1, \ldots, \gamma_m$ 是从 B 中独立均匀随机选取的非零域元素。定义 F_i 和 G_i 分别为多项式 f_i 和 g_i 关于新变量 x_0 的齐次化。定义 $\widehat{G_i} := G_i + t x_i^{\deg g_i}$ 且 $H := u_0 x_0^d + \sum_{i=1}^n w^i x_i^d + \sum_{j=1}^m \gamma_j x_0^{d-\deg F_j} F_j$。定义

$$\beta := \left(\mathrm{TT}_w \, \mathrm{TT}_t \, \mathrm{Res}\left(\widehat{G_1}, \ldots, \widehat{G_n}, H\right)\right)(0),$$

其中，结式结式$\left(\widehat{G_1}, \ldots, \widehat{G_n}, H\right)$是通过将 $\widehat{G_i}$ 和 H 视为关于 $\mathbf{x}$ 的多项式来计算的，其系数属于 $\mathbb{F}(u_0, w, t)$。

以至少 $1 - d^n/|B|$ 的概率，在选择 γ 后，以下结论成立。若 $\beta = 0$，则$\mathrm{V}(f_1, \ldots, f_m, g_1, \ldots, g_n) \neq \varnothing$，特别地$\mathrm{V}(f_1, \ldots, f_m) \neq \varnothing$。反过来，若存在一个孤立点 $\boldsymbol{\alpha}' \in \mathrm{V}(g_1, \ldots, g_n)$ 使得 $\boldsymbol{\alpha}' \in \mathrm{V}(f_1, \ldots, f_m)$，则 $\beta = 0$。

证明。定义 $L := u_0 x_0^d + \sum_{i=1}^n u_i x_i^d + \sum_{j=1}^m v_j x_0^{d-\deg F_j} F_j$，其中 u_i 和 v_j 是变量。令

$$R := \mathrm{Res}\left(\widehat{G_1}, \ldots, \widehat{G_n}, L\right),$$

其中，该结式是将 G_i 和 L 视为以$\mathbf{x}$为变量、系数属于$\mathbb{F}(\mathbf{u}, \mathbf{v}\ t)$的多项式来计算的。设 $R_0^* := \mathrm{TT}_t \, R$，并设 V_0^*为定义 4.5中定义的 G_1，……，G_n的极限集。根据引理 4.7，我们知道 R_0^* 可分解为如下形式的线性形式

$$\sum_{i=0}^n u_i \alpha_i^d + \sum_{j=1}^m v_j \alpha_0^{d-\deg F_j} F_j(\boldsymbol{\alpha}),$$

其中 $\boldsymbol{\alpha} \in V_0^*$是 G_1，……，G_n的极限集中的一个点。如果 R_0^*有一个因子与 v_1，……，v_m无关，那么相应的点 $\boldsymbol{\alpha}$属于 $\mathrm{V}\left(x_0^{d-\deg F_1} F_1, \ldots, x_0^{d-\deg F_m} F_m\right)$。如果该因子还依赖于 u_0，那么我们可以写成 $\boldsymbol{\alpha} = (1, \boldsymbol{\alpha}')$，且点 $\boldsymbol{\alpha}'$属于 $\mathrm{V}(g_1$，……，g_n，f_1，……，$f_m)$。反过来，如果存在一个孤立点 $\boldsymbol{\alpha}' \in \mathrm{V}(g_1$，……，$g_n)$，使得 $\boldsymbol{\alpha}' \in \mathrm{V}(f_1$，……，$f_m)$，那么 $(1$，$\boldsymbol{\alpha}') \in V_0^*$，且 R_0^*中相应的因子将依赖于 u_0，而与 v_1，……，v_m无关。

现在令 r 表示结式

$$\mathrm{Res}\left(\widehat{G_1}, \ldots, \widehat{G_n}, H\right),$$

其中，多项式 G_i和 H被视为关于 $\mathbf{x}$的多项式，其系数属于 $\mathbb{F}(u_0, w, t)$。型 H 由 L 通过将 $u_i \mapsto w^i$ 代入 $i \in [n]$ 、将 $v_j \mapsto \gamma_j$ 代入 $j \in [m]$得到。由于结式是系数的多项式函数，因此我们有 $r = R(t, u_0, w, w^2, \ldots, w^n, \gamma_1, \ldots, \gamma_m)$。在相同的代换下， R_0^* 中与 $\boldsymbol{\alpha} \in V_0^*$对应的因子映射为

$$u_0 \alpha_0^d + \sum_{i=1}^n w^i \alpha_i^d + \sum_{j=1}^m \gamma_j \alpha_0^{d-\deg F_j} F_j(\boldsymbol{\alpha}).$$

R_0^*的每个因子都至少依赖于一个 u_0、……、u_n，因为 $\boldsymbol{\alpha}$是射影空间中的一个点。结合多项式 u_0、w、……、w^n线性无关这一事实可知，在上述代换下， R_0^* 的任何因子都不会映射为零。特别地，在该代换下， R_0^* 非零。这意味着 $\mathrm{TT}_t \, r = R_0^*(u_0$、$w$、$w^2$、……、$w^n$、$\gamma_1$、……、$\gamma_n)$。定义 $r_0^* := \mathrm{TT}_t \, r$。根据定义，我们有 $\beta = (\mathrm{TT}_w \, r_0^*)(0)$。

的任一因子若依赖于$\mathbf{v}$ 中的一个变量，则以至少 $1-1/|B|$的概率 V_0^*的规模至多为 d^n (引理 4.6)，因此， R_0^* 的每个此类因子都会映射为常数项非零的多项式，且概率至少为 $1-d^n/|B|$。我们证明，只要这一事件发生，引理的结论就成立。

因此，假定该事件发生。设 $\beta=0$。这意味着 r_0^* 的某个不被 w 整除的因子具有为零的常数项。根据假设， R_0^* 的每一个依赖于 $\mathbf{v}$ 中某个变量的因子，都会导出 r_0^* 的一个常数项非零的因子，因此必然存在 $\hat{}$ R_0^* 的某个因子 R 不依赖于 $\mathbf{v}$ 中的任何变量。此外，因子 R 依赖于 u_0，因为 r_0^* 的相应因子不能被 w 整除。综合这些条件可知，与 R 对应的 $\hat{}$ 点 $\boldsymbol{\alpha}\in V_0^*\subseteq V(G_1,\ldots,G_n)$ 满足 $\alpha_0\neq 0$，并且对所有 $j\in[m]$ 满足 $F_j(\boldsymbol{\alpha})=0$。这意味着 $\boldsymbol{\alpha}'\in \mathrm{V}(g_1,\ldots,g_n,f_1,\ldots,f_m)$，其中 $\boldsymbol{\alpha}=(1,\boldsymbol{\alpha}')$。因此，如所断言，该集合非空。

反之，假设存在一个孤立点 $\boldsymbol{\alpha}'\in\mathrm{V}(g_1,\ldots,g_n)$，使得 $\boldsymbol{\alpha}'\in\mathrm{V}(f_1,\ldots,f_m)$。因为 $\boldsymbol{\alpha}'$是 $\mathrm{V}(g_1,\ldots,g_n)$ 的一个孤立点，所以我们有 $(1,\boldsymbol{\alpha}')\in V_0^*$，从而存在 R_0^*的一个因子，因而也存在 r_0^*的一个因子，对应于 $(1,\boldsymbol{\alpha}')$。 r_0^* 的相应因子具有如下形式

$$u_0+\sum_{i=1}^{n} w^i\alpha_i^d.$$

该多项式不能被 w 整除，且其常数项为零，因此可得 $\beta=0$，正如所需。

□

借助引理 4.8，我们可以完成命题 4.4的证明。该论证需要以下关于随机超平面截面，以及由给定多项式集合的随机线性组合所定义的簇的标准结果。

引理 4.9. 设 $B\subseteq\mathbb{F}$ 为一个有限集。设 $V\subseteq\mathbb{P}^n$ 为一个维数为 r 、次数为D的射影簇。假设 ℓ 是一个线性形式，其每个系数均独立地从 B中均匀随机选取。则交集 $V\cap\mathrm{V}(\ell)$ 的维数为 $r-1$的概率至少为 $1-D/|B|$。若ℓ_1，……， ℓ_{r+1}是以同样方式选取的线性形式，则 $V\cap\mathrm{V}(\ell_1,\ldots,\ell_{r+1})=\varnothing$ 的概率至少为 $1-(r+1)D/|B|$。

设 $W\subseteq\mathbb{A}^n$ 是维数为 r 、次数为 D的射影簇。假设 ℓ 是一个线性多项式，其每个系数都从 B中独立均匀随机选取。那么，交集 $W\cap\mathrm{V}(\ell)$ 的维数为 $r-1$的概率至少为 $1-2D/|B|$。如果 $\ell_1,\ldots,\ell_{r+1}$是以相同方式选取的线性多项式，那么 $W\cap\mathrm{V}(\ell_1,\ldots,\ell_{r+1})=\varnothing$ 的概率至少为 $1-2(r+1)D/|B|$。

引理 4.10。 设 $B\subseteq\mathbb{F}$ 是一个有限集。设 $f_1,\ldots,f_m\in\mathbb{F}[x_1,\ldots,x_n]$ 是次数至多为 d的多项式。假设 $g_1,\ldots,g_{n+1}$是 $f_1,\ldots,f_m$的线性组合，且每个系数都从 B中独立均匀随机选取。那么，以下结论成立的概率至少为 $1-(n+1)d^n/|B|$。对于每个 $s\in[n+1]$，$\mathrm{V}(g_1,\ldots,g_s)$ 的每个余维数小于 s 的不可约分支，都是$\mathrm{V}(f_1,\ldots,f_m)$的一个分支。因此，$\mathrm{V}(g_1,\ldots,g_{n+1})=\mathrm{V}(f_1,\ldots,f_m)$。射影情形下的类似结果也成立。

引理 4.9 和 引理 4.10 的证明隐含在 Heintz 的方法中 [Hei83]。关于后者的显式证明，参见例如 [KP96，引理 36]。前者基本上可以用相同的论证证明。

命题 *4.4* 的证明。 如果 $\mathbb{F}$ 的系数子域是 $\mathbb{Q}$，令 B 为自然数集合 $\{1,\ldots,15nd^n\}$。如果 $\mathbb{F}$ 的系数子域是有限域，令 B 为该系数子域的非零元素集合。对于固定的 $j\in[n]$，我们按如下方式构造 $G_{0,\,j}$，……， $G_{n,\,j}$。令 $g_{1,\,j}$，……， $g_{j,\,j}$

为 f_1，……，f_m 的随机线性组合，其中系数从 B 中独立且均匀随机选取。令 $g_{j+1,\,j}$，……，$g_{n,\,j}$ 为随机线性多项式，系数从 B 中独立且均匀随机选取。对于 $i \in [n]$，令 $G_{i,\,j}$ 定义为 $G_{i,\,j} := g^h_{i,\,j} + t x_0^{\deg g_i}$，其中 $g^h_{i,\,j}$ 是将 $g_{i,\,j}$ 关于新变量 x_0 齐次化所得。为了构造 $G_{0,\,j}$，我们从 B 中独立且均匀随机选取元素 γ_1，……，γ_m，并令 $G_{0,\,j} := u_0 x_0^d + \sum_{i=1}^n w^i x_i^d + \sum_{k=1}^m \gamma_k$，$x_0^{d-\deg f_k} F_k$，其中 F_k 是将 f_k 关于变量 x_0 齐次化所得。这些多项式具有所声称的次数和高度界。对于每个 j，定义

$$\beta_j := (\mathrm{TT}_w \,\mathrm{TT}_t \,\mathrm{Res}(G_{1,j}, \ldots, G_{n,j}, G_{0,j}))(0).$$

以至少 $1 - nd^n/|B|$ 的概率，引理 4.8 的结论对所有 β_j 成立。在证明的其余部分，我们假定该事件发生。若 $\beta_j = 0$ 对任意 j，则 $\mathrm{V}(f_1, \ldots, f_m) \neq \varnothing$。为完成证明，只需证明：若 $\mathrm{V}(f_1, \ldots, f_m) \neq \varnothing$，则 $\beta_j = 0$ 对某个 j 成立。我们证明这以高概率发生。

为此，令 $s := n - \dim \mathrm{V}(f_1, \ldots, f_m)$。由 引理 4.10，以至少 $1 - 2nd^n/|B|$ 的概率，多项式 $g_{1,s}, \ldots, g_{s,s}$ 定义一个余维数为 s 的等维簇。$\mathrm{V}(f_1, \ldots, f_m)$ 的每个分支都包含在 $\mathrm{V}(g_{1,s}, \ldots, g_{s,s})$ 的某个分支中。特别地，$\mathrm{V}(f_1, \ldots, f_m)$ 的每个极大维数分支都是 $\mathrm{V}(g_{1,s}, \ldots, g_{s,s})$ 的一个分支。

由于$g_{s+1,\,s}$，…… $g_{n,\,s}$ 是系数取自 B的线性多项式，根据引理 4.9，有 t

$$\dim(\mathrm{V}(g_{1,s}, \ldots, g_{s,s}) \cap \mathrm{V}(g_{s+1,s}, \ldots, g_{n,s})) = 0$$

其概率至少为 $1 - 2nd^n/|B|$。特别地，代数簇$\mathrm{V}(g_{1,\,s}$，……，$g_{n,\,s})$ 非空，且每个点都是孤立点。此外，该代数簇包含来自$\mathrm{V}(g_{1,\,s}$，……，$g_{s,\,s})$每个分支的点。根据前面的观察，它包含来自$\mathrm{V}(f_1$，……，$f_m)$的点。引理 4.8的逆向蕴含现在表明 $\beta_s = 0$。利用并集界，我们可推出上述算法成功的概率至少为 $1 - 5nd^n/|B|$，根据 B的规模，可将其下界估计为 $2/3$。

□

4.3 零维系统中的计数

正如我们目前所见，结式是判定多项式方程组可满足性的有用工具，即使在非方阵和仿射情形下也是如此。如果一个方程组可满足，自然的下一步任务是确定该方程组有多少个解。当然，解的空间可能是正维的，这种情况下解有无穷多个。当解集是零维的（因而是一个有限集）时，我们便可以有意义地讨论计数解的个数这一任务。在本小节中，我们将说明，结式对于计算零维方程组的解的个数这一任务同样有用。

我们从较简单的零维射影系统情形开始。

引理 4.11. 假设*(A)*与*(B)*成立，并设 F_1，……，$F_m \in \mathbb{F}[x_1, \ldots, x_n]$ 为次数至多为 d 、高度至多为 h的齐次多项式。假设 $\mathbb{F}$ 的系数子域至少有 $100nd^{2n}$ 个元素。假设$\mathrm{V}(F_1$，……，$F_m)$ 是一个非空有限集。存在一个成功概率为 $2/3$ 的多项式时间蒙特卡罗算法，它以 F_1，……，F_m为输入，并生成两组系数属于 $\mathbb{F}[u]$ 的多项式$G_{0,1}$，……，$G_{n,1}$ 与$G_{0,2}$，……，$G_{n,2}$，且具有以下性质。

- 每个$G_{i,j}$ 关于 x_0，……，x_n 是齐次的，次数至多为 d，且关于 u的次数至多为一。
- 每个 $G_{i,\,j}$ 的高度至多为 $h \cdot (n$对数 $d)^c$，其中通用常数为 c。

- $\mathrm{V}(F_1, \ldots, F_m)$ 的规模恰好等于在 $\mathbb{F}$ 中的不同根的数量：

$$\gcd(\mathrm{Res}(G_{0,1}, \ldots, G_{n,1}), \mathrm{Res}(G_{0,2}, \ldots, G_{n,2})),$$

其中，将 $G_{i,j}$ 视为以 $\mathbb{F}(u)$为系数的关于 $\mathbf{x}$ 的多项式来计算这些结式。

证明。如果 $\mathbb{F}$的系数子域是 $\mathbb{Q}$，令 B为自然数集合 $\{1, \ldots, 100nd^{2n}\}$。如果 $\mathbb{F}$的系数子域是有限域，令 B 为该系数子域的非零元素集合。我们使用以下多项式

$$\left\{x_j^{d-\deg F_i} \cdot F_i \mid i \in [m], j \in \{0, 1, \ldots, n\}\right\}$$

代替原多项式，因为这样不会改变零点集，同时能确保方程组中的所有多项式次数相同。在证明的其余部分，我们继续用$F_1, \ldots, F_m$指代这个新的多项式集合。

令 $V := \mathrm{V}(F_1, \ldots, F_m)$为 $F_1, \ldots, F_m$的零点集。根据贝祖不等式（[BCS97，定理 8.28]），其中至多包含 d^n 个点。我们对坐标进行随机变换，确保 中的所有点都落在图 上。具体做法是将每个 替换为 $,_j x_j$，其中 $\gamma_{i,j}$ 从 B 中独立且均匀随机地选取。经过此线性变换后， V 中的点落在 $x_0 = 1$ 上的概率至少为 $1 - d^n/|B|$。

令 $G_{1,1}, \ldots, G_{n,1}$ 为方程 $F_1, \ldots, F_m$ 的一组随机线性组合，其中每个系数都从 B 中独立且均匀地选取。根据引理 4.10，以至少 $1 - 2nd^n/|B|$ 的概率，零点集 $V_1 := \mathrm{V}(G_{1,1}, \ldots, G_{n,1})$ 是有限集，且包含 V 作为子集。方程组 $F_1|_{x_0=0} = \cdots = F_m|_{x_0=0} = 0$ 不可满足。方程组 $G_{1,1}|_{x_0=0} = \cdots = G_{n,1}|_{x_0=0} = 0$ 由 $F_i|_{x_0=0}$ 的随机线性组合构成，因此根据引理 4.10，该方程组以至少 $1 - 2nd^n/|B|$ 的概率没有根。等价地，以此概率， V_1 中的每个点都位于图 $x_0 = 1$ 上。

类似地，令 $G_{1,2}$，……，$G_{n,2}$ 为 F_1，……，F_m 的一组随机线性组合，并令 V_2 为它们的零点集。它同样是一个有限集，包含 V，且位于图 $x_0 = 1$上。此外，我们声称，若 V_1 是一个有限集，则 $V_1 \cap V_2 = V$成立的概率至少为 $1 - d^n/|B|$。若 $\boldsymbol{\alpha} \in V_1 \setminus V$是一个点，则存在某个 F_j，使得 $F_j(\boldsymbol{\alpha}) \neq 0$，因此以至少 $1 - 1/|B|$的概率，有 $G_{1,2}(\boldsymbol{\alpha}) \neq 0$。 V_1 是有限集这一事实意味着 $|V_1| \leq d^n$，因此由并集界可得 $V_1 \cap V_2 = V$成立的概率满足所声称的下界。

现在，我们独立且均匀地抽取 β_1，……，$\beta_n \in B$，并定义 $L := x_0 + \beta_1 u x_1 + \beta_2 u x_2 + \cdots + \beta_n u x_n$。根据泊松公式（定理 4.3），结式 $\mathrm{Res}(G_{1,1}, \ldots, G_{n,1}, L)$ 可分解为

$$\mathrm{Res}(G_{1,1}, \ldots, G_{n,1}, L) = c \cdot \prod_{\boldsymbol{\alpha} \in V_1} L(\boldsymbol{\alpha})^{m_{\boldsymbol{\alpha}}},$$

其中， $m_{\boldsymbol{\alpha}}$ 是 V_1 和 $c \in \mathbb{F} \setminus \{0\}$中 $\boldsymbol{\alpha}$ 的重数。化简后，并利用所有根都位于仿射图 $x_0 = 1$上的事实，我们得到

$$\mathrm{Res}(G_{1,1}, \ldots, G_{n,1}, L) = c \cdot \prod_{\boldsymbol{\alpha} \in V_1} \left(1 + u \sum_{i=1}^{n} \beta_i \alpha_i\right)^{m_{\boldsymbol{\alpha}}}.$$

由于 β_i 是随机选取的，和 $\sum_{i=1}^{n} \beta_i \alpha_i$ 对不同的根取不同值的概率至少为 $1 - d^{2n}/|B|$。类似地，我们有

$$\mathrm{Res}(G_{1,2}, \ldots, G_{n,2}, L) = c' \cdot \prod_{\boldsymbol{\alpha} \in V_2} \left(1 + u \sum_{i=1}^{n} \beta_i \alpha_i\right)^{n_{\boldsymbol{\alpha}}},$$

其中 $n_{\boldsymbol{\alpha}}$ 是 V_2 中 $\boldsymbol{\alpha}$ 的重数，且 $c' \in \mathbb{F} \setminus \{0\}$。现在很明显，如果我们取这两个结式的最大公因式，那么该最大公因式在 $\mathbb{F}$ 中的不同根的数量就等于 $V_1 \cap V_2 = V$ 中的不同点的数量。因此，令 $G_{0,1} = G_{0,2} = L$，并使用并集界来控制所有所需事件的概率，即可完成证明。

□

现在我们给出主要归约，说明如何利用结式计算零维仿射系统的解的数量。其思路类似于引理 4.11 中的思路。我们将对给定方程组取随机线性组合，将问题归约为变量和多项式数量相同的情形。在这里，我们必须使用广义特征多项式，而不是结式本身，来计算这些随机方程组的零点集的规模。

命题 4.12。假设 *(A)* 和 *(B)* 成立，并设 $f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$ 是次数至多为 d 且高度至多为 h 的多项式。假设 $\mathbb{F}$ 的系数子域至少含有 $100nd^{2n}$ 个元素。假设 $\mathrm{V}(f_1, \ldots, f_m)$ 是有限非空集合。存在一个成功概率为 $2/3$ 的多项式时间蒙特卡洛算法，该算法以 $f_1, \ldots, f_m$ 作为输入，并生成两组多项式 $G_{0,1}, \ldots, G_{n,1}$ 和 $G_{0,2}, \ldots, G_{n,2}$，其系数属于 $\mathbb{F}[u,t]$，并具有以下性质。

- 每个 $G_{i,j}$ 都是关于 $x_0, \ldots, x_n$ 的齐次多项式，次数至多为 d，并且关于 u 和 t 的次数至多为 *1*。
- 每个 $G_{i,j}$ 的高度至多为 $h \cdot (n \log d)^c$，其中 c 是一个通用常数。
- $\mathrm{V}(f_1, \ldots, f_m)$ 的规模恰好等于下列多项式在 $\mathbb{F}$ 中的不同根的个数：

$$\gcd(\mathrm{TP}_u \, \mathrm{TT}_t \, \mathrm{Res}(G_{0,1}, G_{1,1}, \ldots, G_{n,1}), \mathrm{TP}_u \, \mathrm{TT}_t \, \mathrm{Res}(G_{0,2}, G_{1,2}, \ldots, G_{n,2})),$$

其中，计算这些结式时，将 $G_{i,j}$ 视为关于 $\mathbf{x}$ 的多项式，其系数属于 $\mathbb{F}(t,u)$。

证明。若 $\mathbb{F}$ 的系数子域为 $\mathbb{Q}$，令 B 为自然数集合 $\{1, \ldots, 100nd^{2n}\}$。若 $\mathbb{F}$ 的系数子域是有限域，令 B 为该系数子域的非零元素集合。定义 $V := \mathrm{V}(f_1, \ldots, f_m)$。令 $g_{1,1}, \ldots, g_{n,1}$ 和 $g_{1,2}, \ldots, g_{n,2}$ 为 $f_1, \ldots, f_m$ 的两组随机线性组合，系数从 B 中选取。令 $V_1 := \mathrm{V}(g_{1,1}, \ldots, g_{n,1})$，并令 $V_2 := \mathrm{V}(g_{1,2}, \ldots, g_{n,2})$。根据贝祖不等式和引理 4.10，以至少 $1 - 6nd^n/|B|$ 的概率，零点集 V_1 和 V_2 是有限集，并满足 $V_1 \cap V_2 = V$（详情参见引理 4.11 的证明）。

现在定义 $G_{i,j} := g_{i,j}^h + t \cdot x_i^{d_i}$，其中 d_i 是 $g_{i,j}$ 的次数，而 $g_{i,j}^h$ 是相对于新变量 x_0 对 $g_{i,j}$ 进行齐次化得到的结果。最后，定义 $L := x_0 + \beta_1 u x_1 + \cdots + \beta_n u x_n$，其中 $\beta_1, \ldots, \beta_n$ 是从 B 中独立均匀随机抽取的。现在考虑

$$(R_1)_0^* := \mathrm{TT}_t \, \mathrm{Res}(G_{1,1}, \ldots, G_{n,1}, L).$$

根据引理 4.7，我们可以推知，$(R_1)_0^*$ 可分解为线性形式的乘积，极限集合 $(V_1)_0^*$ 中的每个点对应一个线性形式。V_1 中的每个点都属于这个集合，而且，这些也是 $(V_1)_0^*$ 中位于图 $x_0 = 1$ 上的唯一点。对应于超平面 $x_0 = 0$ 上 $(V_1)_0^*$ 中的点的其余因子就是多项式 u。因此，若考虑 $\mathrm{TP}_u(R_1)_0^*$，则每个因子都具有某个 $\boldsymbol{\alpha} \in V_1$ 的 $(1 + u \sum_{i=1}^n \beta_i \alpha_i)$ 形式，而且对每个 $\boldsymbol{\alpha} \in V_1$，都存在一个这种形式的因子。注意，我们并未对重数作出任何断言。以至少 $1 - d^{2n}/|B|$ 的概率，对应于每个点的 u 系数，即 $\sum_{i=1}^n \beta_i \alpha_i$，彼此不同。我们可以对 $g_{1,2}, \ldots, g_{n,2}$ 执行相同操作。那么，$\gcd(\mathrm{TP}_u(R_1)_0^*, \mathrm{TP}_u(R_2)_0^*)$ 在 $\mathbb{F}$ 中的不同根的数量，显然就是 $V_1 \cap V_2$ 的规模；对 $\beta_1, \ldots, \beta_n$ 的选择而言，这一结论以至少 $1 - 2d^{2n}/|B|$ 的概率成立。因此，令 $G_{0,1} = G_{0,2} = L$ 即可完成证明。

□

5 用于结式的常数深度电路

本节将为多元结式 $\mathrm{Res}_{d_0,\ldots,d_n}$设计一个多对数时间一致的常数深度算术电路族。我们的电路将由 $n, d_0, \ldots, d_n$索引，基域为 $\mathbb{Q}$。下一小节将介绍一些记号，并解释我们构造的总体思路。后续小节将给出具体细节。

5.1 记号与证明概述

设 n 为一个正整数，并设 d_0、...、d_n 为正整数。令 $\mathbf{u}0$、...、$\mathbf{u}_n$ 为 $n+1$ 个变量集合，其中对于所有满足 $|\boldsymbol{\alpha}| = d_i$ 的多重指标 $\boldsymbol{\alpha} =$（α_0、...、α_n），都有 $\mathbf{u}_i = (u_{i,\boldsymbol{\alpha}})$。换言之，$\mathbf{u}_i$ 中的每个变量分别对应于由 $n+1$ 个变量构成的、次数为 d_i 的每个单项式。我们用 U 表示这些变量集合的规模之和，因此 $U = \sum_{i=0}^{n} \binom{n+d_i}{d_i}$。我们用 S 表示多项式环 $\mathbb{Q}[\mathbf{u}0、...、\mathbf{u}_n]$，并将其分式域记为 $\mathbb{K}$，其中 S。回顾一下，多元结式（第4.1节）是环 S 中具有整数系数的一个元素。

对于 $j = 0, \ldots, n$，我们将多项式 $F_j \in S[\mathbf{x}]$ 定义为

$$F_j = \sum_{\boldsymbol{\alpha} \in \mathbf{u}_j} u_{j,\boldsymbol{\alpha}} x_0^{\alpha_0} \cdots x_n^{\alpha_n}.$$

任意一组次数为 $P_0, \ldots, P_n$ 的形式 $d_0, \ldots, d_n$ 都可以通过特化 $F_0, \ldots, F_n$得到。我们希望使用泊松公式（定理 4.3）计算多元结式。该公式指出，以下恒等式成立。

$$\mathrm{Res}_{d_0,\ldots,d_n}(F_0, \ldots, F_n) = \mathrm{Res}_{d_0,\ldots,d_{n-1}}(\overline{F}_0, \ldots, \overline{F}_{n-1})^{d_n} \cdot \prod_{\boldsymbol{\alpha} \in \mathrm{V}(f_0,\ldots,f_{n-1})} f_n(\boldsymbol{\alpha})^{m(\boldsymbol{\alpha})},$$

其中 $\overline{F_j} = F_j|_{x_n=0}$ 与 $f_j = F_j|_{x_n=1}$。我们将递归地应用该公式计算第一项，因此需要研究每个 i 对应的多项式 $F_j|_{x_{i+1}=0,\ldots,x_n=0}$ 与 $F_j|_{x_i=1,x_{i+1}=0,\ldots,x_n=0}$。为了便于引用，我们为这些多项式及一些相关对象命名。

对于任意 $i, j \in \{0, 1, \ldots, n\}$，我们用 $\mathbf{u}_{i,j} \subseteq \mathbf{u}_i$ 表示那些满足 $\alpha_{j+1} = \cdots = \alpha_n = 0$ 的变量 $u_{i,\boldsymbol{\alpha}}$。换言之，这些变量 $\mathbf{u}_{i,j}$ 对应于仅依赖于 $x_0, \ldots, x_j$ 的单项式。我们将$F_{i,j}$ 记为多项式

$$F_{i,j} = \sum_{\boldsymbol{\alpha} \in \mathbf{u}_{i,j}} u_{i,\boldsymbol{\alpha}} x_0^{\alpha_0} \cdots x_n^{\alpha_n}.$$

多项式 $F_{i,j}$ 是变量 $x_0, \ldots, x_j$ 的一般次数为 d_i 的形式。我们用 $f_{i,j}$ 表示特化 $F_{i,j}(x_0, \ldots, x_{j-1}, 1)$。

令 $\mathbf{F}^j$ 表示多项式向量 $(F_{0,j}, \ldots, F_{j,j})$。这是由 $j+1$ 个变量上的 $j+1$ 个一般多项式组成的向量，其次数为 $d_0, \ldots, d_j$。我们用 U_j 表示该方程组中的系数个数，因此 $U_j = \sum_{i=0}^{j} \binom{d_i+j}{j}$。

令 $\mathrm{Res}_j \in \mathbb{Q}[\mathbf{u}_{0,j}, \ldots, \mathbf{u}_{j,j}]$ 表示结式 $\mathrm{Res}_{d_0,\ldots,d_j}((F_{0,j}, \ldots, F_{j,j}))$（次数 $d_0, \ldots, d_j$ 始终固定）。多项式 Res_j 取决于次数 $d_0, \ldots, d_j$，但为避免冗长，我们在记号中省略这些次数。给定一组次数为 $d_0, \ldots, d_j$ 的形式 $P_0, \ldots, P_j \in \mathbb{Q}[x_0, \ldots, x_j]$，我们用 $\mathrm{Res}_j(\mathbf{P})$ 表示将 Res_j 在 $P_0, \ldots, P_j$ 的系数处取值。

在上述记号中，泊松公式的第二项涉及多项式$f_{0,\ n}$.....，$f_{n-1,\ n}$的根。这些根位于 $\mathbb{K}$的代数闭包中。然而，要描述 $\mathbb{K}$中的元素并对其进行算术运算，在计算上都很困难。因此，我们将改为处理位于幂级数环中的根。这些根更容易操作，因为我们通常只需将它们计算到某个有限精度。

$f_{0,\,n}$……，$f_{n-1,\,n}$的根无法在环 $\mathbb{Q}[\![\mathbf{u}_0$……，$\mathbf{u}_n]\!]$中表示为幂级数。即使在 $n=1$且 $d_0=2$的情形下，这一点也显而易见。在这种情况下，我们要讨论一般双变量多项式$u_{0,\,(2,0)}x_0^2+u_{0,\,(1,1)}x_0+u_{0,\,(0,2)}$的根。根的表达式涉及判别式$u_{0,\,(1,1)}^2-4u_{0,\,(2,0)}u_{0,\,(0,2)}$的平方根，但该元素在环 $\mathbb{Q}[\![\mathbf{u}_0$……，$\mathbf{u}_n]\!]$中不是平方。

我们将转而利用同伦求$f_{0,n},\ldots,f_{n-1,n}$的幂级数根。我们引入一个新变量 t，并对每个 $i=0,\ldots,n$ 定义多项式

$$H_{i,n}:=(1-t)G_{i,n}+tF_{i,n},$$

其中$G_{i,\,n}\in\mathbb{Q}[x_0,\ldots,x_n]$ 尚待定义。我们有$H_{i,\,n}|_{t=1}=F_{i,\,n}$，以及$H_{i,\,n}|_{t=0}=G_{i,\,n}$。多项式$H_{0,\,n}$、……、$H_{n,\,n}$定义了$F_{0,\,n}$、……、$F_{n,\,n}$的根与$G_{0,\,n}$、……、$G_{n,\,n}$的根之间的一个同伦。由多项式$G_{0,\,n}$、……、$G_{n,\,n}$所定义的方程组称为该同伦的初始系统。我们定义$h_{i,\,n}:=H_{i,\,n}|_{x_n=1}$ 以及$g_{i,\,n}:=G_i|_{x_n=1}$。形式$G_{i,\,n}$ 将被选取，使得方程$g_{0,\,n}$、……、$g_{n-1,\,n}$的根可由无常数均匀常数深度电路轻松计算。我们还将确保该方程组的所有根都是单根，并且每个根处的雅可比矩阵也可由此类电路计算。

根 $g_{0,\,n}$、……、$g_{n-1,\,n}$的简单性所带来的一个结果是，$h_{0,\,n}$、……、$h_{n-1,\,n}$在 t中存在幂级数根，其常数项恰好是 $g_{0,\,n}$、……、$g_{n-1,\,n}$的根。亨泽尔提升和牛顿迭代给出了这些根存在性的构造性证明。事实上，具有线性收敛速度的牛顿迭代给出了上述方程组在 $S[\![t]\!]$中存在根的构造性证明，也就是说，这些根是关于一个变量的幂级数，其系数是其余变量的多项式。尽管牛顿迭代和亨泽尔提升给出了构造性证明，但遵循任一构造过程，只能得到这些根的多对数深度一致电路。这不足以满足我们的应用需求。因此，我们将改用显式隐函数定理来计算这些根（[AY83，命题 20。3]）。

更一般地，为了处理泊松公式中的递归项，我们通过分别特化 $G_{0,\,n}$、……、$G_{n,\,n}$ 和 $H_{0,\,n}$、……、$H_{n,\,n}$，定义多项式$G_{i,j},H_{i,j}$，对所有 $1\le j\le n$ 和 $0\le i\le j$ 均如此。在每种情况下，$G_{0,\,j}$、……、$G_{j,\,j}$ 将是 $H_{0,\,j}$、……、$H_{j,\,j}$ 的初始方程组。我们将应用泊松公式以及上述关于根的显式公式，计算 $H_{0,\,n}$、……、$H_{n,\,n}$ 的结式。这项计算将在 $S[\![t]\!]$ 中进行，精度达到某一指定值。选取这一精度时，将确保截断并令 $t=1$ 后，我们能够恢复 $\mathrm{Res}_n(\mathrm{F}_n)$。

下一小节将介绍初始系统，并说明其根以及在这些根处求值的雅可比矩阵均可由一致常数深度电路计算。再下一小节将完成上述讨论的其余部分。

我们指出，[JS07] 中的算法已将同伦技术与泊松公式结合起来计算结式。该文中的同伦使用了与上文提到的多项式 $g_{i,j}$ 具有类似结构的起始系统，但绕过了引入新变量 t这一步。若令 $\boldsymbol{\nu}_0,\ldots,\boldsymbol{\nu}_j$ 为这些多项式的系数，其算法便使用牛顿迭代生成一个直线程序，用于计算 $f_{0,j},\ldots,f_{j-1,j}$ 在 $\mathbb{Q}[[\mathbf{u}_0-\boldsymbol{\nu}_0,\ldots,\mathbf{u}_{j-1}-\boldsymbol{\nu}_{j-1}]]$中的根的有理函数近似值，再将这些近似值代入乘积公式，并消去除法。[AY83] 中的显式隐函数定理也适用于 [JS07], 中的同伦，但在此语境下会导致规模为双指数的电路。

5.2 初始系统

现在我们来描述初始方程组，也就是多项式 $G_{i,\,j}$。以下构造出自 [HJSS02]（[MSW95]中也简要提及了该构造），适用于更一般的多齐次方程组情形。

定义 5.1（初始方程组）。对于任意整数 m 以及 $j \in \{0, 1, \ldots, n\}$，我们定义线性形式$L_{j,\ m}$ 如下：

$$L_{j,m}(\mathbf{x}) \coloneqq x_0 + mx_1 + \cdots + m^{j-1}x_{j-1} + m^j x_j.$$

我们用 $\ell_{j,m}$ 表示 $L_{j,m}$ 在 $x_j = 1$处的特化。

定义整数子集 $A_0, \ldots, A_n$为 $A_0 \coloneqq \{1, \ldots, d_0\}$, $A_1 \coloneqq \{d_0 + 1, \ldots, d_0 + d_1\}$，依此类推。集合 A_i的规模为 d_i，并且这些集合两两不相交。对于 $i \in \{0, 1, \ldots, n\}$，我们将形式 $G_{i,j} \in \mathbb{Q}[\mathbf{x}]$ 定义为

$$G_{i,j}(\mathbf{x}) \coloneqq \prod_{k \in A_i} L_{j,k}(\mathbf{x}).$$

我们用 $\mathbf{G}^j$表示多项式向量 $(G_{0,j}, \ldots, G_{j,j})$。最后，$g_{i,j}$表示 $G_{i,j}$在 $x_j = 1$处的特化，而 $\mathbf{g}^j$表示多项式向量 $(g_{0,j}, \ldots, g_{j-1,j})$。$\diamondsuit$

注意，每个$G_{i,j}$都是关于变量 $x_0, \ldots, x_j$的次数为 d_i的形式。我们用$\mathbf{g}^j$表示 $g_{0,j}, \ldots, g_{j-1,j}$（而不是更自然的选择 $g_{0,j}, \ldots, g_{j,j}$）的原因是，将泊松公式应用于 $H_{0,j}, \ldots, H_{j,j}$时，与根的乘积对应的项只涉及求解方程组 $H_{0,j}|_{x_j=1}, \ldots, H_{j-1,j}|_{x_j=1}$。

下面的引理概括了关于方程组$\mathbf{g}^j$的零点的一些基本性质。定义$e_0 \coloneqq 0$。对于 $i = 1, \ldots, n$，定义 $e_i \coloneqq d_0 + \cdots + d_{i-1}$。

引理 5.2。对于每个 $j \in \{0, 1, \ldots, n\}$，令 $B_j \coloneqq [d_0] \times [d_1] \times \cdots \times [d_{j-1}]$。对于每个 $\mathbf{c} \in B_j$，线性方程组 $\ell_{j,c_0} = \ell_{j,e_1+c_1} = \cdots = \ell_{j,e_{j-1}+c_{j-1}} = 0$有唯一的公共解，记作 $\mathbf{r_c}$。所有这样的$\mathbf{r_c}$ 恰好构成$\mathbf{g}^j$的公共零点集合。

证明。对于$\mathbf{c}$的每种取值，与该线性方程组对应的矩阵都是范德蒙矩阵，因此可逆。这说明存在唯一解。此外，对于任意固定的$\mathbf{c}$，如果 ℓ 是形如 $\ell_{j,m}$ 的线性形式，其中 m 不属于 $e_0 + c_0, \ldots, e_{j-1} + c_{j-1}$，那么线性方程组

$$\ell, \ell_{j,e_0+c_0}, \ldots, \ell_{j,e_{j-1}+c_{j-1}}$$

不可满足。对此，将方程组齐次化，并注意到对应的矩阵仍是范德蒙矩阵，因此零向量是唯一的解。这两个事实还表明，$\mathbf{g}^j$ 的公共零点恰好是$\mathbf{r_c}$。

□

接下来，我们计算$\mathbf{g}^j$ 在其每个解$\mathbf{r_c}$处的雅可比矩阵。

引理 5.3。沿用 引理 5.2中的定义。对于$\mathbf{c} \in B_j$和 $i \le j$，定义$\kappa_{\mathbf{c},\ i}$ 为

$$\kappa_{\mathbf{c},i} \coloneqq \frac{g_{i,j}}{\ell_{j,e_i+c_i}}(\mathbf{r_c}).$$

$\mathbf{g}^j$ 在$\mathbf{r_c}$处的雅可比矩阵记为 $\mathcal{J}_\mathbf{c}$，它是可逆矩阵，并可分解为

$$\mathcal{J}_\mathbf{c} = \operatorname{diag}(\kappa_{\mathbf{c},0}, \ldots, \kappa_{\mathbf{c},j-1}) \cdot \operatorname{Vand}(e_0 + c_0, \ldots, e_{j-1} + c_{j-1}).$$

证明。关于 x_a 的$g_{i,\ j}$ 的偏导数为

$$\partial_a g_{i,j}(\mathbf{x}) = \sum_{k'=1}^{d_i} \prod_{k \neq k'} \ell_{j,e_i+k}(\mathbf{x}) \cdot \partial_a \ell_{j,e_i+k'}(\mathbf{x}) = \sum_{k'=1}^{d_i} \prod_{k \neq k'} \ell_{j,e_i+k}(\mathbf{x}) \cdot \left(e_i + k'\right)^a.$$

在$\mathbf{r_c}$处求值时，上述求和中只有省略了ℓ_{j,e_i+c_i}的那一项不为零，因为ℓ_{j,e_i+c_i} 在$\mathbf{r_c}$处为零。在这一项中，第一个乘积项在以下位置求值时

$\mathbf{r_c}$ 恰好等于$\kappa_{\mathbf{c},i}$。这证明了所述的雅可比矩阵因式分解。证明引理 5.2表明$\kappa_{\mathbf{c},i}$ 均不为零，因为$\mathbf{r_c}$ 不是任何一个作为$g_{i,j}$因子的线性多项式的根，除了ℓ_{j,e_i+c_i}。雅可比矩阵可逆这一事实现在由因式分解得出。□

对于每个 j，解 $\mathbf{r_c}$、雅可比矩阵 $\mathcal{J}_{\mathbf{c}}$ 及其逆 $\mathcal{J}_{\mathbf{c}}^{-1}$ 都是 $\mathbf{c}$ 的有理函数。下面的引理描述了多对数时间一致、无常数、常深度电路：这些电路以 $\mathbf{c}$ 作为输入，并计算出这些有理函数。

引理 5.4。存在一个多对数时间一致的无常数电路族 $\mathcal{C}^{\text{init}}$，其索引为 j、d_0.....d_{j-1}，并具有以下性质。

- 电路 $C_{\text{init}j、d_0.....d_{j-1}}$ 的规模关于 $j + d_0 + \cdots + d_{j-1}$ 为多项式，且深度由一个通用常数界定。
- 电路 $C_{\text{init}j、d_0.....d_{j-1}}$具有 j 个输入门，其标签为变量 z_0.....z_{j-1}。该电路具有 $j + 2j^2$ 个输出门。
- 在输入 $(c_0、\ .....、\ c_{j-1}) \in [d_0] \times \cdots \times [d_{j-1}]$ 时，该电路计算 $\mathbf{r_c}$、雅可比矩阵的元素 $\mathcal{J}_{\mathbf{c}}$，以及其逆 $\mathcal{J}^{-1}{}_{\mathbf{c}}$ 的元素。

证明。我们首先描述电路 $C = C^{\text{init}}_{j\ d_0,\ ,...,d_{j-1}}$。回顾，$e_k$ 表示和 $d_0 + \cdots + d_{k-1}$。电路 C 包含一些门，通过反复加上常数 1 来计算从 1 到 e_j 的所有整数。它有 $+$ 个门，通过将 z_j 加到整数 e_{j-1} 上来计算多项式 $e_0 + z_0, \ldots, e_{j-1} + z_{j-1}$。该电路包含一些门，用于计算多项式 $-(e_0 + z_0)^j, \ldots, -(e_{j-1} + z_{j-1})^j$。这需要引入更多副本的门来计算 $e_0 + z_0$。这些计算所用的门将命名为 $(1, *)$，其中 $*$ 本身是一个元组；这种命名方式类似于引理 3.1 的证明中对执行类似任务的门的命名。该电路包含一个子电路C' 的副本，用于求规模为 $j \times j$ 的一般范德蒙矩阵的逆矩阵（引理 3.6）；其输入连接到计算上述多项式的门。这些门将命名为 $(2, v)$，其中 v 是电路 C' 中该门的名称。该子电路的输出计算范德蒙矩阵 $\text{Vand}(e_0 + z_0, \ldots, e_{j-1} + z_{j-1})$ 的逆矩阵。随后，电路将该范德蒙矩阵的逆矩阵与向量 $(-(e_0 + z_0)^j, \ldots, -(e_{j-1} + z_{j-1})^j)$ 相乘。将所得向量的元素记为 $\mathbf{r_z}$。这些门将命名为 $(3, *)$。

Next 对于每个 $i \in \{0, \ldots, j-1\}$，电路都有一些门来计算多项式 s

$$\sum_{k'=1}^{d_i} \prod_{k \neq k'} \ell_{j,e_i+k}(x_0, \ldots, x_{j-1}),$$

并在$\mathbf{r_z}$处对它们求值。将这些求值记为 $\kappa_{\mathbf{z},\ i}$，相应的门将命名为 $(4,\ *)$。然后，电路还有一些门来计算矩阵乘积

$$\mathcal{J}_{\mathbf{z}} \coloneqq \text{diag}(\kappa_{\mathbf{z},1}, \ldots, \kappa_{\mathbf{z},j-1}) \cdot \text{Vand}(e_0 + z_0, \ldots, e_{j-1} + z_{j-1})$$

最后，电路利用上述因式分解以及先前计算出的 $\text{Vand}(e_0 + z_0,\ \ldots,\ e_{j-1} + z_{j-1})^{-1}$ 的元素，来计算 $\mathcal{J}_{\mathbf{z}}$ 的逆。这些门也可以按上述方式命名。在所有情况下，每个门的前驱自然编号都可以从描述中清楚地看出。

我们论证，在 $\mathbf{c}$ 上对该电路求值能够正确地计算出根 $\mathbf{r_c}$、雅可比矩阵 $\mathcal{J}_{\mathbf{c}}$ 及其逆。由 $\mathbf{r_c}$ 的定义可知 $\mathbf{r_z(c)} = \mathbf{r_c}$。为看出 $\kappa_{\mathbf{z},i}$(c)= $\kappa_{\mathbf{c},i}$，我们观察到，在 $\mathbf{r_c}$ 处求值时，$\kappa_{\mathbf{z},i}$ 的表达式中唯一不为零的求和项是省略了 ℓ_{j,e_i+c_i} 的那一项。由此并结合引理 5.3 可知，逆与雅可比矩阵被正确计算。

关于该电路的规模与深度的断言由上述构造以及所用子电路的规模界得出。一致性由模拟论证得出，正如对引理 3.2的证明中那样，并结合上述描述。对于 C'的副本中的门，即名为$(2, v)$，对某个 v，由于 v 可由该名称推出，图灵机可以模拟判定来自引理 3.6 的电路族的直接连接语言的机器（在需要时）。对于所有其他门，可以利用上述电路描述来设计图灵机，类似于对引理 3.1的证明。

□

5.3 定义同伦的方程组的结式

我们现在可以描述定义该同伦的方程组。

定义 5.5. 对任意 $i, j \in \{0, 1, \ldots, n\}$，令 $H_{i,j}(\mathbf{x}\ t)$ 表示多项式

$$H_{i,j}(\mathbf{x}, t) \coloneqq (1-t)G_{i,j}(\mathbf{x}) + tF_{i,j}(\mathbf{x}),$$

我们将其视为 $\mathbb{K}(t)[\mathbf{x}]$ 中的一个元素。对任意这样的 i 与 j，我们用 $h_{i,j}$ 表示 $H_{i,j}$ 在 $x_j = 1$ 处的特化。令 $\mathbf{H}j$ 表示多项式向量 $(H_{0,j}, \ldots, H_{j,j})$，并令 $\mathbf{h}j$ 表示多项式向量 $(h_{0,j}, \ldots, h_{j-1,j})$。◊

将 $H_{i,j}$ 与 $h_{i,j}$ 特化到 $t = 0$，分别得到 $G_{i,j}$ 与 $g_{i,j}$；而特化到 $t = 1$ 则得到 $F_{i,j}$ 与 $f_{i,j}$。此外，对 $j \in [n]$，在 $H_{0,j}, \ldots, H_{j-1,j}$ 中将 x_j 设为零，得到 $H_{0,j-1}, \ldots, H_{j-1,j-1}$。借助泊松公式，我们可以推导出结式$_n(\mathbf{H}_n)$ 的一个表达式。

引理 5.6。 对于每个 $j \in \{0, 1, \ldots, n\}$，令 $V_j \subseteq \mathbb{K}(t)^j$表示由$h_{0,\ j}$、…、$h_{j-1,\ j}$的公共零点组成的集合。我们有

$$\mathrm{Res}_n(\mathbf{H}_n) = \big(1 + t\big(u_{0,(d_0,0,\ldots,0)} - 1\big)\big)^{\prod_{i=1}^n d_i} \times \left(\prod_{\boldsymbol{\rho} \in V_1} h_{1,1}(\boldsymbol{\rho})\right)^{\prod_{i=2}^n d_i} \times \left(\prod_{\boldsymbol{\rho} \in V_2} h_{2,2}(\boldsymbol{\rho})\right)^{\prod_{i=3}^n d_i} \times \cdots \times \left(\prod_{\boldsymbol{\rho} \in V_n} h_{n,n}(\boldsymbol{\rho})\right).$$

证明。 我们有 $F_{0,\ 0} = u_{0,\ (d_0,0,\ldots,0)} x_0^{d_0}$以及 $G_{0,\ 0} = x_0^{d_0}$。因此，$\mathrm{Res}(H_{0,0}) = 1 + t\big(u_{0,(d_0,0,\ldots,0)} - 1\big)$，根据单变量单个型的结式就是其系数这一事实（[Jou91，例 2。1]）。对于方程组 $\mathbf{H}j$，泊松公式（定理 4.3）适用，因为特化到 $t = 1$ 会得到一般形式。展开泊松公式的递推关系，即可得到上述表达式。

□

如上所述，集合 V_j 是坐标属于 $\mathbb{K}(t)$的点的有限集。以这种形式，它们不便于用算术电路和图灵机进行处理。定义$\mathbb{A} : = \mathbb{Q}[\mathbf{u}_0, \ldots, \mathbf{u}_n][\![t]\!]$。将 $h_{i,\ j}$视为环 $\mathbb{A}[x_0, \ldots, x_{j-1}]$中的多项式。结合上述观察与 第 5.2 节中的讨论，我们可以对该方程组应用亨塞尔引理。

引理 5.7。 设 $j \in [n]$。作为 $\mathbb{A}[x_0, \ldots, x_{j-1}]$ 中的元素，多项式集合 $\mathbf{h}j$ 有 $d_0 \cdots d_{j-1}$ 个根，位于 $\mathbb{A}$ 中。对于 $\mathbf{r_c} \in B_j$（定义见 引理 5.2），存在一个根 $\boldsymbol{\rho_c} \in \mathbb{A}^j$，它是 $\mathbf{h}j$ 的根，并满足 $\boldsymbol{\rho_c}$（模 t）$= \mathbf{rc}$。该多项式集合在 $\mathbb{A}$ 的任何扩张中都没有其他根。

证明。第一条结论可由多变量版本的亨塞尔引理推出，例如参见 [Eis13，习题 7。26]。最后一条结论由贝祖不等式推出。 □

我们将使用隐函数定理的一个显式版本，以所需精度计算 $\boldsymbol{\rho}_{\mathbf{c}}$。应用该定理时，我们必须进行一些平移和缩放，确保所计算的根 $\boldsymbol{\rho}_{\mathbf{c}}$ 没有常数项，并且平移后原点处的雅可比矩阵是单位矩阵。

Definition 5.8. 设 $j \in [n]$ 和 $\mathbf{c} \in B_j$。定义平移缩放系统 $\mathbf{h}_{\mathbf{c}}$ as

$$\widetilde{\mathbf{h}}_{\mathbf{c}}(\mathbf{x}) \coloneqq \mathcal{J}_{\mathbf{c}}^{-1}\mathbf{h}_j(\mathbf{x}+\mathbf{r}_{\mathbf{c}}).$$

该方程组以 $\boldsymbol{\rho}_{\mathbf{c}} - \mathbf{r}_{\mathbf{c}}$ 为根，且该根的每个坐标的常数项都为零。该方程组在零点处的雅可比矩阵是单位矩阵。令 $\Delta_{\mathbf{c}}$ 表示该方程组的雅可比行列式 $\widetilde{}$。注意，为简洁起见，我们在记号 $\mathbf{h}_{\mathbf{c}}$ 中省略了 j，因为根据上下文总能明确其含义。◊

$\widetilde{}$每个多项式 $\mathbf{h}_{\mathbf{c}}$ 都属于 $S[t, x_0, \dots, x_{j-1}]$。现在我们引用隐函数定理的一个显式版本，并将其专门应用于定义 5.8中描述的方程组。

引理 *5.9*（隐函数定理 [*AY83*，命题 *20*.3]）。设 $\widetilde{\boldsymbol{\rho}}_{\mathbf{c}} = (\widetilde{\rho}_{\mathbf{c},0}(t), \dots, \widetilde{\rho}_{\mathbf{c},j-1}(t))$ 是 $\widetilde{}\mathbf{h}_{\mathbf{c}}$ 的根，且每个坐标的常数项都为零。记 $\widetilde{\rho}_{\mathbf{c},i}(t) = \sum_{N\geq 0} \widetilde{\rho}_{\mathbf{c},i,N} t^N$，其系数为 $\widetilde{\rho}_{\mathbf{c},i,N} \in S$。那么系数 $\widetilde{\rho}_{\mathbf{c},i,N}$ 由下式给出

$$\widetilde{\rho}_{\mathbf{c},i,N} = \sum_{\substack{(b_0,\dots,b_{j-1})\in\mathbb{N}^j \\ |\mathbf{b}|\leq 2N}} (-1)^{|\mathbf{b}|} \operatorname{coeff}(x_i(\widetilde{h}_{\mathbf{c},0}(\mathbf{x}) - x_0)^{b_0} \cdots (\widetilde{h}_{\mathbf{c},j-1}(\mathbf{x}) - x_{j-1})^{b_{j-1}} \Delta_{\mathbf{c}}, t^N x_0^{b_0} \cdots x_{j-1}^{b_{j-1}}).$$

证明。我们引用的 [AY83，命题 20。3] 中的结果是复解析的，但从中推导出上述形式化陈述很简单。

在下文中，j 和 $\mathbf{c}$ 是固定的。引理 5.7 指出，$\widetilde{\rho}_{\mathbf{c}}$ 的系数是 $\mathbf{u}0, \dots, \mathbf{u}_n$ 的多项式，也就是说，对于所有 i, N，$\widetilde{\rho}_{\mathbf{c},i,N}$ 都属于 $\mathbb{Q}[\mathbf{u}0, \dots, \mathbf{u}_n]$。我们用 $Q_{i,N}$ 表示引理 5.9 陈述中作为右端项出现的多项式，因此我们的主张是，对于所有 i 和所有 N，都有 $\widetilde{\rho}_{\mathbf{c},i,N} = Q_{i,N}$（这些多项式实际上只涉及 $\mathbf{u}0, \dots, \mathbf{u}j{-}1$，但这与证明无关）。

$\widetilde{}$选取 $\boldsymbol{\nu}_0, \dots, \boldsymbol{\nu}_n$，其元素属于 $\mathbb{C}$，并令 $\mathbf{h}_{\mathbf{c},\boldsymbol{\nu}}$ 为在 $\mathbb{C}[t][x_0, \dots, x_{j-1}]$ 中将 $\mathbf{u}$ 取值为 $\mathbf{h}_{\mathbf{c}}$ 里的 $\boldsymbol{\nu}$ 后得到的多项式。通过这一取值，我们看到，$\mathbf{h}_{\mathbf{c},\boldsymbol{\nu}} = 0$ 的唯一常数项为零的形式幂级数根是 $\widetilde{\rho}_{\mathbf{c}}(\boldsymbol{\nu}, t)$，其系数为 $\widetilde{\rho}_{\mathbf{c},i,N}(\boldsymbol{\nu})$，其中 $i = 0, \dots, j-1$ 以及 $N \geq 0$。另一方面，将 [AY83，命题 20.3] 应用于 $\mathbf{h}_{\mathbf{c},\boldsymbol{\nu}}$，可知这些方程中常数项为零的唯一解析根的第 i 个坐标为

$$\begin{aligned}
&\sum_{N\geq 0} \sum_{\substack{|\mathbf{B}|\in\mathbb{N}^j \\ |\mathbf{b}|\leq 2N}} (-1)^{|\mathbf{b}|} \operatorname{coeff}(x_i(\widetilde{h}_{\mathbf{c},\boldsymbol{\nu},0}(\mathbf{x}) - x_0)^{b_0} \cdots (\widetilde{h}_{\mathbf{c},\boldsymbol{\nu},j-1}(\mathbf{x}) - x_{j-1})^{b_{j-1}} \Delta_{\mathbf{c},\boldsymbol{\nu}}, t^N x_0^{b_0} \cdots x_{j-1}^{b_{j-1}}) t^N \\
&= \sum_{N\geq 0} Q_{i,N}(\boldsymbol{\nu}) t^N,
\end{aligned}$$

$\widetilde{}$其中 $\Delta_{\mathbf{c},\boldsymbol{\nu}}$ 是 $\mathbf{h}_{\mathbf{c},\boldsymbol{\nu}}$ 关于 $x_0, \dots, x_{j-1}$ 的雅可比行列式（注意，[AY83]使用记号 $D^{\alpha,w^{\beta},z}$ 表示偏导数 $\partial_w^{\alpha}\partial_z^{\beta}$）。

由于解析根也是形式幂级数环上的根，我们推出 $\widetilde{\rho}_{\mathbf{c},i,N}(\boldsymbol{\nu}) = Q_{i,N}(\boldsymbol{\nu})$ 对所有 i、N 和 $\boldsymbol{\nu}$ 成立，从而 $\widetilde{\rho}_{\mathbf{c},i,N} = Q_{i,N}$ 对所有 i 和 N 成立。 □

$\mathbf{h}_j$ 的根 $\boldsymbol{\rho}_{\mathbf{c}}$ 是 $\widetilde{\boldsymbol{\rho}}_{\mathbf{c}}$ 经$\mathbf{r}_{\mathbf{c}}$的平移。若$\rho_{\mathbf{c}、i、N}$是$\boldsymbol{\rho}_{\mathbf{c}}$ 的坐标中 t 的系数，则对 $N \geq 1$有$\rho_{\mathbf{c}、i、N} = \widetilde{\rho}_{\mathbf{c}、i、N}$，以及$\rho_{\mathbf{c}、0、N} = \mathbf{r}_{\mathbf{c}}$。利用引理 5.9，我们因此可以将 $\boldsymbol{\rho}_{\mathbf{c}}$ 计算到任意选定的精度。为计算结式，我们需要N的系数$\rho_{\mathbf{c}、i、N}$直至 $P := \sum_{i=0}^{n} \prod_{j \neq i} d_j$，这是结式$n(\mathbf{H}_n)$关于变量 t 的次数（引理 4.2）。我们现在描述执行上述计算的电路。存在执行上述计算的常数深度电路，这一点直接由上述公式得出。需要费些功夫的部分是证明存在实现引理 5.9中表达式的一致电路族。

我们首先证明，平移缩放系统及其雅可比行列式可以高效计算。

引理 5.10。 存在一个由 $\mathcal{C}^{\mathrm{scaled}}$ 索引、对数时间一致的无常数电路族，满足以下性质。

- 电路 $C_{\text{平移缩放}j,\ d_0,\ \ldots\ldots,\ d_{j-1}}$ 的规模关于 U_j 和 $\exp(\mathrm{poly}(j))$为多项式，且深度由一个通用常数界定。

- 电路 $C_{\text{平移缩放}j,\ d_0,\ \ldots\ldots,\ d_{j-1}}$有 $U_j + 2j + 1$ 个输入门，分别由变量 $\mathbf{u}_0$、……、$\mathbf{u}_j$、 x_0、……、 x_{j-1}、 $z_0 \cdots z_{j-1}$ 、t标记。该电路有 $j+1$ 个输出门。该电路关于$\mathbf{u}_0$、……、$\mathbf{u}_j$、 x_0、……、x_{j-1}、 t无除法。

- 当 z_0、……、 z_{c-1} 取值为$(c_0$、……、$c_{j-1}) \in B_j$时，该电路计算多项式$\widetilde{\mathbf{h}}_{\mathbf{c}}(x_0$、……、$x_{j-1}$、 $t)$以及雅可比行列式 $\Delta_{\mathbf{c}}(x_0$ 、 …… 、 x_{j-1} 、 $t)$。

证明。 构造 $\mathcal{C}^{\mathrm{scaled}}$ 要求我们定义辅助电路族 $\mathcal{C}'$ 和 $\mathcal{C}''$。我们从构造 $\mathcal{C}'$开始。

族 $\mathcal{C}'$ 也由 j、d_0、. . .、d_{j-1}索引，并采用与 $\mathcal{C}$相同的输入变量。我们描述 $C' = C'_{j、d_0、\ldots、d_{j-1}}$。它包含一个子电路，该子电路是引理 5.4 中构造的电路 $C^{\mathrm{init}}_{j\ d_0、,\ldots、d_{j-1}}$的副本，以变量 $\mathbf{z}$ 为输入。令 $\mathbf{r}_{\mathbf{z}}$、 $\mathcal{J}_{\mathbf{z}}$和 $\mathcal{J}_{\mathbf{z}}^{-1}$表示该子电路的输出。电路 C' 还包含一个计算多项式 $\mathbf{h}_j$的子电路。计算多项式 $\mathbf{h}_j$ 相当于计算多项式 $\mathbf{f}_j$ 和 $\mathbf{g}_j$，而利用 $\mathbf{g}_j$的定义即可完成。计算 $\mathbf{h}_j$ 的子电路以 $\mathbf{x} + \mathbf{r}_{\mathbf{z}}$作为输入，因此它计算 $\mathbf{h}_j(\mathbf{x} + \mathbf{r}_{\mathbf{z}})$。接下来， C' 计算 $\mathcal{J}_{\mathbf{z}}^{-1}$与 $\mathbf{h}_j(\mathbf{x} + \mathbf{r}_{\mathbf{z}})$的矩阵向量乘积。将所得输出记为 $\widetilde{\mathbf{h}}_{\mathbf{z}}$。注意，若将 $\mathbf{z}$ 特化为 $\mathbf{c} \in B_j$，则 $\widetilde{\mathbf{h}}_{\mathbf{z}}$ 恰好就是 $\widetilde{\mathbf{h}}_{\mathbf{c}}$。显然，利用引理 3.2 证明中的模拟论证，上述族 $\mathcal{C}'$ 是多对数时间一致的。 C' 的规模关于 U_j是多项式级的，且每个输出关于 $\mathbf{x}$ 的次数均不超过$d_0 + \cdots + d_{j-1}$。 C'的深度有一个通用常数上界。此外，所有除法门的分母都不含任何 $\mathbf{x}$ 中的变量。

现在我们构造 $\mathcal{C}''$。族 $\mathcal{C}''$也由 j、 d_0、…… d_{j-1}索引，并且使用与 $\mathcal{C}$相同的输入变量。它是通过将引理 3.4 应用于族 $\mathcal{C}'$（其指定变量为 x_0、……、 x_{j-1}）得到的。上一段末尾的陈述表明，$\mathcal{C}'$满足应用此插值结果所需的所有假设。由此得到的电路 $C'' = C''_{j、d_0\ldots\ldots、d_{j-1}}$的规模关于 U_j是多项式级的，并且计算 $C'_{j、d_0\ldots\ldots、d_{j-1}}$的每个输出关于变量 x_0、……、x_{j-1}的系数。这个电路族也是多对数时间一致的，并且由常深度电路组成。

现在我们描述电路 $C = C^{\mathrm{scaled}}_{n\ j\ d_0,,,\ldots,d_{j-1}}$。电路 C 包含电路$C' = C'_{j,d_0,\ldots,d_{j-1}}$的一个副本，其输出也作为 C 的输出。这些门将命名为 $(1, v)$，其中 v 是 C' 内该门的名称。接下来， C 包含 $C'' = C''_{j\ ,d_0,\ldots,d_{j-1}}$的一个副本。这些门将命名为 $(2, v)$，其中 v 是通过插值得到的电路中该门的名称。

~利用子电路 C'' 中计算出的 $\mathbf{h_z}$ 的系数，电路 C 接着计算$\mathbf{h_z}$的雅可比矩阵的元素。关于 x_k 的偏导数只是线性~组合，其权重为 x_k 的幂，所用系数是将$\mathbf{h_z}$ 视为关于 x_k 的多项式时的系数。最后，电路 C 使用计算 $j \times j$ 阶矩阵行列式的平凡深度二电路来计算这个雅可比矩阵的行列式，也就是说，将其展开为 $j!$ 个求和项。这些计算所用的门将命名为 $(3, *)$。

我们现在给出 C 的规模上界。子电路 C', C'' 以及用于计算偏导数的电路的规模可由 $\mathrm{poly}(U_j)$ 界定。为计算行列式，我们使用一个规模关于 $j!$ 为多项式的深度二电路，该规模可由 $\exp(\mathrm{poly}(j))$ 界定。因此， C 的规模是关于 U_j 与 $\exp(\mathrm{poly}(j))$ 的多项式，正如所声称的那样。一致性的证明是一个模拟论证，与先前的证明相同。如前所述，我们的命名方案使我们能够推导出每个子电路中某个门的名称，从而在需要时可用于模拟判定每个子电路的直接连接语言的图灵机。 □

利用 引理 5.10，我们现在证明幂级数根的截断可由一致常数深度电路计算。

引理 5.11. 存在一个由参数 n、j、d_0、.....、d_n 索引的无常数电路 $\mathcal{C}^{\mathrm{root}}$ 的多对数时间一致族，具有以下性质。

- 电路 $C_{\text{根}n,j,d_0,\ldots,d_n}$ 的规模以 $P_{\mathrm{poly}(n)}$为界，其中 $P := \sum_{i=0}^{n} \prod_{j \neq i} d_j$，且深度以一个通用常数为界。
- 电路 $C_{\text{根}n,j,d_0,\ldots,d_n}$ 有 $U_j + j + 1$ 个输入门，由变量$\mathbf{u}_0, \ldots, \mathbf{u}^{j-1}, z_0, \ldots, z^{j-1}, t$标记。该电路有 j 个输出门。该电路关于$\mathbf{u}_0, \ldots, \mathbf{u}_j, t$是无除法的。
- 当输入 $z_0, \ldots, z_{j-1}$ 被特化为 $c_0, \ldots, c_{j-1}$时，该电路对每个 $i \leq j-1$计算截断根$\sum_{N \leq P} \rho_{\mathbf{c}\, i,\, N} t^N$ 。

证明。 我们首先定义一个辅助电路族 $\mathcal{C}'$。该族将由参数 $n, j, d_0, \ldots, d_n, k, b_0, \ldots, b_{j-1}$索引。输入变量将是$\mathbf{u}_0, \ldots, \mathbf{u}_j, x_0, \ldots, x_{j-1}, z_0, \ldots, z_{j-1}, t$。

如果 $k \geq j$，或者如果 $b_0 + \cdots + b_{j-1} > 2P$，那么 $\mathcal{C}'$ 中对应的电路就是空电路。这些条件可以在关于索引描述长度的多项式时间内检查。下面描述索引满足 $k < j$ 且 $b_0 + \cdots b_{j-1} \leq 2P$时的电路。

电路 C' 包含引理 5.10 中 $C^{\mathrm{scaled}}_{j\, d_0 \ldots, , , , d_{j-1}}$ 的一个副本。它计算 ~$\mathbf{h_z}$ 及其雅可比行列式 $\Delta_{\mathbf{z}}$。和往常一样，这些门命名为 $(1, v)$，其中 v 是 $C^{\mathrm{scaled}}_{j\, d_0 \ldots, , , , d_{j-1}}$ 中对应门的名称。接着，电路包含 b_0 个求和门的副本，每个门都计算 $h_{\mathbf{z},0}(\mathbf{x}) - x_0$，这些门命名为 $(2, 0, i)$，其中 $i \leq b_0$。类似地，对于每个 $e < j$，都有 b_e~ 个 $h_{\mathbf{z},t}(\mathbf{x}) - x_e$ 的副本，由求和门计算，并命名为 $(2, e, i)$，其中 $i \leq b_e$。对于每个 $e < j$，都有一个乘积门 $(3, e)$，将这些副本相乘以计算 $(h_{\mathbf{z},e}(\mathbf{x}) - x_e)^{b_e}$。最后，有一个乘法门，其输入包括所有 e 对应的 $(3, e)$、变量 x_k，以及由 $C^{\mathrm{scaled}}_{j\, d_0 \ldots, , , , d_{j-1}}$ 的副本计算得到的雅可比行列式 $\Delta_{\mathbf{z}}$。因此，该电路计算多项式

$$x_k(\widetilde{h}_{\mathbf{z},0}(\mathbf{x}) - x_0)^{b_0} \cdots (\widetilde{h}_{\mathbf{z},j-1}(\mathbf{x}) - x_{j-1})^{b_{j-1}} \Delta_{\mathbf{z}}.$$

该电路族的一致性可由模拟论证得出，因为门名称使我们能够恢复 $C^{\mathrm{scaled}}_{j\, d_0 \ldots, 、, 、, 、 d_{j-1}}$ 的副本中的门名称。没有除法门会除以一个依赖于 $\mathbf{x}$ 或 t 的多项式。电路 C' 的规模是关于 P 的多项式（注意， U_j 本身就是多项式）。 C' 计算的多项式关于 $\mathbf{x}$ 和 t 的次数同样可以界定为 $\mathrm{poly}(P)$。

利用电路族 $\mathcal{C}'$，我们定义另一个辅助电路族 $\mathcal{C}''$，其索引相同。电路族 $\mathcal{C}''$ 通过对引理 3.3) 中的 $\mathcal{C}'$ 应用多变量插值，插值得到 t、x_0、.....、x_{j-1} 的系数。上一段末尾的陈述表明，插值所需的假设均成立。总结迄今为止的构造，我们有一个多对数时间一致族 $\mathcal{C}''$，使得 $C'' = C''_{n、j、d_0}$ .....、d_n、k、b_0.....、b_{j-1} 的输入变量为 $\mathbf{u}0$、.....、$\mathbf{u}^{j-1}$、z_0、.....、z_{j-1}，并计算以下各项的系数

$$x_k(\widetilde{h}_{\mathbf{z},0}(\mathbf{x}) - x_0)^{b_0} \cdots (\widetilde{h}_{\mathbf{z},j-1}(\mathbf{x}) - x_{j-1})^{b_{j-1}} \Delta_{\mathbf{z}}$$

作为关于 t、x_0、.....、x_{j-1} 的多项式。C'' 的规模有上界 $P^{\mathrm{poly}(n)}$，且深度为一个通用常数。

有了这个族，我们回到 C_n^{root},j,d_0,...,d_n 的构造。固定指标 $n, j, d_0, \ldots, d_n$。我们描述电路 $C = C_n^{\mathrm{root}}$,j,d_0,...,d_n。对于每个满足 $|\mathbf{b}| \le 2P$ 的向量 $\mathbf{b} \in \mathbb{N}^j$，以及每个 $k < j$，电路 C 都包含 C''_n, j,d_0,...,d_n,k,b_0,...,b_{j-1} 的一个副本。为简洁起见，在接下来的论证中，我们将这个子电路称为 $C_{\mathbf{b},k}$。$C_{\mathbf{b}}$, k 中每个门的名称形式为 $(1, \mathbf{b}\ k, v)$，其中 v 是该子电路中对应门的名称。对于每个 $\mathbf{b}$ k 和每个 $N \le P$，电路 C 都有一个计算以下内容的乘积门

$$(-1)^{|\mathbf{b}|} \cdot \mathrm{coeff}(x_i(\widetilde{h}_{\mathbf{z},0} - x_0)^{b_0} \cdots (\widetilde{h}_{\mathbf{z},j-1} - x_{j-1})^{b_{j-1}} \Delta_{\mathbf{z}}, t^N x_0^{b_0} \cdots x_{j-1}^{b_{j-1}})$$

通过将常数为 -1 的常数门和来自 $C_{\mathbf{b}、k}$ 副本的系数作为输入。这些乘积门命名为 $(2, \mathbf{b}\ k, N)$。对于每个 $1 \le N \le P$ 和每个 $k < j$，电路 C 都包含一个求和门，使用上述门计算

$$\rho_{\mathbf{z},k,N} \coloneqq \sum_{(b_0,\ldots,b_{j-1}),\ |\mathbf{b}| \le 2N} (-1)^{|\mathbf{b}|} \cdot \mathrm{coeff}(x_k(\widetilde{h}_{\mathbf{z},0} - x_0)^{b_0} \cdots (\widetilde{h}_{\mathbf{z},j-1} - x_{j-1})^{b_{j-1}} \Delta_{\mathbf{z}}, t^N x_0^{b_0} \cdots x_{j-1}^{b_{j-1}}).$$

这些门命名为 $(3, N, k)$。求和门的前驱节点根据 $\mathbf{b}$ 按字典序编号。剩下要计算的只有常数项 $\rho_{\mathbf{z},k,0}$，它们就是 $\mathbf{r}_{\mathbf{z}}$。为此，电路 C 包含 $C^{\mathrm{init}}_{j\ d_0、\ ,d_{j-1}}$ 的一个副本，其门命名为 $(4, v)$，其中 v 是子电路中对应门的名称。按照上述方法计算出所有系数 $\rho_{\mathbf{z},i,N}$ 后，电路中有一些乘积门，用于计算每个 $N \le P$ 和 $k \le j-1$ 对应的 $\rho_{\mathbf{z},k,N} t^N$；还有一些加法门，将这些结果相加，计算每个 $k \le j-1$ 对应的 $\sum_{N \le P} \rho_{\mathbf{z},k,N} t^N$。这些门的名称形式为 $(5, *)$。

现在我们来界定电路的规模。向量 $\mathbf{b}$ with $|\mathbf{b}| \le 2P$ 的总数有上界 $P_{\mathrm{poly}(n)}$。每个副本 $C_{\mathbf{b},k}$ 的规模有上界 $P_{\mathrm{poly}(n)}$，因此整个电路的规模有上界 $P^{\mathrm{poly}(n)}$。深度是通用常数这一事实显然成立。

现在我们论证电路族是一致的。令 T_C 为我们将构造的机器名称，该机器用于判定 $\mathcal{C}^{\mathrm{root}}$的直接连接语言。令 $T_{C'}$ 和 $T_{C''}$为分别判定 $\mathcal{C}'$ 和 $\mathcal{C}''$的直接连接语言的机器。设 $(n, j, d_0, \ldots, d_n, a, p, a')$ 是 T_C的一个输入。界 P 可以在多项式时间内根据索引计算得到。设 a 的名称形式为 $(1, \mathbf{b}\ k, v)$。关键观察是，机器 T_C 可以在形如 $(n, j, d_0, \ldots, d_n, k, b_0, \ldots, b_{j-1}, v, p, a'')$ 的输入上模拟机器 $T_{C''}$，其中 a'' 或者是门类型，或者是 $C_{\mathbf{b},k}$内某个门的名称。这将使 T_C 能够使用 $T_{C'}$ 来判定 $(n, j, d_0, \ldots, d_n, a, p, a')$ 是否为是实例。与之前一样，如果 v 是该子电路的输入门或输出门，则 T_C 使用上述构造中的描述来检查该门的连线是否正确。其余论证，以及当 a 的形式为 $(2, *)$、$(3, *)$、$(4, *)$ 或 $(5, *)$ 时的论证，都是我们之前反复使用过的通常模拟论证。

□

由此，我们 c 通过多对数时间一致的常深度电路计算 $\mathrm{Res}_n(\mathbf{F}_n)$ s.

引理 5.12。 存在一个由参数 n、d_0、……、d_n 索引的多对数时间一致族，其中包含弱无除法、无常数电路$\mathcal{C}^{\mathrm{Res}}$，并具有以下性质。

- 电路 $C_{\text{结式}n,\ d_0,\ \ldots,\ d_n}$ 的规模有上界 $P_{\text{多项式}(n)}$，其中 $P = \sum_{i=0}^{n} \prod_{j\neq i} d_j$，且深度有一个通用常数上界。
- 电路 $C_{\text{结式}n,\ d_0,\ \ldots,\ d_n}$ 有 $U := \sum_{i=0}^{n} \binom{n+d_i}{n}$ 个输入门，分别标记为 $\mathbf{u}_0 \ldots, \mathbf{u}_n$。该电路有一个输出门。
- 该电路计算变量 $\mathbf{u}_0, \ldots, \mathbf{u}_n$上的多元结式 结式$_n(\mathbf{F}_n)$。

证明。 我们首先构造一个以 n，$d_0, \ldots, d_n$ 为索引的辅助族 $\mathcal{C}'$。固定索引n，$d_0, \ldots, d_n$。$C' = C'_{n,\ d_0,\ldots,d_n}$ 的输入将是变量 $\mathbf{u}_0, \ldots, \mathbf{u}_n, t$。

现在我们来描述 C'。对于每个 $j \in [n]$，电路 C' 有 $d_0 \cdots d_{j-1}$ 个电路 $C^{\mathrm{root}}_{n,\ j,\ d_0,\ldots,d_n}$ 的副本引理 5.11 作为子电路。门的名称为 $(1,\ j,\ i,\ v)$，其中 $i \leq d_0 \cdots d_{j-1}$ 且 v是子电路中相应门的名称。此外，电路 C' 包含一些门，分别计算整数 $1, \ldots, \sum_{i=1}^{n} d_i$。

$B_j = [d_0] \times \cdots \times [d_{j-1}]$ 的元素是长度为 j 的整数元组，而 B_j 本身的规模为$d_0 \cdots d_{j-1}$。给定以二进制表示的 $d_0, \ldots, d_n, j, n$ 和 i，可以在多项式时间内计算 B_j 按字典序排列的第 i^{th} 个元素。在 C' 中，i^{th} 份 $C^{\mathrm{root}}_{n,j,d_0,\ldots,d_n}$ 的副本，使用上面计算出的整数 $1, \ldots, \sum d_i$，在 B_j 的第 i^{th} 个元素处求值。根据引理 5.11，这些副本的每个输出门都计算出方程组 $\mathbf{h}_j$ 的根的近似值（在 t中）。

电路 C' 还包含若干子电路副本，用于计算多项式 $h_{1,1}, \ldots, h_{n,n}$，如引理 5.10 的证明所示。具体来说，对于 B_j的每个元素，它都有一份 $h_{j,j}$ 的副本。我们将使用 B_j的第 i^{th} 个元素构造出的近似根，连接到 $h_{j,j}$的第 i^{th} 份副本的输入门。因此，对于每个 $\mathbf{c} \in B_j$，电路都会计算 $h_{j,j}(\boldsymbol{\rho}'_{\mathbf{c}})$，其中 $\boldsymbol{\rho}'_{\mathbf{c}} = \boldsymbol{\rho}_{\mathbf{c}} \pmod{t^P}$。最后，电路 C' 还包含一些门，用于使用这些求值结果实现泊松公式（引理 5.6）。

总之，电路 $C'_{n,\ d_0,\ldots,d_n}$ 实现了 Res$_n(\mathbf{H}_n)$ 的泊松公式，只不过它使用的是环 $\mathbb{A}[\![t]\!]$ 中 $\mathbf{h}_j$ 的根的近似值。逼近阶为 $P = \sum_{i=0}^{n} \prod_{j\neq i} d_j$，输出的次数为 $P^{\mathrm{poly}(n)}$。根据与先前构造相同的论证可知，C' 的规模为 $P^{\mathrm{poly}(n)}$、深度为常数，且电路族 $\mathcal{C}'$ 是多对数时间一致的。C' 中的除法门均不涉及除以依赖于 t 的多项式。此外，C' 计算的多项式关于 t 的次数不超过 $P^{\mathrm{poly}(n)}$。

应用引理 3.2 于电路族 $\mathcal{C}'$（指定变量为 t）可得到一个电路族$\mathcal{C}''$，它计算上述对 t 的近似值中 Res$_n(\mathbf{H}_n)$ 的系数。电路族 $\mathcal{C}''$ 是多对数时间一致的，且由规模为 $P^{\mathrm{poly}(n)}$ 的电路组成。

现在我们回到 $C^{\mathrm{Res}}_{n,\ d_0,\ldots,d_n}$ 的构造。这个电路包含 $C''_{n,\ d_0,\ldots,d_n}$ 的一个副本。它还有一个额外的求和门，用来对 $C''_{n,\ d_0,\ldots,d_n}$ 的输出求和，这些输出对应于 t^i 关于 $i \leq P$ 的系数。计算得到的多项式与通过截断结式的近似计算并在 $t = 1$ 处求值所得到的多项式相同。根据泊松公式、结式的次数界以及同伦的构造，该多项式恰好是 Res$_n(\mathbf{F}_n)$。关于规模、深度和一致性的论断也同样显而易见。 □

在第 4.2节和4.3节中，我们看到了结式如何用于解决超出方形齐次系统可满足性的问题。在这些应用中，我们通常需要计算一个多项式集合的结式，而该集合的系数本身也是多项式。如果这些系数来自环 $\mathbb{Q}[w_1, \ldots, w_k]$，那么结式本身就是 $\mathbb{Q}[w_1, \ldots, w_k]$中的一个多项式，可以通过将这些多项式系数直接代入上文构造的Res$_n(\mathbf{F}_n)$电路来计算。

如果系数是 w_1，……，w_k 中的次数至多为 D的多项式，那么所得计算也可以看作有 $U \cdot \binom{k+D}{k}$ 个输入，每个输入对应于每个系数中 $\mathbf{w}$变量的一个单项式；并且至多有 $(Dnd^n)^{O(k)}$ 个输出，其中 $d := \max_i d_i$。这些输出对应于计算所得结式中 $\mathbf{w}$ 变量的系数。下面的推论指出，这一计算可以由常数深度的多对数时间一致电路完成。这是上述结式计算和插值一致性的直接推论。

推论 5.13. 存在一个由参数 n、d_0、…、d_n、k、D 索引的多对数时间一致族弱无除法、无常数电路 $\mathcal{C}^{\text{composed}}$，具有以下性质。

- 电路 C由 n、d_0.....d_n、k、D 组成，其规模不超过 $(PD)^{\text{poly}(n,k)}$，其中 $P = \sum_{i=0}^{n} \prod_{j \neq i} d_j$，且深度不超过一个通用常数。
- 该电路有 $U \cdot \binom{k+D}{k}$ 个输入变量，记为 u_i、$\boldsymbol{\alpha}$、$\boldsymbol{\beta}$（其中 $\boldsymbol{\beta} \in \mathbb{N}^k$ 满足$|\boldsymbol{\beta}| \leq D$）。该电路有 $\binom{DD'+k}{k}$ 个输出，其中 D' 是 结式$_n(\mathbf{F}_n)$ 的次数。

- 在 γ_i、$\boldsymbol{\alpha}$、$\boldsymbol{\beta}$处取值时，输出门计算的是多项式结式中关于 $\mathbf{w}$ 的单项式系数

$$H_i = \sum_{\boldsymbol{\alpha}} \sum_{\boldsymbol{\beta}} \gamma_{i,\boldsymbol{\alpha},\boldsymbol{\beta}} \mathbf{x}^{\boldsymbol{\alpha}} \mathbf{w}^{\boldsymbol{\beta}}$$

关于变量$\mathbf{x}$。

证明。 存在多对数时间一致的常数深度电路，可以计算多项式$\sum_{\boldsymbol{\beta}} u_i$、$\boldsymbol{\alpha}$、$\boldsymbol{\beta}\mathbf{w}^{\boldsymbol{\beta}}$，对每个 i 以及 $\boldsymbol{\alpha}$ 均如此。然后，我们将这些电路与 结式$_n(\mathbf{F}_n)$ 的电路组合，该电路由引理 5.12得到。所得电路是多对数时间一致的，并计算关于变量$\mathbf{w}$ 以及 u_i、$\boldsymbol{\alpha}$、$\boldsymbol{\beta}$的多项式。关于$\mathbf{w}$ 变量的次数至多为 DD'。我们使用引理 3.3 对 $\mathbf{w}$中的单项式系数进行插值消去。所得电路满足我们所要求的深度、规模和一致性条件。 □

6 在计数层级中判定零点定理

本节中，我们证明希尔伯特零点定理可以在计数层级中判定。为此，我们证明一个一般的转移定理，将算术电路的一致构造转化为可在图灵机上运行的算法。

对于每个具有有理数系数的多项式族 $\mathcal{F} = (f_{\mathbf{n}})_{\mathbf{n}}$，都存在一个与之关联的布尔函数族 $\hat{\mathcal{F}} = (f_{\mathbf{n},h})_{\mathbf{n},h}$，其中 $f_{\mathbf{n},h}$ 对应于对 $f_{\mathbf{n}}$ 求值；输入为由高度至多为 h 的整数对表示的有理数元组。我们的目标是证明：如果多项式族 $\mathcal{F}$ 可以由常数深度、指数规模的多对数时间一致算术电路计算，那么这个关联的布尔函数族就可以在计数层级 CH 中计算。做到这一点后，引理 5.12 的一个直接推论将给出一个 FP^{CH} 算法，用于计算多元结式。应用命题 4.4 和 4.12 的归约，将分别得到用于希尔伯特零点定理判定版和计数版的 CH 与 FP^{CH} 算法。

6.1 从一致算术电路到计数层级

我们的转移定理证明分两步进行。首先，我们利用族 $\mathcal{F}$ 对应的多对数时间一致算术电路，构造出规模和深度相近的多对数时间一致阈值电路，用于计算

ˆ布尔函数 $f_{\mathbf{n},h}$。算术电路可以由阈值电路高效模拟，这直接源于迭代加法和迭代乘法属于对数时间一致TC^0（分别对应定理 2.12的第 1 项和第 2 项）。所得阈值电路的一致性，则源于迭代加法和迭代乘法的对数时间一致性，以及计算 $\mathcal{F}$ 的算术电路所具有的假定一致性。

ˆ 接下来，我们证明，这族用于 $f_{\mathbf{n},h}$ 的阈值电路可以在 CH复杂性类中求值。尽管这些阈值电路的规模呈指数级，但由于它们是均匀的，多项式时间图灵机便可利用嵌套的多数数量词来模拟它们。模拟中使用的多数数量词数量，对应于计算 $f_{\mathbf{n},h}$ 的阈值电路深度。由于我们为 $f_{\mathbf{n},h}$ 构造的是常数深度阈值电路，因此得到的求值过程使用的多数数量词数量有界，因而属于计数层级。

这两种思路都不是我们工作中的根本性创新。Agrawal、Allender 和 Datta[AAD00] 指出，算术电路可以转换为阈值电路，从而在 $\{0,1\}$ 值输入上计算相应的多项式，而且这种转换能够保持电路的规模和深度。Allender、Koucký、Ronneburger、Roy 和 Vinay [AKRRV01] 证明了一个与我们结果类似的结论，表明规模呈指数级的常数深度算术电路可以转换为 CH 算法。第二个结果与我们的工作一样，将阈值电路用作中间表示。

尽管以往的工作中已有这些思想，但我们不知道有任何文献从多项式族 $\mathcal{F}$ 的一致算术电路族出发，并得出相应的布尔函数可以在 CH复杂性类中计算。因此，我们在此给出本节各项结果的完整细节。

我们首先将每个算术门实现为一个 TC^0 子电路，从而将算术电路转换为阈值电路。我们使用定理 2.12。由于定理 2.12 所提供的电路是一致的，这一过程保留了算术电路族的一致性。本小节中构造的布尔函数族都将输入视为有理数序列，并以整数对的形式表示。为使这些函数成为全函数而非偏函数，我们约定，若任一这样的整数对形如 $(a,0)$，则该布尔函数的取值为零。下文中，我们默认输入格式正确，因为这可以作为预处理步骤在多项式时间内判定。

引理 6.1。 设 $\mathcal{C}=(C_{\mathbf{n}})_{\mathbf{n}}$ 是一个多对数时间一致的弱无除法、无常数算术电路族，其定义在 $\mathbb{Q}$ 上，规模为 $s_{\mathbf{n}}$，深度为 $\Delta\in\mathbb{N}$。设 $f_{\mathbf{n}}\in\mathbb{Q}[x_1,\ldots,x_{m_{\mathbf{n}}}]$ 是由 $C_{\mathbf{n}}$计算出的多项式ˆ。存在一个布尔函数族 $f_{\mathbf{n},h}$，以$\mathbf{n}$和一个自然数h为索引，并满足以下性质。

- 对于每个$\mathbf{n}$ 和 h，函数 $f_{\mathbf{n}\,h}$ 有 $2\hat{m}_{\mathbf{n}}(h+1)$ 个输入，它们被解释为 $m_{\mathbf{n}}$个有理数，每个有理数由一对高度为 h的整数表示。此外，该函数有$2h\cdot(s_{\mathbf{n}}\log s_{\mathbf{n}})^{\Delta}+2$ 个输出，它们被解释为一个有理数，该有理数由一对高度为 $h\cdot(s_{\mathbf{n}}\log s_{\mathbf{n}})^{\Delta}$的整数表示。

- 若$(a_1,b_1)\ldots,(a_{m_{\mathbf{n}}}\ b_{m_{\mathbf{n}}})$ 是高度至多为 h的有理数的表示，则ˆ$f_{\mathbf{n}\,h}((a_1,b_1)\ldots,(a_{m_{\mathbf{n}}}\ b_{m_{\mathbf{n}}}))$ 是 $f_{\mathbf{n}}(a_1/b_1,\ldots,a_{m_{\mathbf{n}}}/b_{m_{\mathbf{n}}})$的表示。
- 存在一个多对数时间一致族 $\mathcal{D}=(D_{\mathbf{n}\,h})_{\mathbf{n}\,h}$ 阈值电路，其深度为 $O(\Delta)$，规模为 $\mathrm{poly}\left(h,(s_{\mathbf{n}}\log s_{\mathbf{n}})^{\Delta}\right)$，用于计算函数 ˆ$f_{\mathbf{n}\,h}$。

ˆ证明。我们将通过把每个算术门替换为实现有理数迭代加法和迭代乘法的阈值电路，来构造从$f_{\mathbf{n},h}$ 到电路 $C_{\mathbf{n}}$ 的电路，

使用定理 2.12的第 1 项和第 2 项。为此，我们首先需要给出用于表示 $C_{\mathbf{n}}$中间值的整数的高度上界，因为这将决定我们需要多大规模的阈值电路，才能正确模拟 $C_{\mathbf{n}}$中所执行的运算。对于电路 $C_{\mathbf{n}}$中的每个门 v，我们将计算一个有理数 a_v/b_v，用来表示该门在给定输入下的值。为简洁起见，我们在下面的讨论中令$C = C_{\mathbf{n}}$ 和 $s = s_{\mathbf{n}}$。

对于门 v，v 的 深度 是从 v 出发并终止于输入门或常数门的最长路径的长度。例如，输入门和常数门的深度为 0，而仅以常数门为输入的门的深度为 1。我们声称，如果 v 在 C中的深度为 δ，那么只要 C 的输入可以表示为高度至多为 h的整数对，a_v和 b_v的值就可以表示为高度不超过 $h\cdot(s\log s)^{\delta}$的整数。我们用关于 δ的归纳法证明这一点。当 $\delta = 0$时，门 v要么是电路的输入，要么是常数 0，$+1$，-1之一。如果 v 是常数，那么显然 a_v 和 b_v 的高度至多为 1。如果 v 是输入，那么根据假设，分子 a_v 和分母 b_v 的高度都至多为 h。

当 $\delta \geq 1$时，我们根据标记门 v的运算进行分类讨论。

- 假设 $v = v_1 + \cdots + v_k$是一个加法门。由于电路 C的规模有上界 s，我们知道 $k \leq s$。每个 v_i 都表示为一个商 a_i/b_i，其中根据归纳法，整数 a_i和 b_i的高度至多为 $h\cdot(s\log s)^{\delta-1}$。我们将 v的值表示为 a/b，其中

$$a \coloneqq \left(\frac{a_1}{b_1} + \cdots + \frac{a_k}{b_k}\right) b_1 \cdots b_k = a_1 b_2 \cdots b_k + b_1 a_2 b_3 \cdots b_k + \ \cdots \ + b_1 \cdots b_{k-1} a_k$$
$$b \coloneqq b_1 \cdots b_k.$$

  上面对 a 和 b 的定义中出现的每个乘积，都是由 k 个数相乘得到的，每个数的高度均为 $h\cdot(s\log s)^{\delta-1}$。这意味着每个这样的乘积——尤其是整数 b——的高度均为 $kh\cdot(s\log s)^{\delta-1}$。整数 a是 k个这样的项之和，因此其高度为 $k\log(k)h\cdot(s\log s)^{\delta-1}$。由 $k \leq s$可知，a和 b的高度至多为$h\cdot(s\log s)^{\delta}$，证毕。

- 假设 $v = v_1 \times \cdots \times v_k$是一个乘积门。与前一种情况一样，我们知道 $k \leq s$。每个 v_i都表示为一个商 a_i/b_i，其中根据归纳法，整数 a_i 和 b_i 的高度至多为 $h\cdot(s\log s)^{\delta-1}$。我们将 v的值表示为 a/b，其中

$$a \coloneqq a_1 \cdots a_k$$
$$b \coloneqq b_1 \cdots b_k.$$

  与 v 是加法门时的情形进行相同的分析，可知 a 和 b 的高度至多为 $h\cdot(s\log s)^{\delta}$。

- 最后，假设 $v = v_1/v_2$ 是除法门。v_1 和 v_2 的值分别由商 a_1/b_1 和 a_2/b_2表示。根据归纳法，每个 a_i 和 b_i 的高度至多为$h\cdot(s\log s)^{\delta-1}$。我们将 v表示为商 a/b，其中

$$a \coloneqq a_1 b_2$$
$$b \coloneqq a_2 b_1.$$

  显然，a和 b的高度都至多为 $2h\cdot(s\log s)^{\delta-1} \leq h\cdot(s\log s)^{\delta}$，证毕。

ˆ 为布尔函数 $f_{\mathbf{n},h}$ 构造电路时，我们用实现相应运算的阈值电路替换 C 中的每个算术门，使用 TC^0 电路

由 定理 2.12提供。我们还将每个常数门替换为一组 1 与 0 门，以编码相应常数的表示。如上面的分析所示，只需使用能够实现至多 s 个高度为 $h\cdot(s\log s)^{\Delta}$ 的整数的迭代加法和迭代乘法的阈值电路，因为这是在高度至多为 h 的输入上求值时，表示电路中任意门的值所需的最大高度。这些运算可由常数深度、规模为 $h^{O(1)}(s\log s)^{O(\Delta)}$ 的阈值电路完成。算术电路 C 是弱无除法的，这确保只要所有输入格式正确，按照上述方式对电路求值时就不会发生除以零。

形式上，定理 2.12 所给出的阈值电路，对 $h\cdot(s\log s)^{\Delta}$ 个高度为 $h\cdot(s\log s)^{\Delta}$ 的整数执行迭代加法或迭代乘法，尽管 C 中的门的扇入有上界 s。为此，我们将这些阈值子电路多余的输入硬连线到常数 0 （用于迭代加法）以及常数1 （用于迭代乘法）。类似地，这些阈值电路的输出位数会超过 $h\cdot(s\log s)^{\Delta}$。我们忽略这些多余的输出位，因为我们知道它们不会影响模拟结果。

由于电路 C 的规模为 s，深度为 Δ，显然，该过程会得到一个规模为 $h^{O(1)}(s\log s)^{O(\Delta)}$、深度为 $O(\Delta)$ 的阈值电路；它能正确计算输入高度为 h时电路 C 的输出的二进制表示。我们将所得阈值电路记为 $D_{\mathbf{n},h}$，并将布尔函数$f_{\mathbf{n},h}$ 定义为由 $D_{\mathbf{n},h}$计算的函数。

接下来需要界定电路族 $\mathcal{D}=(D_{\mathbf{n},h})_{\mathbf{n},h}$ 的一致性。$D_{\mathbf{n},h}$ 中属于模拟算术的阈值电路的门名称将是一个元组 $(1, v, u)$，其中v 是 $C_{\mathbf{n}}$ 中正在被模拟的门的名称，而 u 是阈值子电路中模拟 v 的算术的某个门的名称。$D_{\mathbf{n},h}$中的其他门，即计算整数 1 和 0 的编码、以便将其用作算术子电路的额外输入的门，其名称形式为 $(2, *)$。设 T_C、T_+ 和 $T_\times$ 分别为判定 $\mathcal{C}$、迭代加法的阈值电路以及迭代乘法的阈值电路的直接连接语言的图灵机。将我们要设计、用于判定 $\mathcal{D}$的直接连接语言的图灵机记为 T_D。

设 $(\mathbf{n}, h, a, p, b)$ 是 T_D 的一个输入。假设 $a=(1, v_a, u_a)$。如果 $p=\epsilon$，那么当 b 表示 a 的类型时，T_D 必须接受。为作出判定，机器 T_D 首先使用T_C计算门 v_a 的类型。如果 v_a 是求和门，则 T_D 模拟 T_+，以计算 u_a 的类型，并在 b 与该类型匹配时接受。如果 v_a 是乘积门，则 T_D 根据情况模拟 T_+ 或 $T_\times$，以计算 u_a 的类型，并据此接受或拒绝。如果 v_a 是除法门，则 T_D 模拟$T_\times$，以计算 u_a的类型。如果 v_a 是该子电路的输入门，但 a 不是$D_{\mathbf{n}}$的输入门，则我们约定（任意地） a的类型为或。

如果 $p\neq\epsilon$，那么机器 T_D 会根据 b进行分支。

- T_D首先 检查 b 是否属于 $(1, v_b, u_b)$ 型。在这种情况下，它会进一步按如下方式分支。

  – 假设 $v_a=v_b$。在这种情况下，a 和 b 属于同一个实现算术的子电路。机器按照上文所述计算门 v_a 的类型，并使用相应的图灵机检查 u_b 是否为 u_a的前驱。如果是，则接受；否则拒绝。– 假设 $v_a\neq v_b$。在这种情况下，机器检查 u_a 是否为阈值子电路中的输入门，如果不是，则拒绝。如果是，则 T_D 计算整数 p_1 和 p_2，使得u_a 是输入到该阈值子电路的有理数 $p_2{}^{\text{th}}$ 的 $p_1{}^{\text{th}}$ 位。然后计算 v_a 的元数，如果元数小于 p_2，则拒绝。如果元数大于p_2，机器使用 T_C 检查 v_b 是否是 $C_{\mathbf{n}}$中 v_a 的第 $p_2{}^{\text{th}}$ 个输入。它还检查 u_b 是否为

其对应阈值子电路的 $p_1{}^{\text{th}}$ 输出位。如果所有这些检查都通过，则接受该字符串。如果其中任何一项检查失败，则拒绝。

- 假设 b 的名称为 $(2,*)$。在这种情况下，与前面一样，机器 T_D 会检查 a 是否为输入位。随后，它计算整数 p_1 和 p_2，使得 u_a 是阈值电路的第 p_2个整数输入中的第 p_1位。机器 T_D 会验证 v_a 的元数至多为 p_2。最后，T_D 计算 a 的类型，并根据 a 是求和门还是乘法门，检查 b 是否为额外输入所用的 0 或 1 的编码中的正确位。如果所有这些检查都通过，T_D 就接受其输入。

对于 $a = (2,*)$ 的情况，可以用类似的方式处理。所有计算所需时间关于最终电路的规模为多对数时间，关于索引的二进制表示为多项式时间。这表明电路族 $\mathcal{D}$ 是多对数时间一致的。

□

尽管 引理 6.1 针对单输出电路族表述，但很容易将其扩展到多输出电路族。在这种情况下，布尔函数 $f_{\mathbf{n},h}$ 会计算一个自然数二进制表示组成的元组，每个输出门对应一个表示，输出门来自 $C_{\mathbf{n}}$。证明本身无需任何改动。

接下来，我们证明常数深度、指数规模的一致阈值电路可以在计数层级中求值。当然，这类电路的输出门数量本身也可能是指数级的，因此未必能在多项式时间内写出完整输出。我们将证明，给定一个多重索引 $\mathbf{n}$、该族中 $\mathbf{n}^{\text{th}}$ 电路的一个输入，以及一个索引 i，可以在 CH复杂性类中计算相应输出的 i^{th} 位。我们将在下文将这一问题形式化。

定义 6.2。令 $\mathcal{F} := \left(f_{\mathbf{n}} \colon \{0,1\}^{m'_{\mathbf{n}}} \to \{0,1\}^{m_{\mathbf{n}}}\right)_{\mathbf{n}}$ 为一个布尔函数的多重索引函数族。与语言 $L_{\mathcal{F}}$ 相对应的 $\mathcal{F}$ 定义为

$$L_{\mathcal{F}} := \{(i,b,x,\mathbf{n}) \mid f_{\mathbf{n}}(x)_i = b\}.$$

如果 $\mathcal{D}$ 是一个电路族，那么我们滥用记号并用 $L_{\mathcal{D}}$ 来表示由 $\mathcal{D}$计算的函数族所对应的语言。◊

接下来，我们证明：若 $\mathcal{D}$ 是指数规模阈值电路的多对数时间一致族，则与 $\mathcal{D}$ 对应的语言 $L_{\mathcal{D}}$ 位于计数层级中。

引理 6.3 (例如参见 [ABKPM09，定理 4 的证明。1])。设 $\mathcal{D} = (D_{\mathbf{n}})_{\mathbf{n}}$ 是一个多对数时间一致的阈值电路族，其规模为 $s_{\mathbf{n}}$，深度为 Δ，其中 $D_{\mathbf{n}}$ 有 $m_{\mathbf{n}}$ 个输入。设 $L_{\mathcal{D}}$ 是按照 定义 6.2 中的定义与该电路族对应的语言 $\mathcal{D}$。假设 $s_{\mathbf{n}} \leq \exp(\text{poly}(m_{\mathbf{n}}))$。那么 $L_{\mathcal{D}} \in$CH复杂性类。

证明。对于一个整数 $\delta \in \mathbb{N}$，考虑辅助语言

$L_\delta := \{(g,\ b,\ x,\ \mathbf{n}) \mid g$ 是电路 $D_{\mathbf{n}}$ 中深度至多为 δ 的一个门，并且在输入 $x\}$ 上的计算结果为 b，

其中，门名称 g 和电路族中的索引 $\mathbf{n}$ 以二进制形式给出。我们将对 δ 使用归纳法证明 $L_\delta \in$属于 CH复杂性类。

首先，我们证明：给定输入 $(g,b,x,\mathbf{n})$，我们可以在关于输入长度的多项式时间内检查 x 的长度是否为 $m_{\mathbf{n}}$。回顾一致性的定义：存在一个多项式有界递增函数 $T \colon \mathbb{N} \to \mathbb{N}$ 和一台图灵机 M，使得给定输入$\mathbf{n}$，机器 M 至多在 $T(\log(s_{\mathbf{n}}) + N)$ 时间内运行，并计算出 $m_{\mathbf{n}}$，其中 $N = \sum_i \log n_i$。

要判定 x 的长度是否为 $m_{\mathbf{n}}$，我们只能使用关于 $|g|+|x|+N$ 的多项式时间，而不能使用 $\log(s_{\mathbf{n}})+N$。设 Q 是一个多项式有界递增函数，满足 $\log(s_{\mathbf{n}}) \le Q(m_{\mathbf{n}})$。要检查 x 的长度是否正确，我们在输入 $\mathbf{n}$ 上模拟 M，最多运行 $T(Q(|x|)+N)$ 步。如果模拟终止，我们就得到 $m_{\mathbf{n}}$，并可检查 $|x|=m_{\mathbf{n}}$ 是否成立。如果模拟未终止，那么我们知道 x 太短，不能作为 $C_{\mathbf{n}}$ 的有效输入。当 x 的长度正确时，$\log(s_{\mathbf{n}}) \le Q(m_{\mathbf{n}})$ 这一事实还意味着，$C_{\mathbf{n}}$ 中每个门的名称长度都以输入 $(g,b,x,\mathbf{n})$ 的长度为界，且该界是一个多项式函数。在本证明的其余部分，我们的所有机器都会先执行上述检查，若检查失败则拒绝。

现在考虑语言 L_0。我们接收 $(g,b,x,\mathbf{n})$ 作为输入，并须判断 g 是否是标记为常数的门，或者 g 是否是 $D_{\mathbf{n}}$ 的输入门；如果是，则判断 g 在输入 x 上是否求值为 b。根据电路族 $\mathcal{D}$ 假定的规模和一致性，我们可以在多项式时间内（相对于 $(g,b,x,\mathbf{n})$ 的长度）判断 g 是否是输入门；如果是，还可以确定 g 标记的是哪个输入位 x_i。在这种情况下，当且仅当 $b=x_i$ 时，我们接受 $(g,b,x,\mathbf{n})$，其中 x_i 是标记 g 的输入位。如果 g 不是输入门，我们可以检查它是否属于类型 0、+1 或 −1，并在类型与 b 相符时接受。其他所有输入均拒绝。这表明 $L_0 \in \mathsf{P} \subseteq$ CH复杂性类。

当 $\delta \ge 1$ 时，我们将证明语言 L_δ 可以通过访问 $L_{\delta-1}$ 预言机在 PP类中判定。由归纳法可知 $L_{\delta-1} \in$ CH复杂性类，因此可以得出 $L_\delta \in$ CH复杂性类。设 $(g,\ b,\ x,\ \mathbf{n})$ 是 L_δ 的输入。根据 $\mathcal{D}$ 假定的规模和一致性，我们可以在关于 $(g,\ b,\ x,\ \mathbf{n})$ 长度的多项式时间内确定门 g 的类型。不失一般性，我们可以假设 $\mathcal{D}$ 仅由多数门和否定门组成，因为输入门和常数门的情形可以像上面那样处理。

- 假设 g 是一个否定门。我们首先非确定性地猜测一个门 h，并利用 $\mathcal{D}$ 的一致性验证 h 是否为 g 的子节点。所有门的名称均受输入 $(g,b,x,\mathbf{n})$ 长度的某个多项式函数所界，这一事实使我们能够执行该步骤。若 h 不是 g 的子节点，则我们再非确定性地分支一次，在一条路径上接受，在另一条路径上拒绝，从而使对应于 g 的非子节点的那些分支贡献相同数目的接受路径与拒绝路径。若 h 是 g 的子节点，则我们利用对 $L_{\delta-1}$ 的预言机访问来检查 $(h,1-b,x,\mathbf{n}) \in L_{\delta-1}$，当且仅当 $(h,1-b,x,\mathbf{n}) \in L_{\delta-1}$ 时接受 $(g,b,x,\mathbf{n})$。多数计算路径为接受，恰好当 g 在输入 x 上求值为 b 时，因此我们可以用一个PP类$^{L_{\delta-1}}$算法判定 $(g,b,x,\mathbf{n}) \in L_\delta$。

- 假设 g 是一个多数门。与前一种情况一样，我们非确定性地猜测一个门 h，并验证 h 是否是 g 的子节点；同样，我们利用 $\mathcal{D}$ 的一致性来完成验证。如果 h 不是 g 的子节点，我们就分支为一条接受路径和一条拒绝路径，使得 g 的非子节点贡献相同数量的接受路径和拒绝路径。如果 h 是 g 的子节点，我们就使用 $L_{\delta-1}$ 预言机来判断 h 在输入 x 上是否求值为 b，并且当且仅当结果如此时才接受。恰好当 g 的子节点中多数在输入 x 上求值为 b 时，多数计算路径才是接受路径，因此我们可以使用 $\mathsf{PP}^{L_{\delta-1}}$ 算法来判定 $(g,\ b,\ x,\ \mathbf{n}) \in L_\delta$。

在这两种情况下，我们都可以如所述使用 $\mathsf{PP}^{L_{\delta-1}}$ 判定 $(g,\ b,\ x,\ \mathbf{n}) \in L_\delta$。由此，我们得到$L_\Delta \in$CH复杂性类。

现在我们来考虑 $L_{\mathcal{D}}$。给定输入 $(i,\ b,\ x,\ \mathbf{n})$，$\mathcal{D}$ 的一致性还使我们能够计算与索引 i 对应的输出门的名称。然后，我们可以使用针对 L_Δ 的预言机来判断该字符串是否为是实例。这证明了 $L_{\mathcal{D}} \in$CH复杂性类。

□

结合前面的引理，我们得出结论：如果多项式族 $\mathcal{F}$ 可以由一个规模为指数级、深度为常数的一致算术电路族计算，且相应的布尔函数族为 $\mathcal{F}$，那么 $L_{\mathcal{F}}$ 属于 CH复杂性类。

推论 6.4. 设 $\mathcal{C}=(C_{\mathbf{n}})_{\mathbf{n}}$ 是一个多对数时间一致族，由规模为 $s_{\mathbf{n}}$的弱无除法、无常数、常数深度算术电路组成，其中 $C_{\mathbf{n}}$ 有 $m_{\mathbf{n}}$ 个输入。令 $\mathcal{D}$ 表示在 引理 *6.1* 中构造的电路族，该族计算与 $\mathcal{C}$计算出的多项式相对应的布尔函数。假设 $s_{\mathbf{n}} \leq \exp(\mathrm{poly}(m_{\mathbf{n}}))$。那么 $L_{\mathcal{D}} \in$ 属于 CH复杂性类。

证明。 结合 $\mathcal{C}$ 中关于电路规模的假设以及 $\mathcal{D}$由 引理 6.1保证的规模界，我们看到 $\mathcal{D}$ 满足 引理 6.3的假设。将 引理 6.3 应用于 $\mathcal{D}$即可得到结论。 □

我们还需要一个最后的模拟结果。假设我们有一个函数族 $(f_n)_n$，它将 n 位映射为 2^n 位。再假设我们有一个多对数时间一致族 $\mathcal{D}=(D_n)_n$，由多项式规模的 TC^0 电路构成，其中 D_n 以 n 位作为输入。在这种情况下，对于每个 n，我们可以定义一个函数族，将 D_{2^n} 与 f_n 复合而得到。下面的引理指出，与这个复合函数族对应的语言可以在 CH复杂性类$^{L_{\mathcal{F}}}$ 中判定。

引理 6.5。 设 $\mathcal{D}=(D_n)_n$ 是一个多对数时间一致的、多项式规模阈值电路族，其深度为 Δ，其中 D_n 有 n 个输入。设 $\mathcal{F}=\left(f_{\mathbf{n}}:\ \{0,1\}^{m'_{\mathbf{n}}} \to \{0,1\}^{m_{\mathbf{n}}}\right)_{\mathbf{n}}$ 是一个布尔函数族。假设 $m_{\mathbf{n}} \leq \exp(\mathrm{poly}(m'_{\mathbf{n}}))$，并且给定 $m'_{\mathbf{n}}$ 的一元表示和 $\mathbf{n}$ 的二进制表示，可以在多项式时间内计算出 $m_{\mathbf{n}}$ 的二进制表示。令 $\mathcal{D}\circ\mathcal{F}=(D_{m_{\mathbf{n}}}\circ f_{\mathbf{n}})_{\mathbf{n}}$ 表示复合函数族。则 $L_{\mathcal{D}\circ\mathcal{F}} \in$ CH 复杂性类 $^{L_{\mathcal{F}}}$。特别地，若 $L_{\mathcal{F}} \in$CH复杂性类，则 $L_{\mathcal{D}\circ\mathcal{F}} \in$CH复杂性类。

证明。 我们按照 引理 6.3 的证明进行。对于 $\delta \in \mathbb{N}$，考虑辅助语言

$$L_\delta := \{(g,\ b,\ x,\ \mathbf{n}) \mid g \text{是深度至多为 } \delta \text{ 的一个门，在 } D_{m_{\mathbf{n}}} \text{ 中，其在输入 } f_{\mathbf{n}}(x) \text{ 上的计算结果为 } b$$

通过对 δ 进行归纳，我们将证明 $L_\delta \in \mathrm{CH}^{L_{\mathcal{F}}}$。

首先，我们在输入 $(1,\ 1,\ x,\ \mathbf{n})$ 和 $(1,\ 0,\ x,\ \mathbf{n})$ 上查询 $L_{\mathcal{F}}$。 x 的长度等于 $m'_{\mathbf{n}}$，当且仅当这两个字符串中恰有一个属于 $L_{\mathcal{F}}$；因此，这些查询使我们能够确保 x 的长度正确，可以作为 $f_{\mathbf{n}}$ 的有效输入。只要 x 的长度正确，根据假设，我们就有$m_{\mathbf{n}} \leq \exp(\mathrm{poly}(|x|))$。在此论证的其余部分中，我们所有的机器都会执行上述检查。

现在考虑 $\delta=0$ 的情形。我们收到 $(g,\ b,\ x,\ \mathbf{n})$ 作为输入，并必须判定 g 是否为 $D_{m_{\mathbf{n}}}$ 的输入门；若是，还要判定其在输入 $f_{\mathbf{n}}(x)$ 上的计算结果是否为 b。由于电路族 $\mathcal{D}$ 是多对数时间一致的，并根据上一段末尾的观察，我们可以在关于输入长度 $(g,\ b,\ x,\ \mathbf{n})$ 的多项式时间内，判定 g 是否为输入门。如果 g 是第 p^{th} 个输入门，那么我们使用 $L_{\mathcal{F}}$ 进行一次预言机调用，以判定 $(p,\ b,\ x,\ \mathbf{n}) \in L_{\mathcal{F}}$，且当且仅当该预言机调用返回 YES 时接受。如果 g 是类型为 0 或 1 的门，则根据 b 接受或拒绝。这表明 $L_\delta \in \mathrm{P}^{L_{\mathcal{F}}} \subseteq \mathrm{CH}^{L_{\mathcal{F}}}$。

对于 $\delta \geq 1$，与引理 6.3 的证明中相同的论证表明， L_δ 可以通过访问 PP类 预言机 $L_{\delta-1}$来判定。由归纳法可得 $L_{\delta-1} \in$ CH复杂性类$^{L_{\mathcal{F}}}$，因此可推出$L_\delta \in$PP类$^{\mathrm{CH}^{L_{\mathcal{F}}}}$ =CH复杂性类$^{L_{\mathcal{F}}}$，如所需。

特别地，取 $\delta=\Delta$ 并使用 $\mathcal{D}$ 引理 6.3证明中的一致性，我们得到 $L_{\mathcal{D}\circ\mathcal{F}} \in$ CH复杂性类$^{L_{\mathcal{F}}}$。若此外 $L_{\mathcal{F}} \in$ CH复杂性类，则有 $L_{\mathcal{D}\circ\mathcal{F}} \in$ CH复杂性类^{CH} = CH复杂性类，如所述。 □

一个常见的 引理 6.5 应用场景是复合两个一致的阈值电路族，其中内部电路族具有指数规模，而外部电路族具有多项式规模。根据 引理 6.3，内部电路族的输出门可以在 CH复杂性类 中求值。结合上面的 引理 6.5 可知，该复合电路也可以在 CH复杂性类 中求值。

我们还会遇到上述情形的以下扩展。我们有一个具有指数规模且带有多输出的电路族。这些输出将以自然方式分组，而我们希望将每组输出分别与一个多项式规模电路进行复合。例如，第一个电路族计算一个多项式的系数，该多项式的系数属于 $\mathbb{Z}$，而我们希望将每个系数模一个素数 p 取模。在此情形下，在相同假设下，我们可以得到与 引理 6.5 相同的结论。基本上，与 引理 6.5 的证明相同的证明适用于此情形，因此我们省略证明。

引理 6.6. 设 $\mathcal{D}=(D_n)_n$ 是一个深度为 Δ、多项式规模的阈值电路多对数时间一致族，其中 D_n 有 n 个输入。设 $\mathcal{F}=\left(f_{\mathbf{n}}:\{0,1\}^{m'_{\mathbf{n}}}\to\{0,1\}^{m^{(1)}_{\mathbf{n}}\times m^{(2)}_{\mathbf{n}}}\right)_{\mathbf{n}}$ 是一个布尔函数族。假设 $m_{\mathbf{n}}\le \exp(\mathrm{poly}(m'_{\mathbf{n}}))$，并且可以根据 $m'_{\mathbf{n}}$ 的一元表示和$\mathbf{n}$的二进制表示，在多项式时间内计算出 $m^{(1)}_{\mathbf{n}}$ 和 $m^{(2)}_{\mathbf{n}}$的二进制表示。令 $\mathcal{D}\circ\mathcal{F}$ 表示这样得到的函数族：将 $f_{\mathbf{n}}$ 的 $m^{(2)}_{\mathbf{n}}$组输出分别与 $D_{m^{(1)}_{\mathbf{n}}}$计算出的函数复合。则 $L_{\mathcal{D}\circ\mathcal{F}}\in \mathsf{CH}^{L_{\mathcal{F}}}$。特别地，如果 $L_{\mathcal{F}}\in\mathsf{CH}$，那么 $L_{\mathcal{D}\circ\mathcal{F}}\in$CH。

6.2 计算结式并判定零点定理

应用推论 6.4 到引理 5.12中得到的多元结式一致电路族 $\mathbb{Z}$，我们可以得出结论：多元结式可以在计数层级中求值。以这个算法作为起点，我们同样可以得出结论：其他整环上的结式也可以在计数层级中计算，例如 $\mathbb{Z}$ 上的结式 $\mathbb{F}_p$。这利用了以下事实：在 $\mathbb{Z}$ 上的结式具有整数系数，而它模 p 后的像恰好是 $\mathbb{F}_p$ 上的结式（参见定义 4.1）。因此，我们可以通过先将输入提升为整数系数多项式，再计算整数上的结式，最后将结果模 p约简，来计算 $\mathbb{F}_p$ 上的结式。类似的想法也能用于计算 $\mathbb{F}_{p^a}$ 和 $\mathbb{F}_{p^a}[y_1,\dots,y_k]$上的结式。

回顾一下，在第2.3节 中，我们讨论了各种整环，以及如何用二进制表示这些整环中的元素。如果 R是这样的任意一个整环，且 $f\in R[x_1,\dots,x_n]$是一个ˆ多项式，那么我们可以定义布尔函数 f_h，它们对应于对 f 求值，输入高度至多为 h；这与上一节中对 $R=\mathbb{Z}$ 和 $R=\mathbb{Q}$所做的类似。

定理 6.7。 设 R 是环 $\mathbb{Z}$、$\mathbb{Z}[y_1,\dots,y_k]$、$\mathbb{F}_p$、$\mathbb{F}_p[y_1,\dots,y_k]$、$\mathbb{F}_{p^a}$ 或 $\mathbb{F}_{p^a}[y_1,\dots,y_k]$ 之一，其中 p 是素数。设 $\mathcal{F}_R$ 是对应于在 R 上计算结式的布尔函数族。那么 $L_{\mathcal{F}_R}\in$CH复杂性类。

证明。 我们根据环 R 的选取进行分类讨论。

- $R=\mathbb{Z}$：应用 推论 6.4 于 引理 5.12中的电路。 引理 5.12给出了电路规模和输入数量的界限，而这些界限满足 推论 6.4的要求。所得阈值电路将输入视为由整数对表示的有理数。通过用整数 a 表示为整数对 $(a,\ 1)$，即可在给定的整数输入处计算这些电路。电路的输出是结式的值，以有理数 $(a,\ b)$ 表示。

  由于结式是一个具有整数系数的多项式，它在整数值点处的取值本身就是整数。这意味着 a/b 是整数，因此 b 必然整除a。为计算 a/b的二进制表示，我们将用于计算结式的阈值电路族与用于整数除法的电路（定理 2.12的第 3 项）组合起来，从而得到一个

能够计算结式整数表示的电路族。由引理 6.1 的结论可知 a 和 b的位复杂度有界，因此满足调用引理 6.5 所需的条件，可以使用执行除法的电路。根据引理 6.5，由于与结式的有理数表示相对应的语言属于CH复杂性类，与结式的整数表示相对应的语言也属于该类。

- $R = \mathbb{Z}[y_1, \ldots, y_k]$: 推论 5.13 构造了一个多对数时间一致算术电路族，它以多项式 F_0，……，$F_n \in \mathbb{Q}[y_1, \ldots, y_k][x_0, \ldots, x_n]$ 为输入，并输出结式 Res(F_0，……，F_n) 的系数，该结式本身是 $\mathbb{Q}[y_1, \ldots, y_k]$ 上的一个多项式。若多项式 F_i 关于 x 变量的次数至多为 d，关于 y 变量的次数至多为 D，则这些电路的规模以 (ndD)poly(n,k) 为上界，就输入个数而言至多为单指数。将推论 6.4 的多输出类比应用于这些算术电路，使我们能够在 CH复杂性类 中判定对应于 $\mathbb{Q}[y_1, \ldots, y_k]$ 上结式的语言。如上所述，推论 5.13 给出了电路规模与输入个数的界，可见它们满足推论 6.4 中的要求。所得阈值电路可以像前一情形那样，通过用 $(a, 1)$ 表示整数 a，在来自 $\mathbb{Z}[y_1, \ldots, y_k]$ 的输入上进行求值。

  与整数情形类似，当输入 $F_0, \ldots, F_n$ 是 $\mathbb{Z}[y_1, \ldots, y_k][x_0, \ldots, x_n]$的元素时，结式$\mathrm{Res}(F_0, \ldots, F_n)$ 是一个具有整数系数的多项式，而非有理数系数。因此，我们可以使用引理 6.6 将用于计算结式的阈值电路族与用于整数除法的电路（定理 2.12的第 3 项）组合，并将其应用于每个系数，从而得到$\mathrm{Res}(F_0, \ldots, F_n)$各系数的整数表示。根据引理 6.6，由于在 $\mathbb{Q}[y_1, \ldots, y_k]$ 上对应于结式的语言属于CH复杂性类，因此对应于这些计算整数结式的复合函数的语言也属于该复杂性类。

- $R = \mathbb{F}_p$: 将输入多项式记为 $F_0, \ldots, F_n \in \mathbb{F}_p[\mathbf{x}]$。我们可以将它们提升为一组$\widehat{\ }$ $\widehat{\ }$多项式 $F_0, \ldots, F_n \in \mathbb{Z}[\mathbf{x}]$，使其具有整数系数：将 $\mathbb{F}_p$ 中的每个元素提升为介于 0 和 $p-1$ 之间（含端点）的整数。利用情形 $R = \mathbb{Z}$的结果，我们可以在 CH复杂性类中判定 Res($F_0, \ldots, F_n$)任意一位的$\widehat{\ }$ $\widehat{\ }$ $\widehat{\ }$ $\widehat{\ }$值。结式 Res($F_0, \ldots, F_n$)是一个整数。由于在 $\mathbb{F}_p$ 上的结式是 $\mathbb{Z}$ 上的结式在映射 $\mathbb{Z} \to \mathbb{F}_p$（见定义 4.1）下的像，这意味着

$$\mathrm{Res}(F_0, \ldots, F_n) = \mathrm{Res}(\widehat{F}_0, \ldots, \widehat{F}_n) \bmod p.$$

  $\widehat{\ }$ $\widehat{\ }$因此，剩下的就是计算 $\mathrm{Res}(F_0, \ldots, F_n)$ 模 p的余数。根据定理 2.12的第 3 项，存在对数时间一致的 TC^0 电路，可执行带余数的整数除法。特别地，存在对数时间一致的 TC^0 电路，用于计算一个整数除以 p所得的余数。根据$\frown$ $\frown$$F_0, \ldots, F_n$，我们可以将这些电路与计算结式的电路复合。由于引理 6.5，与后者对应的语言属于CH复杂性类，因此与复合函数对应的语言也属于该类；这恰好就是在 $\mathbb{F}_p$上计算结式。

- $R = \mathbb{F}_p[y_1, \ldots, y_k]$: 我们将问题归约到 $R = \mathbb{Z}[y_1, \ldots, y_k]$ 的情形，方法与 $R = \mathbb{F}_p$ 的情形完全类似。令 $F_0, \ldots, F_n \in \mathbb{F}_p[y_1, \ldots, y_k][\mathbf{x}]$ 为输入多项式，$\widehat{\ }$ $\widehat{\ }$并令 $F_0, \ldots, F_n \in \mathbb{Z}[\mathbf{y}][\mathbf{x}]$ 为它们在整数上的提升。那么我们有

$$\mathrm{Res}(F_0, \ldots, F_n) = \mathrm{Res}(\widehat{F}_0, \ldots, \widehat{F}_n) \bmod p,$$

  $\widehat{\ }$ $\widehat{\ }$因此，我们可以先计算 $\mathrm{Res}(F_0, \ldots, F_n)$，然后将此结式中的每个系数模 p 约简，就像上面处理 $R = \mathbb{F}_p$ 的情形那样，使用 引理 6.6，从而计算 $\mathrm{Res}(F_0, \ldots, F_n)$。

- $R = \mathbb{F}_{p^a}$：回顾，$\mathbb{F}_{p^a}$ 同构于 $\mathbb{F}_p[z]/(g(z))$，其中 $g \in \mathbb{F}_p[z]$ 是一个次数为 a 的不可约$\widehat{\ }$多项式。设 $F_0, \ldots, F_n \in \mathbb{F}_{p^a}[\mathbf{x}]$ 为输入多项式，$F_0, \ldots, F_n \in \mathbb{Z}[z][\mathbf{x}]$ 为它们在 $\mathbb{Z}[z]$ 中的提升。设 $\hat{g}$ 为 $g(z)$ 在 $\mathbb{Z}[z]$ 中的一个首一提升。与前面的情形一样，根据结式的普适性（见定义 4.1），我们有

$$\mathrm{Res}(F_0, \ldots, F_n) = \mathrm{Res}(\widehat{F}_0, \ldots, \widehat{F}_n) \bmod (p, \hat{g}(z)).$$

$\widehat{\ }$根据这种情况 $R = \mathbb{Z}[z]$，我们可以在CH复杂性类中计算$\mathrm{Res}(F_0, \ldots, F_n)$，它是$\mathbb{Z}[z]$的一个元素。我们使用在 $\mathbb{Z}$ 上进行伪除法的电路（定理 2.12的第 4 项），结合引理 6.5对该多项式除以$\hat{g}$进行伪除法。由于$\hat{g}$ 是首一的，伪商就是实际的商。随后，我们像前面的情况一样，使用整数除法电路将系数模 p 约化，从而得到结式$\mathrm{Res}(F_0, \ldots, F_n)$。

- $R = \mathbb{F}_{p^a}[y_1, \ldots, y_k]$：通过提升输入，我们将问题归约到上述 $R = \mathbb{Z}[\mathbf{y}]$ 的情形。然后计算结式，对每个系数执行除以$\hat{g}$的提升多项式的伪除法，再将每个系数模 p约化。

□

通过调用命题 4.4中从判定零点定理到计算结式的归约，我们得到一个CH复杂性类算法，用于判定多项式方程组的可满足性。为处理输入的系数属于数域的情况，我们使用以下引理将其提升到有理数域。

引理 6.8。设 $\mathbb{K} := \mathbb{Q}[\alpha]$ 是一个数域，且 $g \in \mathbb{Q}[z]$ 是 α的最小多项式。设 $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$ 是一个多项式集合。定义 $f'_1, \ldots, f'_m \in \mathbb{Q}[x_1, \ldots, x_n, z]$ 为由 $f_1, \ldots, f_m$ 得到的多项式，其中将每个 $\mathbb{K}$-系数写成 $\mathbb{Q}[z]$ 中次数小于 次数 g的多项式。那么，$\mathrm{V}(f_1, \ldots, f_m) \neq \varnothing$ 当且仅当 $\mathrm{V}(f'_1, \cdots, f'_m, g) \neq \varnothing$。此外，如果前一个代数簇是零维的且有 r 个点，那么后一个代数簇也是零维的，且有$r \cdot$次数 g 个点。

证明。环 $\mathbb{K}[\mathbf{x}]/(f_1, \ldots, f_m)$ 和 $\mathbb{Q}[\mathbf{x}\ z]/(f'_1, \ldots, f'_m, g)$ 同构。根据零点定理，$\mathrm{V}(f_1, \cdots, f_m) \neq \varnothing$ 当且仅当 $\mathbb{K}[\mathbf{x}]/(f_1, \ldots, f_m)$ 不是零环。类似地，$\mathrm{V}(f'_1, \cdots, f'_m, g) \neq \varnothing$ 当且仅当 $\mathbb{Q}[\mathbf{x}\ z]/(f'_1, \ldots, f'_m, g)$ 不是零环。第一个结论可由这三个事实直接推出。

现在假设 $\mathrm{V}(f_1, \ldots, f_m)$ 是一个零维簇。这个代数簇的规模记为 r，它恰好等于 $\mathbb{K}[\mathbf{x}]/\operatorname{rad}(f_1, \ldots, f_m)$ 作为 $\mathbb{K}$- 向量空间的维数。令 $\mathbb{L}$ 为 g 的一个分裂域。令 $\alpha_1, \ldots, \alpha_e$ 为 g 在 $\mathbb{L}$ 中的根，其中 $e = \deg g$ 且 $\alpha = \alpha_1$。根据定义，$\mathrm{V}(f'_1, \ldots, f'_m, g)$ 中最后一个坐标为 α_1 的点的数量恰好是 r。

设 $\sigma_1, \ldots, \sigma_e$ 是 $\mathbb{L}$ 的自同构，满足对每个 i，$\sigma_i(\alpha) = \alpha_i$。定义 $\mathbb{K}_i := \sigma_i(\mathbb{K})$。同构 σ_i 诱导出同构 $\mathbb{K}[\mathbf{x}]/\operatorname{rad}(f_1, \ldots, f_m) \cong \mathbb{K}_i[\mathbf{x}]/\operatorname{rad}(\sigma_i(f_1) \ldots, \sigma_i(f_m))$。结合上一段中的陈述，这个同构表明，对于每个 i，$\mathrm{V}(f'_1, \ldots, f'_m, g)$ 中最后一个坐标为 α_i 的点的数量为 r。第二个陈述的证明至此完成。

□

现在我们结合命题 4.4 和定理 6.7 来证明希尔伯特零点定理可以在CH复杂性类中判定。

定理 6.9。设 R 是环 $\mathbb{Z}$、$\mathbb{Z}[y_1, \ldots, y_k]$、数域 $\mathbb{K}$、$\mathbb{K}[y_1, \ldots, y_k]$、$\mathbb{F}_p$、$\mathbb{F}_p[y_1, \ldots, y_k]$、$\mathbb{F}_{p^a}$或 $\mathbb{F}_{p^a}[y_1, \ldots, y_k]$之一，其中 p 是素数。那么，在 R 上判定希尔伯特零点定理属于CH复杂性类。

证明。设 f_1、……、 $f_m \in R[x_1, \ldots, x_n]$ 是我们需要判定其可满足性的多项式。设 d和 h 分别是这些多项式的次数和高度的上界。如果 R是 $\mathbb{K}$或 $\mathbb{K}[y_1, \ldots, y_k]$，那么我们使用引理 6.8，将问题归约到 $R = \mathbb{Q}$或 $\mathbb{Q}[y_1, \ldots, y_k]$的情形，然后分别通分，进一步归约到 $R = \mathbb{Z}$或 $R = \mathbb{Z}[y_1, \ldots, y_k]$的情形。如果 R是环 $\mathbb{F}_p$、 $\mathbb{F}_{p^a}$、 $\mathbb{F}_p[y_1, \ldots, y_k]$、 $\mathbb{F}_{p^a}[y_1, \ldots, y_k]$之一，并且 p（或 p^a）小于 $15nd^n$，那么我们使用引理 2.13，将问题转到扩张 $\mathbb{F}_{p^b}$或 $\mathbb{F}_{p^b}[y_1, \ldots, y_k]$，使得 $p^b \geq 15nd^n$。所需扩张的次数关于输入规模是多项式的，因此这样做只会使输入的高度增加一个多项式因子。类似地，可以使用原环 R中的算术，高效地模拟扩张中的算术。此外，将方程组扩张到扩张域并不会改变其可满足性。

将命题 4.4 中的随机化算法应用于输入 $f_1, \ldots, f_m$，并将得到的多项式记为 $G_{i,j} \in R[t, w, u, x_0, \ldots, x_n]$，其中 $i \in \{0, 1, \ldots, n\}$ 且 $j \in [n]$。要判断方程组 $f_1 = \cdots = f_m = 0$ 是否可满足，我们必须判断是否存在一个 $j \in [n]$，使得 $(\mathrm{TT}_w \mathrm{TT}_t \mathrm{Res}(G_{0,j}, \ldots, G_{n,j}))(0) = 0$。

第二项任务可以如下在 CH复杂性类中解决。我们遍历 $j \in [n]$的所有取值。对于每个$j \in [n]$，我们使用定理 6.7中的算法，在 CH复杂性类中计算 $R_j(t, w, u) := \mathrm{Res}(G_{0,j}, \ldots, G_{n,j})$。结式 R_j是关于 x 变量计算的，并且是 $R[t, w, u]$中的一个多项式。我们的任务是判断 $\mathrm{TT}_w \mathrm{TT}_t R_j$是否具有零常数项。我们在 CH复杂性类中这样做：首先非确定性地猜测 R_j 关于 t 和 w的尾单项式的指数，然后验证 (1) u 中的相应多项式具有零常数项；(2) t 和 w 中所有更小的单项式的系数都为零。第一项验证任务可以在 CH复杂性类中完成，因为我们可以在 CH复杂性类中计算 R_j 的系数。第二项可以在带有 CH谕示的 coNP 中完成，因为我们必须验证所有更小的单项式都具有零系数，而任意单个单项式的系数都可以在 CH复杂性类中计算。由于 $\mathrm{coNP}^{\mathrm{CH}}$ =CH复杂性类，第二项验证任务同样可以在 CH复杂性类中完成。

因此，我们得到了一个随机化归约，将判定 $f_1 = \cdots = f_m = 0$ 的可满足性这一任务归约到一个可在CH复杂性类中求解的问题。该归约成功的概率至少为 $2/3$，因此希尔伯特零点定理属于 $\mathrm{BPP}^{\mathrm{CH}}$。由于BPP $\subseteq$PP $\subseteq$ CH，我们可以如所声称的那样在CH复杂性类中判定希尔伯特零点定理。□

6.3 零维系统中的计数

在第4.3节中，我们看到，要计算零维方程组的解的数量，只需计算多元结式、一元最大公因式，以及系数域的代数闭包中一元多项式的不同根的数量。第6.2节的结果表明，我们可以在CH复杂性类中计算多元结式。本节将介绍计算一元最大公因式和一元多项式不同根数量所需的额外工具。对于将这些方法应用于零维方程组的根计数，我们需要对次数呈指数级增长的多项式执行这些运算。这些多项式的系数可以在CH复杂性类中计算；我们的目标是在CH复杂性类中计算最大公因式的系数和不同根的数量。根据引理6.5 和6.6，为此只需证明可以在对数时间一致的多对数时间TC^0中计算最大公因式和不同根的数量。

我们首先注意到，两个多项式的结式可以通过多对数时间一致的 TC^0 电路计算。这是由引理6.1应用于我们为两个多项式的多元结式构造的电路得出的。

引理 6.10。设 R是环 $\mathbb{Z}$、 $\mathbb{Z}[y_1, \ldots, y_k]$、 $\mathbb{Q}$、 $\mathbb{Q}[y_1, \ldots, y_k]$、 $\mathbb{F}_p$、 $\mathbb{F}_p[y_1, \ldots, y_k]$、 $\mathbb{F}_{p^a}$ 或$\mathbb{F}_{p^a}[y_1, \ldots, y_k]$之一，其中 p是素数。那么，系数属于 R 的两个一元多项式的结式可由对数时间一致TC^0计算得出。

证明。 当 $n = 2$ 时，我们在引理 5.12 和推论 5.13中构造的用于计算多元结式的电路具有多项式规模。将引理 6.1 应用于这些电路，便可立即得到对数时间一致的TC^0 电路，分别在 $\mathbb{Q}$ 和 $\mathbb{Q}[\mathbf{y}]$ 上。对于其余的环，我们采用与定理 6.7证明中相同的论证：首先将输入提升到 $\mathbb{Z}$ 或 $\mathbb{Z}[y_1, \ldots, y_k]$，然后计算结式，最后再投影回所需的环 R。 □

在我们开展这项工作之前，已有研究构造出用于计算两个多项式的结式的常数深度代数电路。Andrews 和 Wigderson [AW24] 利用 Girard–Newton 恒等式的常数深度版本，构造了用于计算此类结式的电路，其系数取自 $\mathbb{Q}$；Bhattacharjee、Kumar、Rai、Ramanathan、Saptharishi 和 Saraf [BKR+25b]则利用拉格朗日反演，构造了系数取自任意域的电路。这两项工作都没有讨论其构造的一致性，但借助 $\mathbb{Q}$ 中的结果，不难推导出这些构造的一致性（对于后一项工作，仅当该域为 第 3 节）。

注 6.11。 不难证明，两个一元多项式的结式对于多对数时间一致 TC^0 是完全的。正如 引理 6.10 所示，两个多项式的结式可以通过多对数时间一致 TC^0 计算。为了证明结式是 TC^0-困难的，我们将其归约自已知的TC^0-完全问题——整数幂运算：给定一个 n 位整数 a 和一个 $O(\log n)$ 位整数 b，计算 a^b。Hesse、Allender 和 Mix Barrington [HAM02] 证明了，幂运算对于对数时间一致 TC^0 是完全的。要将整数幂运算归约到结式，只需注意，若将常数 1 视为次数为 b 的多项式，则

$$\operatorname{Res}(a, 1) = a^b.$$

特别地，要计算 a^b，只需计算两个次数至多为 $n^{O(1)}$ 的一元多项式的结式。这证明了结式对于对数时间一致 TC^0 是困难的。◊

现在我们说明如何利用结式计算来计算一元多项式的最大公因式。以下归约出自 [BKR+25b]。

引理 6.12 ([BKR+25b，第 1 节。2])。 设 $\mathbb{F}$ 是一个域。若 f 和 g 是$\mathbb{F}[x]$中的一元多项式，则

$$\gcd(f, g)(y) = \frac{\operatorname{TT}_z \operatorname{Res}_x(z \cdot (y - x) + f(x), f(x) + u \cdot g(x))}{\operatorname{TT}_z \operatorname{Res}_x(z + f(x), f(x) + u \cdot g(x))}.$$

证明。 对于任意一元多项式 a、b和 $c \in \mathbb{F}[x]$，由泊松公式可知，除相差一个符号外，有

$$\operatorname{TT}_z \operatorname{Res}_x(zb + c, a) = a_0^{\max(\deg b, \deg c)} \left(\prod_{\alpha \in \mathrm{V}(a) \setminus \mathrm{V}(c)} c(\alpha)^{m(\alpha)} \right) \times \left(\prod_{\alpha \in \mathrm{V}(a) \cap \mathrm{V}(c)} b(\alpha)^{m(\alpha)} \right),$$

其中， z 是一个新变量， a_0 是 a的首项系数，而 $m(\alpha)$是 α 作为 a的根的重数。因此，除相差一个符号外，有

$$\prod_{\alpha \in \mathrm{V}(a) \cap \mathrm{V}(c)} b(\alpha)^{m(\alpha)} = a_0^{\max(0, \deg b - \deg c)} \frac{\operatorname{TT}_z \operatorname{Res}_x(zb + c, a)}{\operatorname{TT}_z \operatorname{Res}_x(z + c, a)}.$$

现在考虑多项式 $f, g \in \mathbb{F}[x]$，并令 u 为新变量。作为一个系数取自 $\mathbb{F}(u)$ 的多项式， $f(x) + ug(x)$ 可分解为若干线性形式的乘积。 $f(x)$ 与 $f(x) + ug(x)$ 的所有公因子必然都是 $\gcd(f, g)$ 的因子。此外，这些公因子在 $f(x) + ug(x)$ 中的重数，与它们在 $\gcd(f, g)$ 中的重数相同。由前面对域 $\mathbb{F}(u, y)$ 的讨论可得结论，其中 $a(x) = f(x) + u \cdot g(x)$、 $b(x) = (y - x)$，以及$c(x) = f(x)$。

□

通过结合 引理 6.10 与 引理 6.12，我们得到一个多对数时间一致的 TC^0电路，用于计算两个多项式的最大公因式。

引理 6.13. 设 R 是环 $\mathbb{Z}$、 $\mathbb{Z}[y_1, \ldots, y_k]$、 $\mathbb{F}_p$、 $\mathbb{F}_p[y_1, \ldots, y_k]$、 $\mathbb{F}_{p^a}$ 或 $\mathbb{F}_{p^a}[y_1, \ldots, y_k]$ 之一，其中 p 是素数。那么，在 R 的分式域中，系数属于 R 的两个一元多项式的最大公因式可由多对数时间一致的 TC^0 计算。最大公因式的系数将表示为 b_i/c，其中 b_i、 $c \in R$。

证明。设 f 和 g 是输入。我们通过对环 $R[z, u, y]$ 应用引理 6.10，计算结式 $r_1 := \mathrm{Res}_x(z \cdot (y - x) + f, f + u \cdot g)$ 和 $r_2 := \mathrm{Res}_x(z + f, f + u \cdot g)$。根据 r_1、 r_2，可通过检查系数，按如下方式计算末项 $a_1 := \mathrm{TT}_z\, r_1$ 和 $a_2 := \mathrm{TT}_z\, r_2$。对于每个 $0 \le i \le \deg(a_1)$，我们首先通过检查是否存在一个单项式 $z^i u^j y^k$ 在 r_1 中的系数非零，且所有形如 $z^{i'} u^j y^k$ （其中 $i' < i$ ）的单项式的系数均为零，来确定 z^i 在 r_1 中的系数是否对应 $\mathrm{TT}_z\, r_1$。然后，我们计算 $\mathrm{TT}_z\, r_1$ 中单项式 $u^j y^k$ 的系数各位：当且仅当存在某个 i，使得 (1) z^i 的系数对应于 $\mathrm{TT}_z\, r_1$，并且 (2) $z^i u^j y^k$ 在r_1 中的系数的 ℓ^{th} 位为 1 时，该系数的 ℓ^{th} 位才为 1。通过由与门和或门构成的多项式规模常数深度布尔电路，可以直接完成这一计算。采用完全类似的计算即可得到 $a_2 = \mathrm{TT}_z\, r_2$ 的系数。

我们有 $a_1 \in R[u, y]$ 和 $a_2 \in R[u]$。根据引理 6.12，我们知道 a_2 整除 a_1，商与 u无关，并且该商是 f 和 g的最大公因式。设$a_1 = \sum_i a_{1,\,i} y^i$满足$a_{1,\,i} \in R[u]$。要使 a_1/a_2 与 u 无关，唯一的可能是每个$a_{1,\,i}$ 都是a_2 在 R的分式域中的倍数。因此，只需查看首项就能得出这个倍数；也就是说，$a_{1,\,i}/a_2$ 就是$a_{1,\,i}$ 的首项系数除以 a_2的首项系数。令 c 为 a_2 的首项系数，并令 b_i 为$a_{1,\,i}$ 的首项系数，这样就得到了所需形式的最大公因式。

□

接下来，我们将说明如何利用结式计算，求出一元多项式 f 中对应于重数至少为 k的根的因子。这一计算的灵感来自 [AW24]中的无平方因子分解算法。对于系数属于域 f 的一元多项式 $\mathbb{F}$，我们定义 $f_{>k}$ 为

$$f_{>k}(x) := \prod_{\alpha \in \mathrm{V}(f), m(\alpha) > k} (y - \alpha)^{m(\alpha)},$$

所有重数大于 k 的因子的乘积。

引理 6.14。 设 $\mathbb{F}$ 是一个域。如果 f 是 $\mathbb{F}[x]$ 中的多项式，则有

$$f_{>k} = c' \cdot \frac{\mathrm{TT}_z \,\mathrm{Res}_x\big(z \cdot (y - x) + \mathrm{D}(f) + v\,\mathrm{D}^2(f) + \cdots + v^{k-1}\,\mathrm{D}^k(f), f\big)}{\mathrm{TT}_z \,\mathrm{Res}_x\big(z + \mathrm{D}(f) + v\,\mathrm{D}^2(f) + \cdots + v^{k-1}\,\mathrm{D}^k(f), f\big)},$$

其中 $\mathrm{D}^i(f)$ 是 f 的 i^{th} *Hasse* 导数，且 $c' \in \mathbb{F} \setminus \{0\}$。

证明。 我们应用以下等式

$$\prod_{\alpha \in \mathrm{V}(a) \cap \mathrm{V}(c)} b(\alpha)^{m(\alpha)} = a_0^{\max(0, \deg b - \deg c)} \frac{\mathrm{TT}_z \,\mathrm{Res}_x(zb + c, a)}{\mathrm{TT}_z \,\mathrm{Res}_x(z + c, a)},$$

其中 $a(x) = f(x)$、 $b(x) = (y - x)$，以及 $c(x) = \mathrm{D}(f) + v\mathrm{D}^2(f) + \cdots + v^{k-1}\mathrm{D}^k(f)$，其中 v是一个新变量。任何 $\alpha \in \mathrm{V}(f) \cap \mathrm{V}(c)$ 必然是 $\mathrm{D}(f) \ldots, \mathrm{D}^k(f)$ 的根。 f中同时也是这些 Hasse 导数的根的根，恰好是 f 中重数大于k的那些根。因此， $f_{>k}(y)$ 正是 $\prod_{\alpha \in \mathrm{V}(f) \cap \mathrm{V}(c)} (y - \alpha)^{m(\alpha)}$，如所述。□

我们还定义 $f_{=k}$ 为 $f_{>k-1}(x)/f_{>k}$。若 $f_{=k}$ 的次数为 r，那么 $f(x)$ 恰有 r/k 个不同根，其重数恰为 k。注意，引理 6.14中表达式的分母与 y无关，因此，要计算 y-次数 $f_{>k}$，只需计算分子。利用这一观察，我们设计了一个多对数时间一致的TC^0 电路族，用于计算一元多项式的不同根的数量。

引理 6.15. 设 R 是环 $\mathbb{Z}$、$\mathbb{Z}[y_1,\ldots,y_k]$、$\mathbb{F}_p$、$\mathbb{F}_p[y_1,\ldots,y_k]$、$\mathbb{F}_{p^a}$ 或 $\mathbb{F}_{p^a}[y_1,\ldots,y_k]$ 之一，其中 p 是素数。设 $\mathbb{K}$ 是 R 的分式域的代数闭包。那么，系数属于 R 的一元多项式在 $\mathbb{K}$ 中的不同根的数量可以通过多对数时间一致的 TC^0 计算。

证明。设 $f \in R[x]$ 是输入多项式。首先，我们并行计算所有 Hasse 导数 $\mathsf{D}^i(f)$，其中 $1 \le i \le \deg f$。这只涉及整数算术。然后，我们使用引理 6.10 中针对环 $R[z,y,v]$ 的电路，计算结式 $r_k := \mathsf{TT}_z\mathsf{Res}_x\big(z\cdot(y-x) + \mathsf{D}(f) + v\mathsf{D}^2(f) + \cdots + v^{k-1}\mathsf{D}^k(f),\ f\big)$。根据引理 6.14 及其后续讨论，$r_k$ 的 y-次数恰好等于 $f_{>k}$ 的 y-次数。对所有不超过 $\deg f$ 的 k 计算出这些次数后，我们可以计算

$$\deg f - \deg f_{>1} + \frac{\deg f_{>1} - \deg f_{>2}}{2} + \cdots + \frac{\deg f_{>d-1}}{d}$$

利用整数算术的电路，而这正是 f 在 $\mathbb{K}$ 中所求的不同根的个数。 □

既然我们已经有了多对数时间一致的TC^0 算法来计算最大公因式以及根的个数，我们便可以陈述本小节的主要结果。利用命题 4.12，我们得到一个CH复杂性类算法，用以计数零维多项式方程组的解的个数。

定理 6.16. 设 R 是环 $\mathbb{Z}$、$\mathbb{Z}[y_1,\ldots,y_k]$、数域 $\mathbb{K}$、$\mathbb{K}[y_1,\ldots,y_k]$、$\mathbb{F}_p$、$\mathbb{F}_p[y_1,\ldots,y_k]$、$\mathbb{F}_{p^a}$ 或 $\mathbb{F}_{p^a}[y_1,\ldots,y_k]$ 之一，其中 p 是一个素数。设 $\mathbb{L}$ 是 R 的分式域的代数闭包。存在一个 $\mathsf{FP}^{\mathsf{CH}}$ 算法，用以计数系数属于 R 的零维多项式方程组在 $\mathbb{L}^n$ 中的解的个数。

证明。设 f_1，……，$f_m \in R[x_1,\ldots,x_n]$ 是我们必须计数其根的多项式。设 d 和 h 分别是这些 f_i 的次数与高度的上界。若 R 为 $\mathbb{K}$ 或 $\mathbb{K}[y_1,\ldots,y_k]$，则我们利用引理 6.8 分别化归到 $R=\mathbb{Q}$ 或 $\mathbb{Q}[y_1,\ldots,y_k]$ 的情形，随后再通分到公分母，化归到 $R=\mathbb{Z}$ 或 $R=\mathbb{Z}[y_1,\ldots,y_k]$ 的情形，因为用域元素进行缩放并不改变根的个数。若 R 是环 $\mathbb{F}_p$、$\mathbb{F}_{p^a}$、$\mathbb{F}_p[y_1,\ldots,y_k]$ 或 $\mathbb{F}_{p^a}[y_1,\ldots,y_k]$ 之一，并且 p（或 p^a）小于 $100nd^{2n}$，则我们利用引理 2.13 过渡到扩张 $\mathbb{F}_{p^b}$ 或 $\mathbb{F}_{p^b}[y_1,\ldots,y_k]$，使得 $p^b \ge 100nd^{2n}$。所需扩张的次数关于输入规模是多项式的，因此这样做仅使输入的高度增加一个多项式因子。类似地，扩张中的算术可以用原环 R 中的算术高效模拟。此外，过渡到扩张并不改变根的个数。

将命题 4.12 中的随机化算法应用于输入 $f_1,\ldots,f_m$，并将所得多项式记为 $G_{i,j} \in R[t,u,x_0,\ldots,x_n]$，其中 $i \in \{0,1,\ldots,n\}$ 且 $j \in \{1,2\}$。要计算 $f_1 = \cdots = f_m = 0$ 的根的个数，我们必须计算 $\mathsf{TP}_u\,\mathsf{TT}_t\,\mathsf{Res}(G_{0,1},\ldots,G_{n,1})$ 与 $\mathsf{TP}_u\,\mathsf{TT}_t\,\mathsf{Res}(G_{0,2},\ldots,G_{n,2})$ 的最大公因式的不同根的个数。

该任务可按如下方式在CH复杂性类中求解。对于 $j=1$，2，我们使用定理 6.7的算法在CH复杂性类中计算 $R_j(t,u) := \text{结式}(G_{0,j},\ldots,G_{n,j})$。结式 R_j 是关于x变量计算的，并且是 $R[t,u]$上的多项式。我们首先非确定性地猜测 R_j 关于 t的尾单项式的指数，然后验证 t 中所有更小的单项式的系数为零。这可以在带有CH谕示的coNP中完成，因为 u 中系数的系数

t 中任意单个单项式的都可以在CH复杂性类中计算。由于coNP^{CH} =CH复杂性类，该验证任务可以在CH复杂性类中完成。

接下来，我们非确定性地猜测 u 在 $\mathrm{TT}_t\, R_j$中末尾单项式的指数。这同样可以在 CH复杂性类中完成。接下来，我们可以访问多项式 $\mathrm{TP}_u\mathrm{TT}_t\, R_j$，其形式为 CH复杂性类预言机，能够查询每个单项式的系数。利用 引理 6.5 和 引理 6.13，我们可以构造 CH复杂性类预言机，以查询这两个多项式的最大公因式的系数。这些系数将表示为带有公分母的比值，但我们可以忽略分母，因为缩放不会影响下一步。最后，再次利用 引理 6.5 并结合 引理 6.15，我们可以计算不同根的个数，这与原方程组的根数相同。

因此，我们将计算$f_1 = \cdots = f_m = 0$根数的任务随机化归约为一个可在 FP^{CH} 中求解的问题。该归约以至少 $2/3$ 的概率成功，因此，希尔伯特零点定理的计数版本属于 BPP^{CH} 的函数版本，而后者又包含于 FP^{CH}。

□

7 零点定理的应用

本节给出几个可归约到希尔伯特零点定理的问题示例。此前，人们只知道这些问题属于 PSPACE，而我们的结果表明，实际上可以在 CH复杂性类中解决这些问题。此列表远非详尽。本节中，我们令 $\mathbb{F}$ 表示任意一个适用于我们结果的域，即 $\mathbb{Q}$、一个数域 $\mathbb{K}$、一个有限域 $\mathbb{F}_q$，或以上述某个域为常数域的函数域。在函数域的情形下，我们假设输入仅限于多项式，而非任意有理函数。

第一个应用是判定代数闭包中的根理想成员问题。等价地说，就是检验给定多项式是否在给定代数簇上恒为零。

推论 7.1. 给定多项式 $g, f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$，判定是否

$$g \in \mathrm{rad}\big((f_1, \ldots, f_m)\overline{\mathbb{F}}[x_1, \ldots, x_n]\big)$$

可以在 CH复杂性类 中完成。

证明。 考虑方程组 $f_1 = \cdots = f_m = 1 - zg = 0$，其中 z 是一个新变量。根据零点定理， $g \in \mathrm{rad}\big((f_1, \ldots, f_m)\mathbb{F}[x_1, \ldots, x_n]\big)$ 成立这一条件，等价于该方程组不可满足。这通常称为 Rabinowitsch技巧。可满足性可以在 CH复杂性类中判定，因此，判定元素是否属于理想 $\mathrm{rad}\big((f_1, \ldots, f_m)\mathbb{F}[x_1, \ldots, x_n]\big)$也可以在 CH复杂性类中完成。 □

第二个问题是：给定代数簇的定义方程，计算其维数。为将其转化为判定问题，我们的算法还会将一个数作为输入，并判定维数是否等于该数。Koiran [Koi97]。给出了计算代数簇维数与希尔伯特零点定理之间的类似归约。

推论 7.2. 给定多项式 $f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$ 和整数 r，判断是否

$$dim\, \mathrm{V}(f_1, \ldots, f_m) = r$$

可以在 CH复杂性类 中完成。

证明。 我们设计了一种针对可满足性问题的随机图灵归约。设 $d :=$ 最大次数 f_i，并设 $B \subseteq \mathbb{F}$是一个规模至少为 $100n^2d^n$的子集。如果 $\mathbb{F}$ 的规模不足以选取该子集，我们就利用 引理 2.13转至一个足够大的域扩张。设 $\ell_1, \ldots, \ell_n$ 为随机线性多项式，其系数

从 B中均匀且独立地选取。对于任意整数 k，如果 $\dim \mathrm{V}(f_1, \ldots, f_m) \geq k$，那么该方程组以至少 $1 - 2nd^n/|B|$的概率 $f_1 = \cdots = f_m = \ell_1 = \cdots = \ell_k = 0$ 可满足（引理 4.9）。反之，如果 $\dim \mathrm{V}(f_1, \ldots, f_m) < k$，那么该方程组以相同的概率$f_1 = \cdots = f_m = \ell_1 = \cdots = \ell_k = 0$ 不可满足。因此，根据这些方程组对所有 $k \in [n]$是否可满足，我们可以计算 $\mathrm{V}(f_1, \ldots, f_m)$ 的维数，并判断其是否等于r。 □

我们讨论的最后一个应用，是计算 $\mathbb{F}$上的张量秩。给定一个张量 $T \in \mathbb{F}^{d_1} \otimes \cdots \otimes \mathbb{F}^{d_k}$ 和一个自然数 $r \in \mathbb{N}$ 作为输入，我们需要判断 T的秩是否 T 等于 r。很容易写出一个多项式方程组，当且仅当 T 的秩至多为 r时，该方程组可解。由于定理 6.9 允许我们判定该方程组在代数闭包 $\mathbb{F}$ 上的可解性，且复杂度为CH复杂性类，同样可以在CH复杂性类 中判定 T作为代数闭包 $\mathbb{F}$上的张量时，秩是否为 r 。

推论 7.3。 给定一个整数 r 以及一个以元素列表形式显式给出的张量 $T \in \mathbb{F}^{d_1} \otimes \cdots \otimes \mathbb{F}^{d_k}$，判断 T作为 $\mathbb{F}^{d_1} \otimes \cdots \otimes \mathbb{F}^{d_k}$ 的一个元素，其秩是否恰好为 r，属于CH复杂性类。

证明。 $\mathbb{F}^{d_1} \otimes \cdots \otimes \mathbb{F}^{d_k}$ 中的每个张量的秩都至多为 $d_1 \cdots d_k$，因此如果 $r > d_1 \cdots d_k$，我们就立即拒绝该输入。否则，令$x_{i,j,p}$ 为一组变量，其中 $i \in [k]$、 $j \in [d_i]$且 $p \in [r]$。对于每个索引 $(j_1, \ldots, j_k) \in [d_1] \times \cdots \times [d_k]$，我们写出多项式方程

$$T_{j_1,\ldots,j_k} = \sum_{p=1}^{r} \prod_{i=1}^{k} x_{i,j_i,p}.$$

综合起来，这些方程表达了张量 T 可以写成 r 个秩一张量之和，其中第 p^{th} 个张量是向量$\mathbf{x}_{1,\bullet,p} \otimes \cdots \otimes \mathbf{x}_{k,\bullet,p}$ （对$\mathbf{x}_{i,\bullet,p} = (x_{i,1,p}, \ldots, x_{i,d_i,p})$ ）的外积。因此，该方程组在 $\mathbb{F}$ 上有解，当且仅当T作为 $\mathbb{F}$上的张量秩至多为 r 。

这是一个至多包含 $d_1 \cdots d_k$ 个方程的方程组，涉及至多 $k \cdot (d_1 \cdots d_k)^2$ 个变量。由于张量 T以 $d_1 \cdots d_k$ 个域元素组成的列表给出，我们可以在关于输入规模的多项式时间内写出这个方程组。应用定理 6.9 中的算法，我们可以判定 T 的秩是否至多为 r ，且判定过程属于 CH复杂性类。要判定 T 的秩是否恰好为 r，我们使用相同的过程来检验 T的秩是否至多为 $r - 1$，该检验同样属于 CH复杂性类。 □

参考文献

[AAD00] Manindra Agrawal、Eric Allender 和 Samir Datta。《关于 TC0、AC0 与算术电路》。载于：《计算机与系统科学杂志》60.2 (2000)，第 395–421 页。ISSN：0022-0000。DOI：10.1006/jcss.1999.1675 （引自第42页）。[ABKPM09] Eric Allender、Peter Bürgisser、Johan Kjeldgaard-Pedersen 和 Peter Bro Miltersen。《数值分析的复杂性》。载于：《*SIAM*计算杂志》38.5 (2009)，第 1987–2006 页。DOI：10.1137/070697926 （引自第45页）。[ABNSW25] Rida Ait El Manssour、Nikhil Balaji、Klara Nosan、Mahsa Shirmohammadi 和 James Worrell。《希尔伯特零点定理的参数化版本》。载于：*2025* 年算法简洁性研讨会（*SOSA*）。2025，第444–451页。DOI：10.1137/1.9781611978315.32 （引自第2页）。

[AiK81] L. A. A˘ izenberg 和 A. M. Kytmanov。《牛顿公式的多维类比：非线性代数方程组及其若干应用》。载于：Sibirsk. Mat. Zh. 22.2 (1981)，第 19–30、235 页。ISSN：0037-4474（引自第7页）。[AKRRV01] Eric Allender、Michal Koucký、Detlef Ronneburger、Sambuddha Roy 和 V. Vinay。《计数层级中的时间—空间权衡》。载于：第16届IEEE计算复杂性年度会议（CCC 2001）论文集。2001，第295–302页。DOI：10.1109/CCC.2001.933896（引自第42页）。[AW24] Robert Andrews 和 Avi Wigderson。《用于线性代数问题的常数深度算术电路》。载于：第65届IEEE计算机科学基础年度研讨会（FOCS 2024）论文集。2024。DOI：10.1109/FOCS61266.2024.00138。arXiv：2404.10839 [cs.CC]（引自第5、7、9、23、52、53页）。[AW90] Eric Allender 和 Klaus W. Wagner。《计数层级：多项式时间与常数深度电路》。载于：Bull. EATCS 40 (1990)，第182–194页（引自第3页）。[AY83] L. A. Aizenberg 和 A. P. Yuzhakov。《多维复分析中的积分表示与留数》。第58卷。数学专著译丛。美国罗得岛州普罗维登斯：美国数学会，1983。ISBN：0821815504（引自第32、36页）。[BC06] Peter Bürgisser 和 Felipe Cucker。《数值计算的计数复杂性类 II：代数集与半代数集》。载于：《复杂性杂志》22.2 (2006)，第147–191页。ISSN：0885-064X。DOI：https://doi.org/10.1016/j.jco.2005.11.001（引自第2、4页）。[BCL05] Peter Bürgisser、Felipe Cucker 和 Martin Lotz。《数值计算的计数复杂性类 III：复射影集》。载于：Found. Comput. Math. 5.4 (2005)，第351–387页。DOI：10.1007/S10208-005-0146-X（引自第4页）。[BCS97] Peter Bürgisser、Michael Clausen 和 M. Amin Shokrollahi。《代数复杂性理论》。第315卷。数学科学基础丛书 [数学科学基本原理]。Thomas Lickteig 合作编写。Springer-Verlag，柏林，1997，第xxiv+618页。ISBN：3-540-60582-7。DOI：10.1007/978-3-662-03338-8（引自第25、29页）。[BCSS98] Lenore Blum、Felipe Cucker、Michael Shub 和 Steve Smale。《复杂性与实数计算》。Richard M. Karp 作序。Springer-Verlag，纽约，1998，第xvi+453页。ISBN：0-387-98281-7。DOI：10.1007/978-1-4612-0701-6（引自第2页）。[BKR+25a] Somnath Bhattacharjee、Mrinal Kumar、Shanthanu Rai、Varun Ramanathan、Ram-prasad Saptharishi 和 Shubhangi Saraf。Furstenberg 一项结果所揭示的因式分解封闭性。电子计算复杂性讨论会（ECCC），技术报告 TR25-084。2025（引自第7页）。[BKR+25b] Somnath Bhattacharjee、Mrinal Kumar、Shanthanu Rai、Varun Ramanathan、Ram-prasad Saptharishi 和 Shubhangi Saraf。任意特征下多项式最大公因式的常数深度电路。电子计算复杂性讨论会（ECCC），技术报告 TR25-085。2025（引自第23、52页）。[BL07] Peter Bürgisser 和 Martin Lotz。《计算光滑等维复射影簇的希尔伯特多项式的复杂性》。载于：Found. Comput. Math. 7.1 (2007)，第59–86页。DOI：10.1007/S10208-005-0175-0（引自第4页）。

[Bor77] Allan Borodin.《论时间与空间同规模和深度的关系》。载于：《SIAM计算杂志》6.4（1977），第733–744页。doi：10.1137/0206054（引文见第2页）。[Bro87] W. Dale Brownawell.《零点定理中次数的界》。载于：《数学年刊》126.3（1987），第577–591页。issn：0003486X，19398980。doi：10.2307/ 1971361（引文见第1页）。[BSS89] Lenore Blum、Mike Shub 和 Steve Smale.《实数上的计算与复杂性理论：NP完全性、递归函数与通用机》。载于：《美国数学会通报》（新辑）21.1（1989），第1–46页。issn：0273- 0979，1088-9485。doi：10.1090/S0273-0979-1989-15750-9（引文见第2页）。[BvH82] Allan Borodin、Joachim von zur Gathen 和 John Hopcroft.《快速并行矩阵与最大公因数计算》。载于：《信息与控制》52.3（1982），第241–256页。issn：0019-9958。doi：https://doi.org/10.1016/S0019-9958(82)90766-5（引文见第2页）。[Can90] John Canny.《广义特征多项式》。载于：《符号计算杂志》9.3（1990）。计算代数复杂性专题，编者按，第241–250页。issn：0747-7171。doi：https://doi.org/10.1016/S0747-7171(08)80012-0（引文见第8、24页）。[CGH88] Léandro Caniglia、André Galligo 和 Joos Heintz.《任意特征域上零点定理中次数的简单指数界》（法文）。载于：《巴黎科学院院报》第一辑数学307.6（1988），第255–258页（引文见第1页）。[Cha02] Charalambos A. Charalambides.《计数组合学》。CRC离散数学及其应用丛书。Chapman & Hall/CRC，美国佛罗里达州博卡拉顿，2002年，第xvi+609页。isbn：1-58488-290-5（引文见第16页）。[CLO05] David A. Cox、John Little 和 Donal O’Shea.《代数几何》。第2版。施普林格，纽约州纽约，2005年。doi：10.1007/b138611（引文见第22、23页）。[Csa76] L. Csanky.《快速并行矩阵求逆算法》。载于：《SIAM计算杂志》5.4（1976），第618–623页。doi：10.1137/0205040（引文见第2、5页）。[DPR61] Martin Davis、Hilary Putnam 和 Julia Robinson.《指数丢番图方程的判定问题》。载于：《数学年刊》（第二辑）74（1961），第425–436页。issn：0003-486X。doi：10.2307/1970289（引文见第1页）。[EFP98] Alfredo Eisinberg、Giuseppe Franzé 和 Paolo Pugliese.《整数节点上的范德蒙矩阵》。载于：《数值数学》80.1（1998），第75–85页（引文见第16页）。[Eis13] David Eisenbud.《交换代数：兼论代数几何》。第150卷。施普林格科学与商业媒体，2013年（引文见第36页）。[FG90] Noaï Fitchas 和 André Galligo.《形式计算中的有效零点定理与Serre猜想（Quillen-Suslin定理）》（法文）。载于：《数学新闻》149（1990），第231–253页。doi：10.1002/mana.19901490118（引文见第1页）。[For24] Michael A. Forbes.《任意域上的低深度代数电路下界》。载于：第39届计算复杂性会议（CCC 2024）。Rahul Santhanam 编。第300卷。莱布尼茨国际信息学会议录（LIPIcs）。德国达格施图尔：Schloss Dagstuhl – Leibniz信息学中心，2024年，31:1–31:16。isbn：978-3-95977-331-7。doi：10.4230/LIPIcs.CCC.2024.31（引文见第23页）。[FSS84] Merrick L. Furst、James B. Saxe 和 Michael Sipser.《奇偶性、电路与多项式时间层级》。载于：《数学系统理论》17.1（1984），第13–27页。doi：10.1007/BF01744431（引文见第6页）。

[Gat86] Joachim von zur Gathen.《并行算术计算：综述》。载于：第11届数学基础与计算机科学国际研讨会论文集（MFCS 1986）。Jozef Gruska、Branislav Rovan 和 Juraj Wiedermann 编。柏林，海德堡：施普林格柏林海德堡，1986年，第93–112页。isbn：978-3-540- 39909-4。doi：10.1007/BFb0016236（引文见第12页）。[GG13] Joachim von zur Gathen 和 Jürgen Gerhard.《现代计算代数》。第3版。剑桥大学出版社，2013年（引文见第15、16页）。[GKZ94] Israel M. Gelfand、Mikhail M. Kapranov 和 Andrei V. Zelevinsky.《判别式、结式与多维行列式》。第1版。Birhaäuser，美国马萨诸塞州波士顿，1994年，第x+523页。isbn：978-0-8176-4771-1。doi：10.1007/978- 0- 8176- 4771- 1（引文见第22页）。[HAM02] William Hesse、Eric Allender 和 David A. Mix Barrington.《用于除法和迭代乘法的统一常数深度阈值电路》。载于：《计算机与系统科学杂志》65.4（2002）。《复杂性2001》特刊，第695–716页。issn：0022-0000。doi：https://doi.org/10.1016/S0022-0000(02)00025-9（引文见第5、6、14、52页）。[Hei83] J. Heintz.《代数闭域中的可定义性与快速量词消去》。载于：《理论计算机科学》24（1983），第239–277页（引文见第27页）。[Her26] Grete Hermann.《多项式理想理论中有限步数的问题。（采用K. Hentzelt遗留下来的定理）》（德文）。载于：《数学年刊》95（1926），第736–788页。doi：10.1007/BF01206635（引文见第1页）。[Hil02] David Hilbert.《数学问题》。载于：《美国数学会通报》8.10（1902），第437–479页。issn：0002-9904。doi：10.1090/S0002-9904-1902-00923- 3（引文见第1页）。[HJSS02] J. Heintz、G. Jeronimo、J. Sabia 和 P. Solerno.《交理论与形变算法：多齐次情形》。手稿。2002年（引文见第32页）。[Ier89a] Doug Ierardi.《代数闭域理论中的量词消去》。载于：第21届ACM计算理论年度研讨会论文集（STOC 1989）。David S. Johnson 编。ACM，1989年，第138–147页。doi：10.1145/73007.73020（引文见第8、24、25页）。[Ier89b] Doug J I erardi.《代数闭域理论中量词消去的复杂性》。技术报告。康奈尔大学，1989年（引文见第24页）。[IK93] Douglas Ierardi 和 Dexter Kozen.《并行结式计算》。载于：《并行算法综合》。John H. Reif 编。Morgan Kaufmann Publishers Inc.，1993年，第679–720页（引文见第22页）。[Jel05] Zbigniew Jelonek.《有效零点定理》。载于：《数学发明》162.1（2005），第1–17页。doi：10.1007/s00222-004-0434-8（引文见第1页）。[Jou91] Jean-Pierre Jouanolou.《结式形式体系》（法文）。载于：《数学进展》90.2（1991），第117–263页。issn：0001-8708, 1090-2082。doi：10 . 1016 / 0001 - 8708(91) 90031 - 2（引文见第22、23、35页）。[JS07] Gabriela Jeronimo 和 Juan Sabia.《使用直线程序计算多齐次结式》。载于：《符号计算杂志》42.1-2（2007），第218–235页。issn：0747-7171，1095-855X。doi：10.1016/j.jsc.2006.03.006（引文见第23、32页）。

[Koi96] Pascal Koiran. “希尔伯特零点定理属于多项式层级”。载于：《复杂性杂志》12.4（1996），第273–286页。doi: https://doi.org/10.1006/jcom.1996. 0019（引文见第2页）。[Koi97] Pascal Koiran. “代数簇维数的随机化与确定性算法”。载于：第38届IEEE计算机科学基础研讨会（FOCS 1997）论文集。IEEE计算机学会，1997，第36–45页。isbn: 0818681977。doi: 10.1109/SFCS.1997.646091（引文见第2、55页）。[Kol88] János Kollár. “尖锐有效零点定理”。载于：J. Amer. Math. Soc. 1.4（1988），第963–975页。doi: 10.2307/1990996（引文见第1页）。[KP96] T. Krick 和 L. M. Pardo. “丢番图逼近的计算方法”。载于：《代数几何与应用中的算法》。Laureano González-Vega 和 Tomás Recio 编。巴塞尔：Birkhäuser Basel，1996，第193–253页。isbn: 978-3-0348-9104-2（引文见第27页）。[KPS01] Teresa Krick、Luis Miguel Pardo 和 Martín Sombra. “算术零点定理的尖锐估计”。载于：杜克数学杂志 109.3（2001），第521–598页。doi: 10.1215/S0012-7094-01-10934-4（引文见第1页）。[LST21] Nutan Limaye、Srikanth Srinivasan 和 Sébastien Tavenas. “针对低深度代数电路的超多项式下界”。载于：第62届IEEE计算机科学基础研讨会（FOCS 2021）论文集。2021，第804–814页。doi: 10.1109/FOCS52979.2021.00083（引文见第23页）。[LST25] Nutan Limaye、Srikanth Srinivasan 和 Sébastien Tavenas. “针对低深度代数电路的超多项式下界”。载于：ACM杂志 72.4（2025），26:1–26:35。doi: 10.1145/3734215（引文见第5页）。[Mat70] Ju. V. Matijasevič. “可枚举集的丢番图性”。载于：苏联科学院通报 191（1970），第279–282页。issn: 0002-3264（引文见第1页）。[MM82] Ernst W. Mayr 和 Albert R. Meyer. “交换半群与多项式理想的字问题的复杂性”。载于：Adv. in Math. 46.3（1982），第305–329页。issn: 0001-8708。doi: 10.1016/0001-8708(82)90048-2（引文见第4页）。[MS58] Nathaniel Macon 和 Abraham Spitzbart. “范德蒙矩阵的逆矩阵”。载于：美国数学月刊 65.2（1958），第95–100页。doi: 10.2307/2308881（引文见第16页）。[MSW95] Alexander P. Morgan、Andrew J. Sommese 和 Charles W. Wampler. “贝祖数的乘积-分解界”。载于：SIAM数值分析杂志 32.4（1995），第1308–1325页。doi: 10.1137/0732061（引文见第32页）。[MV05] Peter Bro Miltersen 和 N. V. Vinodchandran. “使用击中集对Arthur-Merlin博弈去随机化”。载于：Comput. Complex. 14.3（2005），第256–279页。doi: 10.1007/S00037-005-0197-7（引文见第2页）。[RT92] John H. Reif 和 Stephen R. Tate. “论阈值电路与多项式计算”。载于：SIAM J. Comput. 21.5（1992），第896–908页。issn: 0097-5397。doi: 10.1137/0221053（引文见第14页）。[Sei74] A. Seidenberg. “代数构造”。载于：Trans. Amer. Math. Soc. 197（1974），第273–313页。issn: 0002-9947,1088-6850。doi: 10.2307/1996938（引文见第1页）。[Som99] Martín Sombra. “稀疏有效零点定理”。载于：Adv. in Appl. Math. 22.2（1999），第271–295页。doi: 10.1006/aama.1998.0633（引文见第1页）。

[Tod91] Seinosuke Toda. “PP类与多项式时间层级一样难”。载于：《SIAM计算杂志》20.5（1991），第865–877页。doi: 10.1137/0220053（引文见第3页）。[Tor91] Jacobo Torán. “由计数量词定义的复杂性类”。载于：ACM杂志 38.3（1991），第753–774页。doi: 10.1145/116825.116858（引文见第3页）。[Vol99] Heribert Vollmer.《电路复杂性导论：一种统一方法》。施普林格科学与商业媒体，1999。doi: doi.org/10.1007/978-3-662-03927-4（引文见第10页）。[Wag86] Klaus W. Wagner. “具有简洁输入表示的组合问题的复杂性”。载于：《计算机学报》23.3（1986），第325–356页。doi: 10. 1007 / BF00289117（引文见第3页）。