arXiv:2601.06299v1 [cs.CC] 9 Jan 2026

常深度与多线性理想证明系统的分离结果

Amik Raj Behera* Magnus Rahbek Dalgaard Hansen † Nutan Limaye ‡ Srikanth Srinivasan §

2026年1月13日

摘要

在这项工作中，我们为理想证明系统（IPS）的若干子系统建立了分离定理。理想证明系统（IPS）是 Grochow 和 Pitassi 提出的一种代数证明系统（《ACM期刊》，2018年）。在经典复杂性理论、布尔值电路复杂度和代数复杂性的背景下，分离定理已得到深入研究。

在 Forbes、Shpilka、Tzameret 和 Wigderson 的一项重要工作中（《计算理论》，2021年），他们提出了两种证明技术，用于证明 IPS 子系统的下界，即函数方法 和 倍数方法。我们运用这些技术并得到以下结果。

1. **常数深度 IPS 的层级定理**。 近期，Limaye、Srinivasan 和 Tavenas（《ACM期刊》，2025年）证明了常深度代数电路的层级定理。我们改编了这一结果，并证明了常数深度 IPS 的层级定理。我们证明，存在一个不可满足多线性实例，它可以由深度为 Δ 的 IPS 反驳，但对它的任何深度为 $(\Delta/10)$ 的 IPS 反驳都必须具有超多项式规模。该结果通过构建在倍数方法之上得以证明。

2. **多线性 IPS 的分离定理**。 在一项颇具影响力的研究中，Raz（《计算理论》，2006年）无条件地分离了两个代数复杂性类，即多线性 NC^1 和多线性 NC^2。在这项工作中，我们针对多线性 IPS 的一个经过深入研究的片段证明了类似结果。

   具体而言，我们给出一个不可满足实例，使其函数式反驳（即在布尔立方体上与该多项式的逆相等的唯一多线性多项式）具有一个规模较小的多线性-NC^2 电路。然而，针对该实例的任何多线性-NC^1 IPS 反驳（$\mathrm{IPS}_{\mathrm{LIN}}$）都必须具有超多项式规模。这一结果是基于

*哥本哈根大学计算机科学系，丹麦。研究经费由 Srikanth Srinivasan 获得的哥本哈根大学启动基金支持。电子邮箱：ambe@di.ku.dk

†丹麦哥本哈根信息技术大学，电子邮箱：ramh@itu.dk。获 VILLUM 基金会资助的哥本哈根基础算法研究中心（BARC）支持，资助项目编号为 54451。

‡丹麦哥本哈根信息技术大学，电子邮箱：nuli@itu.dk。获丹麦独立研究基金支持（资助协议编号：10.46540/3103-00116B），同时也获 VILLUM 基金会资助的哥本哈根基础算法研究中心（BARC）支持，资助项目编号为 54451。§丹麦哥本哈根大学计算机科学系。获欧洲研究理事会（ERC）资助（资助协议编号：101125652, ALBA）。电子邮箱：srsr@di.ku.dk

函数方法。

给定一个多项式 $p(\mathbf{x})$，令 $\text{Image}(p(\mathbf{x}))$ 表示将 $p(\mathbf{x})$ 在布尔立方体上求值时所得值的集合。我们的关键观察是，如果该集合的基数为 $\mathcal{O}(1)$，那么函数方法和倍数方法可用于证明 IPS 子系统的分离定理。我们通过使用寻址构件提升源自代数电路复杂性的困难实例，来获得这样的多项式实例。

致谢。 作者感谢 Varun Ramanathan 在项目早期阶段提供的有益讨论。

目录

1 引言 **1**

1.1 理想证明系统 .1 1.2 代数电路复杂性 .2 1.2.1 分离结果 .3 1.3 结果与技术：常数深度IPS 层级定理 .4 1.4 结果与技术：多线性-NC^1 与多线性-NC^2 .6

2 常深度层级 **7**

2.1 在求和门处添加寻址构件 .8 2.2 证明.10 2.2.1 关于 f_Δ 的反驳上界.10 2.2.2 关于 f_Δ 的反驳下界.14

3 多线性分离定理 **15** 3.1 多线性-NC^1与多线性-NC^2-IPS .16 3.2 定理 3.5 的证明.18

参考文献 **19**

A 复形　　证明提升的子集和的能力 **23**

1 引言

证明系统由一组公理和一套推理规则定义，这些推理规则规定了如何从已有陈述推导出新陈述。其目标是从给定的公理开始，应用这些推理规则，在系统内推导出定理（或重言式）。如果一个证明系统只证明有效陈述，则称其具有可靠性；如果每个有效陈述都能在其中被推导出来，则称其具有完备性。

命题证明复杂性研究这些系统在命题逻辑情境下的相对强度和效率。Cook 和 Reckhow 的一项奠基性成果 [CR79]证明，如果能够给出一些命题重言式，使得它们在每一种命题证明系统中都需要指数规模的证明（也就是说，证明长度——大致对应推理步骤的数量——呈指数增长），那么这将分离复杂性类NP 和coNP。因此，证明复杂度中的下界与计算复杂性理论中的一些核心未决问题密切相关。

在这项工作中，我们关注代数证明系统：我们考察由多项式方程组成的不可满足系统，并通过多项式加法、乘法等代数运算进行推理。具体而言，我们考察一种称为理想证明系统（IPS）的代数证明系统，该系统由 Grochow 和 Pitassi 引入 [GP18]。过去十年间，一系列研究从不同方面探讨了这一证明系统 [FSTW21;AF22; GHT22; ST21; HLT24a; LST25; BLRS25; EGLT25; CGMS25]。本文通过研究这一背景下的分离定理，为这条研究脉络作出贡献。

层级定理是一类分离定理，表明更多资源会带来严格更强的能力。例如，经典的时间层级定理 [HS65] 指出，增加可用的运行时间会严格提升机器的计算能力。对于空间等多种资源，也已知有类似结果 [SHI65], 、电路深度 [Sip83; Has86],以及电路规模 [Juk12; Sha49]。在本文中，我们提出关于层级定理的问题，并更一般地研究不同理想证明系统子系统的分离定理IPS。

为了介绍我们的结果，我们首先简要介绍理想证明系统第 1.1 节。随后，我们回顾代数电路复杂性中的一些结果，具体见第 1.2 节，这些结果将在我们的工作中发挥关键作用。我们的结果和技术将在第 1.3 节以及第 1.4 节中介绍。

1.1 理想证明系统

我们首先回顾代数证明系统的一般框架，重点关注所谓的静态系统。[1] 令$\mathbf{x}$ 表示变量集合 $\{x_1, x_2, \ldots\ldots, x_N\}$。给定一组多项式公理 $f_1(\mathbf{x}), f_2(\mathbf{x}), \ldots\ldots, f_m(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$，目标是证明，不存在能同时满足所有等式 $f_1(\mathbf{x}) = f_2(\mathbf{x}) = \cdots = f_m(\mathbf{x}) = 0$ 的变量布尔赋值。为确保解为布尔值，系统还加入了布尔公理 $\{x_i^2 - x_i = 0\}_{i\in[n]}$。

根据希尔伯特零点定理，该增广系统无解这一事实可以用代

[1]在文献中，这类系统通常称为静态证明系统。其他变体的证明按行给出，称为动态证明系统。本文仅考虑静态系统。

数方式表示。具体而言，如果该系统在 $\mathbb{F}$ 上没有公共零点，那么存在多项式$A_1(\mathbf{x}), \ldots, A_m(\mathbf{x})$和 $B_1(\mathbf{x}), \ldots, B_N(\mathbf{x})$，使得

$$\sum_{i\in[m]} A_i(\mathbf{x}) \cdot f_i(\mathbf{x}) + \sum_{j\in[N]} B_j(\mathbf{x}) \cdot (x_j^2 - x_j) = 1. \tag{1}$$

这个恒等式构成原系统的反驳（或证明）。这种反驳的复杂度以多项式的复杂度 $\{A_i\}$和 $\{B_j\}$来衡量。

在*Grochow* 和 *Pitassi* 提出的理想证明系统（IPS） [GP18], 中，多项式 $A_i(\mathbf{x})$和 $B_j(\mathbf{x})$ 由代数电路表示。这自然引出了若干复杂度参数，例如 IPS 证明的电路规模和电路深度。现在我们正式定义理想证明系统。

定义 1.1（理想证明系统 [GP18]）。设 f_1，……，$f_m \in \mathbb{F}[x_1$，……，$x_n]$ 是布尔立方体 $\{0,\ 1\}^n$上的一组不可满足多项式。换言之，不存在一个布尔赋值$\mathbf{a} \in \{0,\ 1\}^n$ 赋给变量 x_1，……，x_n 使得 $f_i(\mathbf{a}) = 0$ 对所有 $i \in [m]$.

给定一类代数电路 $\mathcal{C}$，系统方程 f_1、…、f_m 的 $\mathcal{C}$-IPS反驳 是一个关于变量 x_1、…、x_n、y_1、…、y_m、z_1、…、z_n 的代数电路 $C \in \mathcal{C}$，满足

- $C(\mathbf{x}, \mathbf{0}, \mathbf{0}) = 0,\ and$
- $C(\mathbf{x}, f_1, \ldots, f_m, x_1^2 - x_1, \ldots, x_n^2 - x_n) = 1.$

该反驳的规模就是电路 C. 的规模

此外，如果电路 C 关于变量 $\mathbf{y}$ 和 $\mathbf{z}$ 的个别次数至多为 1，那么我们称 C 为 $\mathcal{C}$-IPS$_{\mathsf{LIN}}$ 反驳。如果电路 C 关于变量 $\mathbf{y}$ 的个别次数至多为 1（但关于 $\mathbf{z}$ 的个别次数不一定如此），则称 C 为 $\mathcal{C}$-IPS$_{\mathsf{LIN}'}$ 反驳。

一般的 IPS 允许类 $\mathcal{C}$ 为代数电路的情形，可以在多项式时间内模拟扩展 Frege [GP18], 是已知最强的命题证明系统之一。此外，要为这类一般 IPS 建立下界，将意味着得到强有力的代数电路下界，这是代数复杂性中的一个核心未解问题。

尽管这仍然是一个雄心勃勃的开放问题，但我们已经针对若干受限类别取得了许多令人信服的新下界结果 $\mathcal{C}$，例如只读代数分支程序、常深度电路和多线性公式 [FSTW21；GHT22；HLT24b；BLRS25；EGLT25]。

这些下界是通过利用代数复杂性中相应计算模型已知的下界而建立的。我们也受到这一框架的启发。具体而言，我们利用代数复杂性理论中的分离结果和层级定理，为 IPS 推导出类似结果。现在我们回顾已知的分离结果。

1.2 代数电路复杂度

我们首先回顾一些与我们的结果相关的标准计算模型。

代数电路、公式、常深度电路、多线性多项式和电路。代数电路是一种有向无环图，其中每个节点要么计算其输入的和（或线性组合），

要么计算其输入的乘积。叶节点要么是变量，要么是常数。代数电路的规模是电路中边或连线的数量，而代数电路的深度是从叶节点（源节点）到输出节点（汇节点）的最长路径。代数公式是一种代数电路，其中每个节点的输出最多馈入另一个节点；换句话说，代数公式的底层图是一棵树。如果代数电路/公式的深度是一个固定常数，且与其他参数无关，则称其为常深度电路/公式。

多项式 $f(\mathbf{x}) \in \mathbb{F}[x_1, \ldots\ldots, x_n]$ 是多线性的，当且仅当多项式的每个单项式中，任一变量的次数至多为 1。若代数电路/公式的每个门都计算一个多线性多项式，则该代数电路/公式是多线性的。若任一乘法门的子节点所计算的多项式涉及互不相交的变量集，则该代数电路是语法多线性的。

1.2.1 分离结果

我们的工作很大程度上依赖于代数复杂性理论中已知的分离结果。我们关于多线性 IPS 的结果基于以下多线性分离结果。

多线性公式与电路。代数复杂性领域一项著名成果，是证明了多线性公式与多线性电路之间存在分离。Raz 在一项具有重要影响力的工作中确立了这一结果 [Raz04], ，该工作提出了一个由多项式规模的多线性电路计算的多项式，但计算它的任何多线性公式都需要超多项式规模。

关键思路是为多项式构造一种复杂度度量，使其对困难多项式取值很大，而对所有小规模多线性公式取值都显著较小。Raz 的度量 [Raz04]定义如下。

定义 1.2 （秩度量 [Raz04]）。令 $\mathbf{x} = \{x_1, \ldots, x_{2n}\}$。令 $\mathbf{y} \cup \mathbf{z}$ 为 $\mathbf{x}$ 的一个等分划分，即 $|\mathbf{y}| = |\mathbf{z}|$。对于给定的多项式 $f(\mathbf{x})$，令 $M_{\mathbf{y},\mathbf{z}}(f)$ 为一个矩阵，其行以关于 $\mathbf{y}$ 变量的多线性单项式标记，列以关于 $\mathbf{z}$ 变量的多线性单项式标记。对于关于 $\mathbf{y}$ 变量的单项式 $m_{\mathbf{y}}$ 以及关于 $\mathbf{z}$ 变量的单项式 $m_{\mathbf{z}}$，矩阵的 $M_{\mathbf{y},\mathbf{z}}(f)[m_{\mathbf{y}}, m_{\mathbf{z}}]^{th}$ 项是多项式 f 中单项式 $m_{\mathbf{y}} \cdot m_{\mathbf{z}}$ 的系数。该度量是此矩阵的秩。

如果多项式 f 关于划分 $\mathbf{y}, \mathbf{z}$ 的秩为满秩，即 $M_{\mathbf{y},\mathbf{z}}(f)$ 的秩是满的，也就是 2^n，我们就称其为满秩多项式。

Raz 已证明 [Raz04] ，计算任意满秩多项式 $f(\mathbf{x})$所需的多线性公式规模至少为 $n^{\Omega(\log n)}$。在我们的工作中，我们基于 Raz 和 Yehudayoff 后续工作中定义的满秩多项式展开 [RY08]。

常深度层级定理 在我们的工作中，我们为常深度IPS建立了常深度层级定理。为此，出发点是 Limaye、Srinivasan 和 Tavenas 提出的常深度层级定理 [LST21]。对于每个深度 Δ，他们构造了一个多项式，该多项式可由多项式规模的深度为 Δ 的电路计算，但任何深度甚至比Δ 小 1 的电路计算它都需要超多项式规模。由于当深度为常数时，电路可以转换为规模仅发生多项式增长的公式，我们在下文陈述层级定理的公式版本。

形式化地说，它表述如下。

定理 1.3（常数深度代数公式层级）。 *[LST21，定理 5]*。对于每个深度参数 $\Delta = \mathcal{O}(1)$，都存在一个显式集合多线性多项式 $Q_\Delta \in \mathbb{F}[x_1, \ldots\ldots, x_n]$使得：

1. 存在一个无常数[2]代数公式，其输入门带有来自 $\mathbf{x} \cup \{0, 1\}$并在深度 $Q_\Delta(\mathbf{x})$ 下计算 Δ，规模为 s。*2.* 任何在深度 $Q_\Delta(\mathbf{x})$ 下计算 $(\Delta/2 - 1)$ 的代数公式都需要规模 $s^{\omega(1)}$。

备注 1.4。 在 *[LST21]*, 中可以得到更紧的分离结果。具体而言，深度层级区分了两个连续的深度，Δ 与 $\Delta - 1$相比。然而，由此得到的公式不是无常数的。如上文所述，只需在参数上略有损失，即可得到无常数公式的深度层级。

现在我们可以陈述本文的贡献了。

1.3 结果与技术：常数深度 IPS 层级定理

作为第一个结果，我们证明了常数深度 IPS 的深度层级定理。更具体地说，我们证明以下定理。

定理 1.5 (常数深度 IPS 层级**)**。 设 $\mathbb{F}$ 为一个特征为零的域。对于每个增长参数 $N \in \mathbb{N}$ 以及满足 $\Gamma = \mathcal{O}(1)$的深度参数 $\Gamma \in \mathbb{N}$，以下结论成立。对于每个深度参数 Γ，存在一个多线性多项式 $f_\Gamma \in \mathbb{F}[x_1, \ldots, x_N]$，它在 $\{0,1\}^N$ 上不可满足（即不存在满足 $f_\Gamma(\mathbf{a}) = 0$的**一个** $\in \{0,1\}^N$），使得以下两个条件成立：

1. 存在一个深度为 Γ 、规模为 $\mathcal{O}(s^5)$的 IPS 反驳，针对 $f_\Gamma(\mathbf{x})$ 。*2.* 任何针对 $f_\Gamma(\mathbf{x})$ 、深度为 $\leqslant \Gamma/10$ 的IPS 反驳都需要规模为 $s^{\omega(1)}$。

为了描述证明策略，我们先针对一个更简单的情形证明上述定理。设 $Q_\Delta(\mathbf{x})$ 是 [LST21] 在定理 1.3 中使用的多项式。现在考虑定义为 $Q_\Delta(\mathbf{x}) \cdot y \cdot (1 - y)$的 $g_\Delta(\mathbf{x}\ y)$，其中 y 是一个新变量。首先注意，该多项式在布尔立方体上的求值为 0。事实上，只考虑 y的布尔赋值时，这一点仍然成立。因此，$g_\Delta(\mathbf{x}\ y) - 1$ 不可满足。此外，$g_\Delta(\mathbf{x}\ y) - 1 \equiv 1$ 模 $y^2 - y$。而且很容易看出，$g_\Delta(\mathbf{x}\ y)$ 与 $Q_\Delta(\mathbf{x})$具有相同的上界。因此，我们得到这个上界。

对于下界，我们将使用倍数方法。该方法由 [FSTW21]提出，并已成功用于 IPS下界证明，见 [FSTW21；AF22；以及25]。现在我们来说明如何使用这一方法得到一个下界。

考虑 $g_\Delta(\mathbf{x}\ y) - 1$。利用 定理 1.3，我们知道它不存在深度为 $(\Delta/2 - 1)$的多项式规模公式。此外，鉴于近期关于常深度公式因子的研究 [BKRRSS25]，，我们还知道，深度为 $(\Delta/2 - \mathcal{O}(1))$ 的多项式的每个倍数都必须具有超多项式规模。也就是说，多项式 $g_\Delta(\mathbf{x}\ y) - 1$ 及其所有倍数对于深度

[2] 如果电路或公式 $C(\mathbf{x})$ 除输入处外不含任何常数，且所有输入门的标签均为 $\mathbf{x} \cup \{-1、0, 1\}$，则称其为无常数的。

为 $(\Delta/2-\mathcal{O}(1))$ 都是困难的。这一性质足以使倍数方法适用，下面将对此作出解释。具体而言，我们的多项式系统是 $f_\Delta = g_\Delta(\mathbf{x}\ y) - 1, \{x_i^2 - x_i\}_{i\in[N]}$, 和 $\{y^2 - y\}$。IPS 反驳满足 $C(\mathbf{x}\ y,\ u,\ \mathbf{0},\ 0) = 0$ 以及 $C(\mathbf{x}\ y,\ f_\Delta,\ \mathbf{x}^2-\mathbf{x}\ y^2-y) = 1$，其中 $\mathbf{x}^2-\mathbf{x}$ 表示$\{x_i^2 - x_i\}_i$。

现在，我们将 $C(\mathbf{x}\ y, f_\Delta, \mathbf{x}^2-\mathbf{x}\ y^2-y)$ 表示为关于 f_Δ 的一元多项式，并得到

$$\sum_{i\geqslant 1} C_i(\mathbf{x}, y, \mathbf{x}^2-\mathbf{x}, y^2-y) f_\Delta^i = 1 - C(\mathbf{x}, y, 0, \mathbf{x}^2-\mathbf{x}, y^2-y)$$

对于某个 $C_i s$。这表明， f_Δ 的一个倍数与 $C(\mathbf{x}\ y, \mathbf{0}, \mathbf{x}^2-\mathbf{x}\ y^2-y)$具有相同的复杂度。但我们知道， f_Δ 的所有倍数都是困难的。这就给出了一个 IPS 下界。

注 1.6。上述证明概要基本上证明了 定理 *1.5*在困难实例是非多线性的情况下成立。注意，多项式 Q_Δ 是多线性的，但困难实例在y中是非多线性的。我们扩展了上述概要中提出的思路，从而得到一个多线性的困难实例。

一个多线性困难实例。 我们工作的技术挑战在于设计一个多线性实例。我们之所以要寻找这样的实例，是因为：在代数证明复杂性中，目标是找到一个实例，其本身计算起来相当容易，但对它的反驳却很困难。衡量容易程度的方法有很多。不过，一种标准做法是要求困难实例为多线性。该领域几乎所有已知的困难实例都是多线性的。（例如，参见 [FSTW21；GHT22；HLT24b]。）事实上，由合取范式可满足性问题的代数编码自然得到的困难实例也是多线性的。

当我们要求实例是多线性的时，会遇到一些挑战。

使实例多线性化。如上所述，困难多项式 Q_Δ 来自 [LST21]已经是多线性的。然而遗憾的是，我们不知道如何给出 Q_Δ 本身在深度 Δ下的 IPS 反驳复杂度上界。为了解决这一问题，我们修改 Q_Δ，使得（新的）困难实例在布尔赋值下只取 $\mathcal{O}(1)$ 个不同的值。我们的上界证明依赖这一事实（见下文讨论）。如果多项式在布尔立方体上只取 0-1 值，我们的上界证明还会进一步简化。因此，我们在多项式的设计中融入了这两个性质：(a) 它是多线性的；(b) 它在布尔超立方体上只取布尔值。

我们从 Q_Δ （如定理 1.3所示）出发，并采用其常深度公式实现。在这个公式中，我们为每个寻址构件引入一个 $+$ 门。寻址构件是一种多线性多项式，其作用类似于多路复用器。当输入到该构件多项式的是 0-1 值时，它会激活加法门的一个输入，并抑制所有其他输入。因此，如果我们归纳地维持布尔立方体上所有门的求值均为 0-1 值，该构件就能让我们将这一性质传递到下一个门。

证明上界。 我们使用公式 C，它计算我们的困难多项式实例。根据多项式的构造，我们可以保证公式中的每个门在超立方体上取值为 0 或 1。利用这一事实，我们按公式的深度归纳，证明对于门 g，多项式 $g^2 - g$ 属于由 $\{g_i^2 - g_i\}_i$ 和布尔公理生成的理想，其中 $\{g_1、\ldots\ldots、g_t\}$ 是门 g 的输入。由此即可得到整体上界。

证明下界。 下界证明的思路是注意到，存在一个对构件变量的赋值，使得在该赋值下，困难实例等于困难多项式 Q_Δ，该多项式来自定理 1.3。由于这个多项式及其所有倍数都是困难的（由 [BKRRSS25]得出），我们使用倍数方法得到下界。

使用倍数方法（而非函数式方法）的优势在于，我们得到的是针对 IPS 的下界定理，而不仅仅是针对限制更严格的 IPS_{LIN}。

1.4 结果与技术：多线性-NC^1 与多线性-NC^2

本节陈述针对多线性-IPS 系统的分离定理。对于在布尔立方体上不可满足的多项式实例 $Q(\mathbf{x})$，我们称多项式 $G(\mathbf{x})$ 为函数式反驳，如果它满足 $G(\mathbf{x}) \cdot Q(\mathbf{x}) \equiv 1$ 模 $\mathbf{x}^2 - \mathbf{x}$。此外，如果 $G(\mathbf{x})$ 是多线性的，我们称其为多线性函数式反驳。我们证明以下定理。

定理 1.7 (多线性NC^1 与多线性NC^2-IPS)。 固定一个特征为0的域 $\mathbb{F}$。对于每个增长参数 $N \in \mathbb{N}$，都存在一个多线性多项式 $Q \in \mathbb{F}[x_1, \ldots, x_N]$，它在 $\{0,1\}^N$ 上不可满足，使得

1. 存在一个针对 $Q(\mathbf{x})$ 的多线性函数式反驳，例如 $G(\mathbf{x})$，它可由一个多项式规模且深度为 $O(\log^2 N)$ 的语法多线性电路计算。

2. 任何针对它的多线性-NC^1-$\text{IPS}_{\text{LIN}'}$ 都需要规模为 $N^{\Omega(\log N)}$。

注 1.8. 请注意，在上述定理中，下界适用于多线性-NC^1-$\text{IPS}_{\text{LIN}'}$。然而，上界并非多线性-NC^2-$\text{IPS}_{\text{LIN}'}$。相反，我们只能证明该反驳模布尔公理具有多线性-NC^2 电路。我们无法给出反驳布尔公理的复杂度界。尽管如此，我们相信上述结果带来了一些此前未知的结论。

- 多线性-NC^1-$\text{IPS}_{\text{LIN}'}$ 的下界自 *[FSTW21]* 的研究以来就已为人所知。其困难实例是一个 提升的子集和，即 $f(\mathbf{x}、\mathbf{z}) = \sum_{i,\ j} z_{i,\ j} x_i x_j$。我们注意到，它的函数式反驳相当困难。具体而言，它编码了布尔立方体上的团多项式。这意味着，除非 *VP* 等于 *VNP*，否则它不可能有小规模的函数式反驳。（见 附录 *A*）。

- 已知存在多线性IPS_{LIN} 和多线性$\text{IPS}_{\text{LIN}'}$ 的子系统，能够反驳有趣的不可满足实例（第 *4, [FSTW21]*节）。例如，它们能够反驳以下类型的子集和实例 $\sum_i \alpha_i x_i - \beta$，其中 α_i*s* 是 $O(1)$，而 β的选取使得该实例不可满足[3]。虽然这类实例具有多线性上界，但上界证明似乎严重依赖于子集和多项式的次数为1。考虑一个简单实例 $xy = 2$。这是一个布尔立方体上的不可满足实例。以下是它的一种反驳：

$$x^2y^2 - xy = x^2y^2 - x^2y + x^2y - xy = x^2(y^2 - y) + y(x^2 - x).$$

请注意，布尔公理 $y^2 - y$ 的反驳不是多线性的。（同一个例子还有另一种反驳，而在那种反驳中，另一个布尔公理的反驳不是多线性的。）事实上，这个例子的任何反驳都不是多线性的。（参见例 *4.7*

[3]它们允许稍微一般化的 α_is。更多详情请参见 [FSTW21] 中的命题 4.15。

中 *[FSTW21]*。）这表明，次数为2（或次数大于2）的困难实例未必一定有多线性证明。

- 我们的下界是通过函数方法得到的。这确保了我们实例的困难性可以归因于反驳该实例的困难性，而与反驳布尔公理的复杂度无关。因此，这一结果实现了对我们实例的函数式反驳的分离。

为了描述证明的各个组成部分，我们先从一个非常简单的例子开始。令 $z \in \{0, 1\}$。在这种情况下，很容易看出 $2 - z$ 不可满足，且 $2 - z \times \frac{1+z}{2} \equiv 1$ 模 $z^2 - z$ 成立。也就是说，$\frac{1+z}{2}$ 是在布尔公理模下对 $2 - z$ 的反驳。我们在证明中运用了这个思路。为了证明定理，我们再次构造一个多项式 $p(\mathbf{x})$，使其在布尔立方体上的取值为 0 或 1。于是，我们的不可满足实例为 $2 - p(\mathbf{x})$，其函数式反驳为$(1 + p(\mathbf{x}))/2$。

如果我们能够设计一个多线性多项式，使得

- 它由多线性 NC^2 电路计算，
- 任何计算它的多线性 NC^1 电路都需要 $N^{\Omega(\log N)}$ 规模，
- 并且它在布尔立方体上只取布尔值

那么我们就得到了分离结果。Raz 的一项著名工作 [Raz04] 给出了一个满足上述前两项性质的多项式。Raz 和 Yehudayoff 随后的工作 [RY08] 也提出了另一个候选多项式。遗憾的是，这两个多项式都不具备第三项性质。我们利用寻址构件对 [RY08] 中的多项式进行调整，以确保得到一个具备所有这些性质的多线性多项式。

该技术的适用性。 用于证明 定理 1.7的证明方法表明，它可以应用于其他场景。例如，同样的证明方法可以用于常深度层级定理的情形（如 定理 1.5所示）。上界保持不变，而下界则通过上述方法获得。这种方法可行，并将为 $\mathsf{IPS}_{\mathsf{LIN}}$ 给出下界，而非为IPS给出下界。

代数复杂性中还已知其他分离结果，尤其是在多线性情形下。例如， [RY09；CELS18]等人的结果。我们的证明方法可能适用于所有这些情形，从而针对 IPS 的不同子系统，得到源自这些分离结果的分离结果，正如我们从 Raz [Raz04；RY08]的分离结果证明了定理 1.7一样。

2 常深度层级

本节将证明定理 1.5。为此，我们从定理 1.3 中的困难多项式出发，并使用寻址构件对其进行修改。

在本节中，不失一般性地假设每个代数公式 C 都是分层的，且加法门和乘法门交替出现，顶层门为加法门。对于公式 $C(x_1, \ldots, x_N)$中的每个门 g，

- $f_g(x_1, \ldots, x_N)$ 表示在门 g处计算得到的多项式。
- 令 $\mathsf{depth}(g)$ 表示门 g 的深度，即从输入到该门的最长路径长度。令 $\mathsf{size}(g)$ 表示以 g 为根的子公式中的连线数。最后，令 $\mathsf{fanin}(g)$表示门 g 的扇入。

2.1 在求和门处添加寻址构件

在本小节中，我们为任意给定的代数公式定义一种修改，使得新公式在布尔输入上取值于 $\{0,\ 1\}$。此外，通过对新公式的变量进行偏求值，可以轻易地从新公式中恢复原公式所计算的多项式。

定义 2.1. 令 $n \in \mathbb{N}$。对于每个 $0 \leqslant j \leqslant n$，令 $t_n \in \mathbb{N}$ 表示满足$2^{t_n} > n$的最小 t_n 。令 $B_{n,\ 0}(j) \subseteq \{0$、$1$、...、$t_n\}$ 表示 $j + 2^{t_n}$ 的二进制表示中值为0 的索引。类似地，令 $B_{n,\ 1}(j) \subseteq \{0$、$1$、...、$t_n\}$ 表示 $j + 2^{t_n}$ 的二进制表示中值为 1 的索引集合。

j 在 n 中的寻址构件 定义如下

$$A_{n,j}(y_0, ..., y_{t_n}) = \prod_{i \in B_{n,0}(j)} (1 - y_i) \prod_{i \in B_{n,1}(j)} y_i.$$

注意，$A_{n,\ j}$对所有 $0 \leqslant j \leqslant n$ 都恰好使用一次相同的变量集 $\{y_0,\ .....,\ y_{t_n}\}$，因为 $j + 2^{t_n}$总是恰好使用 $j < 2^{t_n}$所需的 $t_n + 1$ 位。特别地，$A_{n,\ j}$ 是多线性的。

引理 2.2。 设 $n,\ j \in \mathbb{N}$满足 $0 \leqslant j \leqslant n$，并设 $(b_0,\ .....,\ b_{t_n}) \in \{0,\ 1\}^{t_n+1}$满足 t_n，其定义见 *Definition* 2.1。那么，对于任意特征为 $p \neq 2$ 的域，以下结论成立： $\mathbb{F}$,

1. $A_{n,j}(b_0, ..., b_{t_n}) = \begin{cases} 1 & \text{if } b_i = 0 \text{ for all } i \in B_{n,0}(j) \text{ and } b_i = 1 \text{ for all } i \in B_{n,1}(j), \\ 0 & \text{for all other choices of } (b_0, ..., b_{t_g}) \in \{0,1\}^{t_g+1} \end{cases}$
2. $A_{n,j}(\frac{1}{2}, \frac{1}{2}, ..., \frac{1}{2}, 2^{t_n}) = 1.$

证明。 1. 由构造可知，这一点显然。

2. 由于 $j + 2^{t_n}$的二进制表示中对应于 y_{t_n} 的位始终为 1，因此 y_{t_n} 是 $A_{n,\ j}$的一个因子。因此，求值变为

$$\left(\prod_{i \in B_{n,0}(j)} \left(1 - \frac{1}{2}\right) \prod_{i \in B_{n,1}(j) \setminus \{t_n\}} \frac{1}{2} \right) \cdot 2^{t_n} = \frac{1}{2^{t_n}} \cdot 2^{t_n} = 1,$$

因为$|B_{n,\ 0}(j)| + |B_{n,\ 1}(j) \setminus \{t_n\}| = t_n$。

■

下面的引理说明了如何应用这些寻址构件：

引理 2.3。 设 $C(\mathbf{x})$ 是一个规模为 s、深度为 Δ 、用于计算某个多项式$f(\mathbf{x})$的无常数公式。我们按如下方式构造一个新公式 $C'(\mathbf{x}, \mathbf{y})$，用于计算一个新多项式 $f'(\mathbf{x}, \mathbf{y})$:

对于任意加法门，

$$g(\mathbf{x}) = \sum_{j=0}^{\text{fanin}(g)-1} g_j(\mathbf{x})$$

属于 $C(\mathbf{x})$，我们将 g 替换为子电路，

$$g'(\mathbf{x}, \mathbf{y}_g) = \sum_{j=0}^{\text{fanin}(g)-1} g_j(\mathbf{x}) \cdot A_{g,j}(\mathbf{y}_g),$$

其中我们稍微滥用一下记号，将$A_{g,j} := A_{\text{fanin}(g)-1,j}$ 和 $t_g := t_{\text{fainin}(g)-1}$ 记作；并且$\mathbf{y}_g = \{y_{g,0}, ..., y_{g,t_g}\}$ 是为每个加法门 g新引入的一组变量。于是

$$\mathbf{y} = \bigcup_{g \text{ addition gate in } C(\mathbf{x})} \mathbf{y}_g,$$

其中 $|\mathbf{y}| = \mathcal{O}(s\log\ s)$。乘法门保持不变。

那么，对于任意特征为 $p \neq 2$ 的域 $\mathbb{F}$，以下结论成立：

1. 若$\mathbf{b}$ 是 $j + 2^{t_g}$ 作为向量的二进制表示，则 $g'(\mathbf{x},\mathbf{b}) = g_j(\mathbf{x})$ 。*2.* 对任意选择的 $(\mathbf{a}, \mathbf{b}) \in \{0,$ $f'(\mathbf{a}, \mathbf{b}) \in \{-1, 0, 1\}$ 。*3.* 存在$\mathbf{b} \in \mathbb{F}^{|\mathbf{y}|}$ 使得 $f'(\mathbf{x}, \mathbf{b}) = f(\mathbf{x})$。

4. $C'(\mathbf{x},\mathbf{y})$ 的规模为 $\mathcal{O}(s \log\ s)$，深度至多为 $2\Delta + 2$。

证明。 1. 这直接由 引理 2.2 得出。

2. 这直接由第 1 部分以及对电路层的归纳法得出。基础情形由 C 是无常数的假设得出。

3. 对于每个加法门， g'，我们令

$$\mathbf{b}_g = \left(\frac{1}{2}, \frac{1}{2}, \ldots, \frac{1}{2}, 2^{t_g}\right).$$

于是根据 引理 2.2 ，每个加法门 g'在此求值下变为

$$g'(\mathbf{x}, \mathbf{b}_g) = \sum_{j=0}^{\text{fanin}(g)-1} g_j(\mathbf{x}) \cdot A_{g,j}(\mathbf{b}_g) = \sum_{j=0}^{\text{fanin}(g)-1} g_j(\mathbf{x}) = g(\mathbf{x}).$$

4. 令n_g 表示门 g （加法或乘法）的扇入。由于 $A_{g,\ j}$ 可以由规模为 $\mathcal{O}(\log n_g)$ 的公式计算，并且对任意 g， $n_g \leqslant s$ ，因此我们得到 C' 的公式大小至多为 $\mathcal{O}(s\log\ s)$。

对于每个加法门 g，我们需要增加一个乘法层来相乘所有的 $g_j \cdot A_{g,\ j_0}$。由于 $A_{g,\ j}$ 的深度为 2，因此我们得到的深度至多为 $2\Delta + 2$。

■

引理 2.3 的第 3 部分 要求 $\mathbb{F}$ 的特征为 $p \neq 2$。该陈述的其余部分在任意域上均成立。

注 2.4. 如果 $C(\mathbf{x})$ 的输入门带有来自 $\mathbf{x} \cup \{0、1\}$，那么 $f'(\mathbf{a}、\mathbf{b}) \in \{0, 1\}$ 对于 $(\mathbf{a}、\mathbf{b}) \in \{0$ 的任意取值，$1\}^{|\mathbf{x}|+|\mathbf{y}|}$。特别地，这适用于 Q_Δ 中 定理 *1.3* 的公式。

2.2 证明

定理 定理 *1.5* 的证明。设 $\mathbb{F}$ 是一个特征为零的域，并固定任意深度 $\Delta \in \mathbb{N}$。设 $Q_\Delta \in \mathbb{F}[x_1、\ldots、x_n]$ 为 [LST21 定理 21] 中的多项式，满足以下条件：

1. 存在一个无常数代数公式，在深度 Δ、规模 s 下计算 Q_Δ。将其记为 $C(x_1、\ldots、x_n)$。

2. 对于每个计算 Q_Δ 的代数公式，若其深度为 $\Delta/2 - 1$，则其规模至少为 $s^{\omega(1)}$。

不可满足实例。设 $C(\mathbf{x})$ 是计算 $Q_\Delta(\mathbf{x})$ 的深度为 Δ 的公式。令 $C'(\mathbf{x}, \mathbf{y})$ 表示对 $C(\mathbf{x})$ 应用引理 2.3 中所述过程后得到的公式，并令 $f'_\Delta(\mathbf{x}, \mathbf{y})$ 表示由 $C'(\mathbf{x}, \mathbf{y})$ 计算得到的多项式。根据引理 2.3，C' 的深度为 $2\Delta + 2$，规模为 $\mathcal{O}(s\log\ s)$。定义多项式 f_Δ 为

$$f_\Delta(\mathbf{x}, \mathbf{y}) := f'_\Delta(\mathbf{x}, \mathbf{y}) - 2.$$

令 $(\mathbf{a}, \mathbf{b}) \in \{0、1\}^{|\mathbf{x}|+|\mathbf{y}|}$ 为 f'_Δ 中变量的任意布尔赋值。根据引理 2.3（以及注 2.4），我们得到 $f'_\Delta(\mathbf{a}, \mathbf{b}) \in \{0、1\}$，因此 $f_\Delta(\mathbf{a}, \mathbf{b}) \in \{-2、-1\}$。所以，$f_\Delta = 0$ 在布尔立方体上不可满足。令 C_Δ 表示一个深度为 $2\Delta + 2$、规模为 $s_\Delta = O(s\log\ s)$ 的 f_Δ 公式。
现在我们证明 f_Δ 满足 定理 1.5中所述的两个性质。也就是说，我们证明对 f_Δ的反驳的复杂度的上界和下界。

2.2.1 对 f_Δ的反驳的上界

本节专门用于证明以下引理。

引理 2.5 (上界**)**。设 $f_\Delta \in \mathbb{F}[\mathbf{x}、\mathbf{y}]$ 如上文所定义。存在一个深度为 $\Delta' = 4\Delta + 6$、规模为 $s' \leqslant 100s_\Delta^5$ 的常深度IPS 反驳。

为了证明该引理，我们对 C_Δ的结构使用归纳法。我们证明以下归纳引理，它蕴含 引理 2.5。

引理 2.6。设 g 是 C_Δ中的任意一个门。那么，

$$g^2 - g = \sum_{i=1}^{n} E_{g,i} \cdot (x_i^2 - x_i) + \sum_{j=1}^{m} F_{g,j} \cdot (y_j^2 - y_j),$$

其中 m 是$\mathbf{y}$ 变量的数量，并且

- 规模$(E_{g,\ i})$，规模$(F_{g,\ i})$ 至多为 $100 \cdot$(规模$(g))^4$，
- 且深度$(E_{g,\ i})$，深度$(F_{g,\ i})$ 至多为 $2 \cdot$深度(g)。

我们假设 引理 2.6 并证明 引理 2.5。我们知道 f'_Δ 可以由一个深度为 $2\Delta+2$ 且规模为 s_Δ的公式计算得到。根据 引理 2.6，我们知道存在多项式 E_j 和 F_j使得

$$(f'_\Delta)^2 - f'_\Delta \;=\; \sum_{j=1}^{n} E_j(\mathbf{x},\mathbf{y})\cdot(x_j^2 - x_j) \;+\; \sum_{j=1}^{m} F_j(\mathbf{x},\mathbf{y})\cdot(y_j^2 - y_j),$$

其中

- 对于每个 j，多项式 E_j 都可以用深度为 $2(2\Delta+2)$、规模为$100\cdot s_\Delta^4$的公式计算。
- 对于每个 j，多项式 F_j 都可以用深度为 $2(2\Delta+2)$、规模为$100\cdot s_\Delta^4$的公式计算。

由于 $f_\Delta = f'_\Delta - 2$，我们得到：

$$\frac{-1}{2}\left((f'_\Delta(\mathbf{x},\mathbf{y})+1)\cdot f_\Delta(\mathbf{x},\mathbf{y}) \;+\; \sum_{j=1}^{n} E_j(\mathbf{x},\mathbf{y})\cdot(x_j^2 - x_j) \;+\; \sum_{j=1}^{m} F_j(\mathbf{x},\mathbf{y})\cdot(y_j^2 - y_j)\right) \;=\; 1.$$

因此，我们得到了一个针对 f_Δ 的 IPS 反驳，其深度为 $2(2\Delta+2)+2$，规模至多为 $s_\Delta + O(1) + (n\cdot(100\cdot s_\Delta^4 + O(1)) + (m\cdot(100\cdot s_\Delta^4 + O(1)))$。由于 m 和 n 都被 s_Δ所界定，因此这个量被 $100 s_\Delta^5$所界定。至此，证明结束[4] 了引理 2.5。接下来，我们证明引理 2.6。

引理的证明 引理 2.6。我们将对 C_Δ的结构进行归纳来证明该命题。基础情形显然成立。对于归纳步骤，分两种情况：要么 g 是一个 $\times$门，要么是一个 $+$门。

情况 1：$g = \prod_{\ell=0}^{r-1} g_\ell$。

在这种情况下，

$$\begin{aligned} g^2 - g =& (g_0\cdot g_1\cdot\ldots\cdot g_{r-1})^2 - (g_0\cdot g_1\cdot\ldots\cdot g_{r-1}) \\ =& (g_0\cdot g_1\cdot\ldots\cdot g_{r-1})^2 - g_0(g_1\cdot\ldots\cdot g_{r-1})^2 + g_0(g_1\cdot\ldots\cdot g_{r-1})^2 - (g_0\cdot g_1\cdot\ldots\cdot g_{r-1}) \\ =& (g_0^2 - g_0)(g_1\cdot\ldots\cdot g_{r-1})^2 + \big((g_1\cdot\ldots\cdot g_{r-1})^2 - (g_1\cdot\ldots\cdot g_{r-1})\big) \end{aligned}$$

使用与上面相同的思路，即裂项求和，可得

$$g^2 - g = \sum_{\ell=0}^{r-1}\prod_{t<\ell} g_t\cdot\prod_{t>\ell} g_t^2\cdot(g_\ell^2 - g_\ell), \tag{2}$$

其中，t 的取值介于 0 和 $r-1$ 之间；若 $\ell=0$，则为$\prod_{t<\ell} g_t = 1$；若 $\ell = r-1$，则为$\prod_{t>\ell} g_t^2 = 1$。令 $H_\ell = \prod_{t<\ell} g_t\cdot\prod_{t>\ell} g_t^2$。注意，$H_\ell$的规模至多为 $2\cdot$规模(g)。根据关于 $g_\ell^2 - g_\ell$的归纳假设，可得

$$g^2 - g = \sum_{i=1}^{n}\underbrace{\sum_{\ell=0}^{r-1} H_\ell\cdot E_{g_\ell,i}}_{E_{g_i}}\cdot(x_i^2 - x_i) + \sum_{j=1}^{m}\underbrace{\sum_{\ell=0}^{r-1} H_\ell\cdot F_{g_\ell,i}}_{F_{g,j}}\cdot(y_j^2 - y_j)$$

[4]注意，w　　我们得到 Nullstellensatz 反驳的规模上界，从而得到 IPS_{LIN} 反驳的上界　　.

现在，上述表达式使我们能够如下界定 $E_{g\text{的规模和深度},\ i}$ 对每个 $i \in [n]$ 均如此；并界定 $F_{g\text{的规模},\ j}$ 对每个 $j \in [m]$ 均如此。

大小界。 在开始分析之前，我们回顾一下：我们用公式中的连线数量来衡量公式的规模。我们还给出参数的一些界。我们假设 $s_g > 1$。令 s_g 作为 $\mathsf{size}(g)$ 的简写；对于固定的 g，令 $s_{g,\ \ell}$ 表示$0 \leqslant \ell \leqslant r-1$的 $\mathsf{size}(g_\ell)$ 。

$$\sum_\ell s_{g,\ell} \leqslant (s_g - r) \text{ and } \sum_\ell s_{g,\ell}^4 \leqslant (s_g - r)^4 \tag{3}$$

此外，对于任意参数 $s > 1$，都有 $(s-1)^4 \leqslant s^4 - s^3/2$。

现在我们来界定 $E_{g,\ i}$的规模。为此，我们已经知道 H_ℓ 的规模至多为 s_g。我们还可以用归纳法界定$E_{g\ell,\ i}$ 的规模。因此，

$$\text{size of } E_{g,i} \leqslant \left(\sum_\ell 2s_g + 100s_{g,\ell}^4\right) + 3r \leqslant 3 \cdot s_g \cdot r + 3r + 100 \cdot (s_g - 1)^4.$$

类似地，也可以证明$F_{g,\ j}$的规模界。

第一个界来自应用关于 H_ℓ、 $E_{g\ell,\ i}$ 的界，并计算连入外层求和的连线数量。第二个界则来自使用 公式（3）以及$s_g - r \leqslant s_g - 1$这一事实。

$E_{g,\ i} \leqslant 6 \cdot s_g \cdot r + 100 \cdot s_g^4 - 100s_g^3/2 \leqslant 100 \cdot s^4$的规模。

深度上界。 深度$(E_{g,\ i}) \leqslant 2 \cdot (\text{深度}(E_{g\ell,\ i})) + 2 \leqslant 2 \cdot (\text{深度}(g) - 1) + 2 \leqslant 2 \cdot \text{深度}(g)$。$F_{g,\ i}$ 的深度也可以用类似的方法界定。

情形 2：$g = \sum_{\ell=0}^{r-1} g_\ell \cdot A_{g,\ \ell}$。

为了证明这一情形，我们将用到几个简单的引理。

引理 2.7。 </style}设 ，ℓ，则对于任意 ℓ, $(A_{g,\ \ell})^2 - (A_{g,\ \ell}) = \sum_{j=0}^{t_g} C_{\ell,\ j} \cdot (y_{g,\ j}^2 - y_{g,\ j})$，其中规模$(C_{\ell,\ j}) \leqslant 6 \cdot r$。

证明。 注意，附加到门 g的任意寻址构件只使用$\mathbf{y}_g$中的变量。具体而言，设该寻址构件为$A_{g,\ell}(\mathbf{y}_g) = \prod_{t \in Y} y_{g,t} \times \prod_{t \in Y'} (1 - y_{g,t})$, 其中，$\mathbf{y}_g$ 的索引被划分为 Y和 Y'。

于是，我们得到

$$(A_{g,\ell})^2 - (A_{g,\ell}) = \left(\prod_{t \in Y} y_{g,t} \times \prod_{t \in Y'} (1 - y_{g,t})\right)^2 - \left(\prod_{t \in Y} y_{g,t} \times \prod_{t \in Y'} (1 - y_{g,t})\right)$$

再次利用关于$\mathbf{y}_g$ 变量的伸缩求和思想，我们可以证明

$$(A_{g,\ell})^2 - (A_{g,\ell}) = \sum_{j=0}^{t_g} C_{\ell,j} \cdot (y_{g,j}^2 - y_{g,j})$$

其中，$C_{\ell,\ j}$ 由$\mathbf{y}_g$ 中的单项式组成，并且是一个关于$\mathbf{y}_g$ 变量的 $\Pi\Sigma$ 电路。乘积门的输入可以是以下几种情况之一：变量本身出现，或其平方出现，或作为$(1-y)$ 出现，或作为 $(1-y)^2$出现。每个线性因子的规模可由 $3\cdot t_g$ 界定，因此整体规模可由 $6\cdot t_g$界定。其上界为 $6\cdot r$。■

引理 2.8. 设 $g=\sum_{\ell=0}^{r-1} g_\ell\cdot A_{g,\ell}$，则对于任意 $\ell\neq\ell'$，存在 $j\in\{0,\ldots,t_g\}$，使得$A_{g,\ell}\times A_{g,\ell'}=C_{\ell,\ell',j}\cdot(y_j^2-y_j)$，其中 规模$(C_{\ell,\ell',j})\leqslant 6\cdot r$。

证明. 显然，对于 $\ell\neq\ell'$，必定存在一个变量 y_j，使得 y_j整除 $A_{g,\ell}$，且 $(1-y_j)$ 整除 $A_{g,\ell'}$，或者反之。因此，$y_j\cdot(1-y_j)$ 整除 $A_{g,\ell}\times A_{g,\ell'}$。因此，我们得到 $A_{g,\ell}\times A_{g,\ell'}=C_{\ell,\ell',j}\cdot(y_j^2-y_j)$，其中 $C_{\ell,\ell',j}$ 只是由一个关于 $\mathbf{y}_g$ 个变量的多项式构成的电路。与引理 2.7 中一样，这里同样得到规模$(C_{\ell,\ell',j})\leqslant 6\cdot r$。■

现在我们继续证明情形 2，即 g 为求和门的情形。我们再次分析g^2-g。

$$\begin{aligned}
g^2-g&=\left(\sum_{\ell=0}^{r-1} g_\ell\cdot A_{g,\ell}\right)^2-\sum_{\ell=0}^{r-1} g_\ell\cdot A_{g,\ell}\\
&=\sum_{\ell=0}^{r-1}(g_\ell\cdot A_{g,\ell})^2+\sum_{\ell\neq\ell'} g_\ell\cdot A_{g,\ell}\cdot g_{\ell'}\cdot A_{g,\ell'}-\sum_{\ell=0}^{r-1} g_\ell\cdot A_{g,\ell}\\
&=\sum_{\ell=0}^{r-1}(g_\ell\cdot A_{g,\ell})^2-\sum_{\ell=0}^{r-1} g_\ell\cdot(A_{g,\ell})^2+\sum_{\ell=0}^{r-1} g_\ell\cdot(A_{g,\ell})^2-\sum_{\ell=0}^{r-1} g_\ell\cdot A_{g,\ell}+\sum_{\ell\neq\ell'} g_\ell\cdot g_{\ell'}\cdot A_{g,\ell}\cdot A_{g,\ell'},
\end{aligned}$$

其中我们加上并减去了相同的量（第二个和第三个求和式）。重新整理后，我们得到

$$g^2-g=\sum_{\ell=0}^{r-1}\left(g_\ell^2-g_\ell\right)\cdot(A_{g,\ell})^2+\sum_{\ell=0}^{r-1} g_\ell\cdot\left(A_{g,\ell}^2-A_{g,\ell}\right)+\sum_{\ell\neq\ell'} g_\ell\cdot g_{\ell'}\cdot A_{g,\ell}\cdot A_{g,\ell'},$$

现在我们对第一项应用归纳法，并对引理 2.7 和引理 2.8 分别应用于第二项和第三项。

$$\begin{aligned}
g^2-g=&\sum_{i=1}^{n}\underbrace{\sum_{\ell=0}^{r-1}(A_{g,\ell})^2\cdot E_{g_\ell,i}}_{(E_{g,i})}\cdot(x_i^2-x_i)+\sum_{j=1}^{m}\underbrace{\sum_{\ell=0}^{r-1}(A_{g,\ell})^2\cdot F_{g_\ell,j}}_{(I)}\cdot(y_j^2-y_j)\\
&+\sum_{j=0}^{t_g}\underbrace{\sum_{\ell=0}^{r-1} C_{\ell,j}\cdot g_\ell}_{(II)}\cdot(y_j^2-y_j)+\underbrace{\sum_{\ell\neq\ell'} g_\ell\cdot g_{\ell'}\cdot C_{\ell,\ell',j}}_{(III)}\cdot(y_j^2-y_j)
\end{aligned}$$

利用这 个表达式，我们现在可以推导出反驳大小的规模和深度上界。

大小界。

现在我们将对上述表达式中的每一项进行界定。

对 $E_{g,i}$ 的规模进行界定。 $A_{g,\ell}$ 的规模可由 $2r$ 界定。每个 $E_{g_\ell,i}$ 的规模都可以通过归纳法界定。最后，输入到外层求和中的连线数可由 $3r$ 界定。因此，我们得到如下界

$$\begin{aligned}\text{size}(E_{g,i}) &\leqslant \sum_{\ell=0}^{r-1}(2r+100s_{g,\ell}^4)+3r \leqslant 2r^2+100\sum_{\ell}s_{g,\ell}^4+3r \leqslant 5r^2+100\sum_{\ell}s_{g,\ell}^4 \\ &\leqslant 5r^2+100(s-r)^4 \qquad \text{Using Equation (3)} \\ &\leqslant 5r^2+100s^4-100s^3/2 \leqslant 100s^4. \qquad \text{Using the bound on } s-r \text{ and } (s-1)^4\end{aligned}$$

对 $F_{g,i}$ 的规模进行上界估计。 $F_{g,i}$ 的规模上界可通过分析上文的项 (I)、(II) 和 (III) 得到。注意，项 (I) 的上界与 $E_{g,i}$ 的上界相同。因此，我们有

$$\text{size of (I)} \leqslant 5r^2+100\sum_{\ell}s_{g,\ell}^4 \qquad (a).$$

为了对 (II) 的规模进行上界估计，我们将使用引理 引理 2.7。可得

$$\text{size of (II)} \leqslant \left(\sum_{\ell}6\cdot r+s_{g,\ell}\right)+3\cdot r \leqslant 9r^2+\sum_{\ell}s_{g,\ell} \qquad (b)$$

最后，我们对 (III) 的规模进行上界估计。

$$\begin{aligned}\text{size of (III)} &\leqslant \left(\sum_{\ell\neq\ell'}6\cdot r+s_{g,\ell}+s_{g,\ell'}\right)+4\cdot r^2 \\ &= \sum_{\ell\neq\ell'}6\cdot r+\sum_{\ell\neq\ell'}s_{g,\ell}+\sum_{\ell\neq\ell'}s_{g,\ell'}+4\cdot r^2 \\ &\leqslant 6r^3+2r\sum_{\ell\neq\ell'}s_{g,\ell}+4r^2 \qquad (c)\end{aligned}$$

将 (a)、(b) 和 (c) 合并，并合并各项后可得

规模$(F_{g,i}) \leqslant 25r^3+3rs+100\sum_\ell s_\ell^4 \leqslant 25r^3+3rs+100(s-1)^4 \leqslant 25r^3+3rs+100s^4-100s^3/2 \leqslant 100s^4$

深度上界。 深度上界的推导与上文情形 1 中的推导类似。$\mathsf{depth}(E_{g,i}) \leqslant 2\cdot(\mathsf{depth}(E_{g_\ell,i}))+2 \leqslant 2\cdot(\mathsf{depth}(g)-1)+2 \leqslant 2\cdot\mathsf{depth}(g)$。$F_{g,i}$ 的深度也可以用类似方法进行界定。■

2.2.2 对 f_Δ 的反驳下界

本节重点研究常数深度 IPS 对 f_Δ 的反驳规模下界。回顾一下，$Q_\Delta(\mathbf{x})$ 表示 [LST21 定理 2 中的多项式，1] 并令 s表示计算 Q_Δ 的深度为 Δ 的电路规模。

引理 2.9 （下界）。令 f_Δ 如上所定义。每个深度为 $\Delta'' \leqslant \Delta/2-11$ 的常深度 IPS 反驳都需要规模为 $s'' = s^{\omega(1)}$。

证明。令 $C''((\mathbf{x}、\mathbf{y})、u、\mathbf{v}、\mathbf{z})$ 为 $f_\Delta(\mathbf{x}、\mathbf{y})$ 的 IPS 反驳。令 s'' 和 Δ'' 分别表示 C'' 的电路规模和深度。于是我们有以下事实：

1. 根据定义 $C''((\mathbf{x}、\mathbf{y})、0、\mathbf{0}、\mathbf{0})=0$ 以及 $C''((\mathbf{x}、\mathbf{y})、f_\Delta、\mathbf{x}^2-\mathbf{x}、\mathbf{y}^2-\mathbf{y})=1$ 因此，利用 [FSTW21，引理 6。1] 我们有

$$1-C''((\mathbf{x},\mathbf{y}),0,\mathbf{x}^2-\mathbf{x},\mathbf{y}^2-\mathbf{y})=f_\Delta\cdot h,$$

对于某个多项式 $h(\mathbf{x}、\mathbf{y})$。

2. 根据 [BKRRSS25，定理 1。1], 由 $1-C''((\mathbf{x}、\mathbf{y})、0、\mathbf{x}^2-\mathbf{x}、\mathbf{y}^2-\mathbf{y})$ 我们可以提取一个关于 $f_\Delta(\mathbf{x}、\mathbf{y})$ 其规模为多项式级，(s'') 且其深度至多为 $\Delta''+10$。

3. 根据 c onstruction of $f_\Delta(\mathbf{x}、\mathbf{y})$ 并根据 引理 2.3 存在某个 $\mathbf{b}\in\mathbb{F}^{|\mathbf{y}|}$ 使得

$$f_\Delta(\mathbf{x},\mathbf{b})=Q_\Delta(\mathbf{x}),$$

因此 an 在深度 $\Delta''+10$ 计算 f_Δ 的公式也会在深度 $\Delta''+10$ 计算 Q_Δ .

4. [LST21，定理 2。1]（亦见定理 1.3）指出，每个在深度 $\Delta/2-1$ 下计算 Q_Δ 的代数公式，其规模至少为 $s^{\omega(1)}$。

综合以上结果可知，若 $\Delta''+10\leqslant\Delta/2-1$，则 $C''((\mathbf{x}、\mathbf{y})、u、\mathbf{v}、\mathbf{z})$ 需要规模为$s^{\omega(1)}$。■

注释 2.10. 我们利用 *[BKRRSS25]* 近期的因式分解结果来证明我们的下界。不过，我们也想指出，在我们的情形下这并非必要。根据 *[CKS19]*, 的结果，已知由多项式规模的常深度电路/公式计算的任意多项式，其低次数因子也可由多项式规模的常深度电路/公式计算。由于 *[LST21]* 中的困难多项式以及我们的寻址构件次数都很低，我们的困难实例次数也很低（即相对于变量数量为对数级）。因此，它的所有因子次数也都很低。也就是说，*[CKS19]* 适用于我们的情形。

我们使用 *[BKRRSS25]*来呈现证明，因为如果未来能够得到更强的代数复杂性下界，这样做将有助于我们更直接地将证明策略推广到其他情形。

现在我们利用引理 2.5和引理 2.9 完成定理 1.5的证明。注意，针对IPS f_Δ 的反驳的深度为 $4\Delta+6$，规模为多项式规模(s)；而任何深度小于$\Delta/2-11$的电路都需要超多项式规模。因此，对于 $\Gamma=4\Delta+6$，我们得到 f_Γ具有一个深度为 Γ 的IPS反驳，而任何深度小于 $\Gamma/10$ 的IPS反驳都需要超多项式规模。至此，定理 1.5的证明完成。■

3 多线性分离定理

我们首先证明一个引理，它将在本节余下部分发挥作用。

引理 3.1。 设 $N\in\mathbb{N}$，并设 $\mathbf{x}=\{x_1,\ldots,x_N\}$。设 $f(\mathbf{x})$是一个多线性多项式，使得$f(\mathbf{a})\in\{0,1\}$对任意的 $a\in\{0,1\}^N$均成立，则

1. 下列恒等式成立。

$$(2-f(\mathbf{x}))\times\frac{1+f(\mathbf{x})}{2}\equiv 1\mod \mathbf{x}^2-\mathbf{x}$$

2. $2 - f(\mathbf{x}) = 0$ 在布尔立方体上不可满足。

3. 唯一满足 $g(\mathbf{x})$ 且 $g(\mathbf{x})(2 - f(\mathbf{x})) \equiv 1$ 模 $\mathbf{x}^2 - \mathbf{x}$ 的多线性函数是 $(1 + f(\mathbf{x}))/2$。因此，它与 $2 - f(x)$ 具有相同的多线性电路规模和深度。

证明。引理的第一部分很容易验证。若 $f(\mathbf{a}) = 1$，左侧的值为 1。类似地，当 $f(\mathbf{a}) = 0$ 时，它的值也为 1。第二部分成立，是因为我们假设 $f(\mathbf{x})$ 只取布尔值。最后，第三部分可直接由第一部分推出。■

3.1 多线性-NCNC^1 与多线性-NCNC^2-IPS

本节将证明 定理 1.7。

我们将构造一个多项式，使其可由多线性 NC^2 电路计算，且在布尔超立方体上只取布尔值。结合 引理 3.1，即可得到所需的分离结果。

记号。 令 $[n] = \{1,\ldots,n\}$，并令 $\mathbf{u} = \{u_1,\ldots,u_{2n}\}$ 和 $\mathbf{v} = \{v_{i,j,k}\}_{i,j,k\in[2n]}$。对于 $i,j \in [n]$，令 $[i,j]$ 表示区间 $\{k \mid i \leqslant k \text{ 和 } k \leqslant j\}$。令 $\ell([i,j])$ 表示该区间的长度，即 $j - i + 1$。当 $j < i$ 时，则有 $[i,j] = \varnothing$。

我们首先回顾由 [RY08], 定义的困难多项式，它是对 [Raz04], 定义的多项式的简化版本；该多项式展示了多线性公式与电路之间的第一个分离。

该多项式按如下方式归纳定义。对于 $i \in [n]$，令 $f_{i,i}(\mathbf{u},\mathbf{v}) = 1$。若 $\ell([i,j])$ 是一个大于 0 的偶数，则

$$f_{i,j}(\mathbf{u},\mathbf{v}) = (1 + u_i u_j) \cdot f_{i+1,j-1}(\mathbf{u},\mathbf{v}) \; + \sum_{r\in[i+1,j-1]} v_{i,r,j} \cdot f_{i,r}(\mathbf{u},\mathbf{v}) \cdot f_{r+1,j}(\mathbf{u},\mathbf{v})$$

最后，困难多项式为 $F(\mathbf{u},\mathbf{v}) = f_{1,2n}(\mathbf{u},\mathbf{v})$。他们证明了关于该多项式的以下定理。

引理 3.2 ([Raz04], [RY08])。设 $n \in \mathbb{N}$，并设 $\mathbf{u} = \{u_1,\ldots,u_{2n}\}$ 和 $\mathbf{v} = \{v_{i,j,k}\}_{i,j,k\in[2n]}$ 为两组变量。设 $F(\mathbf{u}、\mathbf{v})$ 为上述定义的多项式。则有以下结论。

1. $F(\mathbf{u}, \mathbf{v})$ 可以由一个规模为$\mathrm{poly}(n)$ 、深度为 $O(\log^2 n$的多线性电路计算).

2. 任何计算 $F(\mathbf{u}、\mathbf{v})$ 的多线性公式，其规模都必须为 $n^{\Omega(\log n)}$。

注记 3.3. 注意， $F(\mathbf{u}、\mathbf{v})$ 在布尔超立方体上求值时可能取很大的值。（事实上， $F(\mathbf{1}, \mathbf{1})$ 会随 n 呈指数增长。）为了使引理 *3.1* 适用，我们需要一个在超立方体上仅取布尔值的多项式。

我们通过修改 $F(\mathbf{u}、\mathbf{v})$来构造这样的多项式。我们使用一组新的构件变量来设计该多项式，并将其称为$\mathbf{w}$。这些变量有双重用途：首先，它们将帮助我们为 $+$ 门构造寻址构件；其次，它们将在 $F(\mathbf{u}、\mathbf{v})$的定义中充当$\mathbf{v}$ 变量。

令 $\mathbf{u} = \{u_1,\ldots,u_{2n}\}$。对于区间 $[i,j]$，令 $W^{[i,j]}$ 表示以下变量集合。

$$W^{[i,j]} = \{w^{[i,j]}_{\text{top}}\} \cup \{w^{[i,j]}_{\text{leaf}}\} \cup \tilde{W}^{[i,j]},$$

其中，$\tilde{W}^{[i,j]}$ 由我们将用于寻址构件的变量组成。回顾一下，对于 $n \in \mathbb{N}$，t_n表示满足 $2^{t_n} > n$ 的最小整数。令 $t_{i,j}$ 作为 $t_{\ell([i+1,j-1])}$ 的简写，并令 $n_{i,j}$ 作为 $\ell([i+1, j-1])$的简写。令 $\tilde{W}^{[i,j]} = \{w^{[i,j]}_r \mid 0 \leqslant r \leqslant t_{i,j}\}$。

最后，我们定义 $\mathbf{w} = \bigcup_{[i,j]} W^{[i,j]}$，其中并集遍历所有区间 $[i, j]$，其中 $1 \leqslant i < j \leqslant n$且 $\ell([i, j])$ 是偶数[5]。这里，任意集合 $W^{[i,j]}$的规模为 $O(\log n)$，因此我们有 $O(n^2 \log n)$ 个变量。我们用 $m(n)$表示$\mathbf{w}$ 和 m的基数，其中上下文已明确给出 n。

定义 3.4。困难多项式按如下方式归纳定义：若 $\ell([i, j]) = 0$，则 $p_{[i,j]}(u, w) = 1$。若 $\ell([i, j]) > 0$ 且为偶数，则

$$\begin{aligned} p_{i,j}(\mathbf{u}, \mathbf{w}) = \quad & (1 - w^{[i,j]}_{top}) \left((1 - w^{[i,j]}_{leaf}) + w^{[i,j]}_{leaf} \cdot u_i \cdot u_j \right) \times p_{i+1,j-1} \\ + \quad & w^{[i,j]}_{top} \times \left(\textstyle\sum_{r \in [i+1, j-1]} g_r(\tilde{W}^{[i,j]}) \times p_{i,r} \cdot p_{r+1,j} \right), \end{aligned}$$

g_r 是寻址构件，即

$$g_r(\tilde{W}^{[i,j]}) = \prod_{t \in B_{n_{i,j},0}(r)} (1 - w^{[i,j]}_t) \cdot \prod_{t \in B_{n_{i,j},1}(r)} w^{[i,j]}_t$$

这里，集合 $B_{n_{i,j},0}$ 和 $B_{n_{i,j},1}$ 的定义同 定义 *2.1*。

最后，$P(\mathbf{u}、\mathbf{w}) = p_{1,2n}(\mathbf{u}、\mathbf{w})$。

现在我们将证明，上文定义的多项式 $P(\mathbf{u}, \mathbf{w})$ 保留了多项式 $F(\mathbf{u}, \mathbf{v})$的性质，也就是说，它可由多线性电路计算，且对多线性公式而言很难。此外，我们还将证明，该多项式在布尔超立方体上仅取布尔值。形式化地说，我们证明以下定理。

定理 3.5。设 $n \in \mathbb{N}$ 并设 $\mathbf{u}$ 和 $\mathbf{w}$ 如上文所定义。另外，设 $P(\mathbf{u}, \mathbf{w})$ 为定义 *3.4* 中的多项式定义 *3.4*。那么，以下结论成立。

1. $P(\mathbf{u}、\mathbf{w}) \in \{0$在布尔超立方体上取值时为布尔值。*2.* $P(\mathbf{u}、\mathbf{w})$ 可由规模为 多项式 (n)、深度为 $O(对数^2\, n)$的多线性电路计算。

3. 任何计算 $P(\mathbf{u}、\mathbf{w})$ 的多线性公式，其规模都必须为 $n^{\Omega(\log n)}$。

在给出该定理的证明之前，我们将利用它来证明主要定理 定理 1.7，现将其重述如下。

定理 1.7（多线性 NC^1 对多线性NC^2-IPS）。固定一个特征为 0 的域 $\mathbb{F}$。对于每个增长参数 $N \in \mathbb{N}$，存在一个多线性多项式 $Q \in \mathbb{F}[x_1, \ldots\ldots, x_N]$，它在 $\{0、1\}^N$ 上不可满足，使得

1. 存在针对 $Q(\mathbf{x})$ 的多线性函数式反驳，例如 $G(\mathbf{x})$，它可由多项式规模且深度为 $O(\log^2 N)$ 的语法多线性电路计算得出。*2.* 对它的任何多线性-NC^1-$\mathsf{IPS}_{\mathsf{LIN}'}$ 都需要规模为 $N^{\Omega(\log N)}$。

[5]我们在归纳过程中只使用长度为偶数的区间。

定理 1.7 的证明。令 $N = n + m$，其中 n 是 $\mathbf{u}$ 的基数，m 是 $\mathbf{w}$ 的基数，并令 $\mathbf{x} = \mathbf{u} \cup \mathbf{w}$。我们将定义 $Q(\mathbf{x}) = 2 - P(\mathbf{x})$，其中 P 如定理 3.5 所述。显然，$Q(\mathbf{x})$ 在布尔超立方体上不可满足。根据引理 3.1，我们知道，$Q(\mathbf{x})$ 的反驳模布尔公理为 $((P(\mathbf{x})) + 1)/2$。因此，$Q(\mathbf{x})$ 的函数式反驳可由规模为 $\mathrm{poly}(n)$、深度为 $O(\log^2 n)$ 的多线性电路计算得出。

此外，根据 定理 3.5 我们知道，$P(\mathbf{x})$ 需要一个规模为 NC^1 的多线性电路 $n^{\Omega(\log n)}$。由于该反驳的规模为 $(P(\mathbf{x}) + 1)/2,$，我们还可得出，该问题的多线性 NC^1-$\mathsf{IPS}_{\mathsf{LIN}'}$ 反驳[6] 的规模必须为 $n^{\Omega(\log n)}$。由于 N和 n在多项式意义下等价，这也给出了多线性 NC^1-$\mathsf{IPS}_{\mathsf{LIN}}$ 反驳的证明大小下界。■

3.2 定理 3.5的证明

定理 3.5的第一部分。 我们利用 $P(\mathbf{u}、\mathbf{w})$ 的归纳结构来证明这一陈述。具体来说，我们将证明，对于任意区间 $[i, j]$，与之对应的多项式，即 $p_{i,j}(\mathbf{u}、\mathbf{w}) \in \{0, 1\}$，在布尔超立方体上求值。我们对区间的长度进行归纳。只需考虑长度为偶数的区间。

基础情形。 假设 $\ell([i, j]) = 0$ 那么该结论显然成立。

归纳步骤。 假设 $\ell([i, j]) > 0$。多项式 $p_{i,j}$ 的定义见 定义 3。4.
假设 $w^{[i,j]}$ 顶点 $= 0$，那么

$$p_{i,j} = \left((1 - w^{[i,j]}_{\text{leaf}}) + w^{[i,j]}_{\text{leaf}} \cdot u_i \cdot u_j\right) \cdot p_{i+1,j-1}.$$

注意，若 $w^{[i,j]}$ 叶子 $= 0$，则 $p_{i,j} = p_{i+1,j-1}$，根据归纳假设，它是布尔值。若 $w^{[i,j]}$ 叶子 $= 1$，则 $p_{i,j} = u_i u_j p_{i+1,j-1}$；当 u_i、u_j 和 $p_{i+1,j-1}$ 取布尔值时，该值为 0 或 1。
另一方面，若 $w^{[i,j]}$ 顶点 $= 1$，那么

$$p_{i,j} = \left(\sum_{r \in [i+1,j-1]} g_r(\tilde{W}^{[i,j]}) \times p_{i,r} \cdot p_{r+1,j}\right).$$

现在，假设集合 $\tilde{W}^{[i,\ j]}$ 中的变量被赋为 0 和 1，使得布尔赋值等于 $r + 2^{t_{i,\ j}}$，那么我们得到 $p_{i,\ j} = p_{i,\ r} \cdot p_{r+1,\ j}$。根据归纳假设，$p_{i,\ r} \in \{0,\ 1\}$ 以及 $p_{r+1,\ j} \in \{0,\ 1\}$。证明至此完成。

定理 3.5 的第二部分。注意，多项式 $F(\mathbf{u},\ \mathbf{v})$ 由 [RY08] 定义，与$P(\mathbf{u},\ \mathbf{w})$非常相似。不同之处在于，我们不是使用 $\mathbf{v}$ 个变量，而是通过寻址构件进行小规模的局部修改。寻址构件本身是常深度（无界扇入）多线性电路。显然，通过实现 $p(\mathbf{u},\ \mathbf{v})$的归纳定义，我们将得到一个多项式规模且多项式深度的多线性电路。利用 [RY08], 的深度缩减结果，我们可以得到一个用于该多项式的多项式规模、$O($对数$^2\, n)$深度多线性电路。

[6]由于我们使用函数方法，因此得到了 $\mathsf{IPS}_{\mathsf{LIN}'}$ 中的下界，而不仅仅是针对 $\mathsf{IPS}_{\mathsf{LIN}}$。

定理 3.5 的第三部分。首先，我们将证明，对于将$\mathbf{u}$中的变量划分为两个大小相等的集合的任意划分，设这两个集合为$\mathbf{u} = \mathbf{y} \cup \mathbf{z}$，矩阵$M_{\mathbf{y},\,\mathbf{z}}(p_{1,\,2n})$的秩等于$2^n$。这个界将进而推出 IPS 证明大小的下界。这一步相当标准，但为完整起见，我们仍将给出证明。

引理 3.6. 设$n \in \mathbb{N}$和$p_{1,\,2n}$如上所定义。那么，对于将$\mathbf{u}$划分为$\mathbf{y} \cup \mathbf{z}$且每部分基数均为$n$的任意划分，都存在一种将$\mathbf{w}$中的变量赋值为域常数的方法，使得秩$(M_{\mathbf{y},\,\mathbf{z}}(p_{1,\,2n})) = 2^n$。

证明。我们将对n使用归纳法来证明这一点。

基础情形。假设$n = 1$，则$p_{1,\,2} = \left((1 - w^{[1}_{,\,2]\text{叶子}}) + w^{[1}_{,\,2]\text{叶子}} \cdot u_1 \cdot u_2\right)$。令$w^{[1}_{,\,2]\text{叶子}} = 1/2,$，可得$p_{1,\,2} = \frac{1}{2} \cdot (1 + u_1 \cdot u_2)$，因此该结论显然成立。

归纳步骤。设$n > 1$。我们分两种情况讨论：u_1和u_{2n}要么在将$\mathbf{u}$划分为$\mathbf{y} \cup \mathbf{z}$时属于同一部分，要么属于不同部分。

u_1和u_{2n}位于不同部分。我们令$w^{[1,\,2n]\text{顶层}} = 0$和$w^{[1,\,2n]\text{叶子}} = 1/2$。在这一代换下，$p_{1,\,2n} = \frac{1}{2}(1 + u_1 \cdot u_{2n}) \cdot p_{2,\,2n-1}$。根据归纳假设，$p_{2,\,2n-1}$是满秩的，即对于其变量的任意等大小划分，$2^{n-1}$。而$(1 + u_1 u_{2n})$的秩为 2。还需注意，$p_{2,\,2n-1}$不使用变量$u_1$和$u_{2n}$。因此，这种情况下结论成立。

u_1和u_{2n}位于同一部分。在这种情况下，存在一个$r \in [i+1,\ j-1]$，使得区间$[1,\ r]$和$[r+1,\ 2n]$将$\mathbf{y}$变量和$\mathbf{z}$变量均匀划分。我们令$w^{[1,\,2n]\text{顶层}} = 1$，并将寻址构件中的变量设为$r + 2^{t_{i,\,j}}$的二进制编码。由此得到$p_{1,\,2n} = p_{1,\,r} \cdot p_{r+1,\,2n}$。对$p_{1,\,r}$，$p_{r+1,\,2n}$使用归纳法，并注意到这两个多项式没有共享任何变量，我们便得到$p_{1,\,2n}$的秩满足所需界限。■

参考文献

[和25] Robert Andrews. “VNC⁰中的代数伪随机性”。载于：第40届计算复杂性会议（CCC 2025）。Srikanth Srinivasan 编。第339卷。莱布尼茨信息学国际论文集（LIPIcs）。德国达格斯图尔：Schloss Dagstuhl – Leibniz-Zentrum f¨ur Informatik，2025年，15:1–15:15。 ISBN：978-3-95977- 379-9。 DOI：10.4230/LIPIcs.CCC.2025.15。 URL：https://drops.dagstuhl.de/entities/document/10.4230/LIPIcs.CCC.2025.15（引于第4页）。[AF22] Robert Andrews 和 Michael A. Forbes。“理想、行列式与标准化：证明并运用多项式理想的下界”。载于：第54届 ACM SIGACT计算理论年度研讨会论文集。STOC 2022。意大利罗马：计算机协会，2022年，第389–402页。 ISBN：9781450392648。DOI：10 .1145/ 3519935. 3520025。 URL：https : / / doi . org/ 10. 1145/3519935 . 3520025（引于第1、4页）。

[BLRS25] Amik Raj Behera、Nutan Limaye、Varun Ramanathan 和 Srikanth Srinivasan。“正特征下理想证明系统的新界”。载于：第52届自动机、语言与编程国际研讨会（ICALP 2025）。Keren Censor-Hillel、Fabrizio Grandoni、Jo¨el Ouaknine 和 Gabriele Pup-pis 编。第334卷。莱布尼茨信息学国际论文集（LIPIcs）。德国达格斯图尔：Schloss Dagstuhl – Leibniz-Zentrum f¨ur Informatik，2025年，22:1–22:20。ISBN：978-3-95977-372-0。 DOI：10 .4230 /LIPIcs .ICALP .2025 .22。 URL：https : // drops.dagstuhl.de/entities/document/10.4230/LIPIcs.ICALP.2025.22（引于第1、2页）。[BKRRSS25] Somnath Bhattacharjee、Mrinal Kumar、Shanthanu S. Rai、Varun Ramanathan、Ramprasad Saptharishi 和 Shubhangi Saraf。“Furstenberg的一项结果所蕴含的因式分解封闭性”。载于：CoRR abs/2506.23214（2025）。 DOI：10.48550/ARXIV. 2506.23214。arXiv：2506.23214（引于第4、6、15页）。[B¨ur98] Peter B¨urgisser。“代数复杂性理论中的完备性与归约”。载于：7（1998年8月）。 DOI：10.1007/978-3-662-04179-6_1（引于第23页）。[CGMS25] Prerona Chatterjee、Utsab Ghosal、Partha Mukhopadhyay 和 Amit Sinhababu。公式与只读代数分支程序之和的IPS下界。2025年7月。 DOI：10.48550/ arXiv.2507.09515。arXiv：2507.09515 [cs.CC]。 URL：https://arxiv.org/abs/ 2507.09515（引于第1页）。[CELS18] Suryajith Chillara、Christian Engels、Nutan Limaye 和 Srikanth Srinivasan。“小深度多线性电路的近最优深度层级定理”。载于：第59届IEEE计算机科学基础年会，FOCS 2018，法国巴黎，2018年10月7日至9日。Mikkel Thorup 编。IEEE计算机学会，2018年，第934–945页。 DOI：10.1109/FOCS.2018.00092。 URL：https://doi.org/10.1109/FOCS.2018.00092（引于第7页）。[CKS19] Chi-Ning Chou、Mrinal Kumar 和 Noam Solomon。“多项式因式分解的封闭性结果”。载于：计算理论15（2019），第1–34页。 DOI：10.4086/ TOC.2019.V015A013。 URL：https://doi.org/10.4086/toc.2019.v015a013（引于第15页）。[CR79] Stephen A. Cook 和 Robert A. Reckhow。“命题证明系统的相对效率”。载于：符号逻辑杂志44.1（1979），第36–50页。 DOI：10.2307/ 2273702（引于第1页）。[EGLT25] Tal Elbaz、Nashlen Govindasamy、Jiaqi Lu 和 Iddo Tzameret。有限域上理想证明系统的下界。2025年6月。 DOI：10.48550/arXiv. 2506.17210。arXiv：2506.17210 [cs.CC]。 URL：https://arxiv.org/abs/2506. 17210（引于第1、2页）。

[FSTW21] Michael A. Forbes、Amir Shpilka、Iddo Tzameret 和 Avi Wigderson。“证明复杂度下界源自代数电路复杂性”。载于：*Theory Comput.*17（2021年），第 1–88 页。 URL：https://theoryofcomputing.org/articles/v017a010/（引文见第1、2, 4–7, 15, 23）.

[GHT22] Nashlen Govindasamy、Tuomas Hakoniemi 和 Iddo Tzameret。“低深度代数证明的简单困难实例”。载于：*2022 年 IEEE 第 63 届年度研讨会计算机科学基础会议（FOCS）*。2022 年，第 188–199 页。 DOI：10.1109/FOCS54457.2022.00025（引自第1、2、5页）。

[GP18] Joshua A. Grochow 和 Toniann Pitassi。“电路复杂度、证明复杂度，以及多项式恒等式测试：理想证明系统”。载于：《*ACM*期刊》65.6（11月，2018年）。 ISSN：0004-5411。 DOI：10.1145/3230742。 URL：https://doi.org/10.1145/3230742（引自第1、2页）。

[HLT24a] Tuomas Hakoniemi、Nutan Limaye 和 Iddo Tzameret。“函数式下界载于《代数证明：对称性、提升与障碍》。第 *56* 届年度美国计算机协会计算理论研讨会。STOC 2024。加拿大不列颠哥伦比亚省温哥华，加拿大：计算机协会，2024 年，第 1396–1404 页。 ISBN：9798400703836。 DOI：10.1145/3618260.3649616。 URL：https://doi.org/10.1145/3618260.3649616（引自第 1 页）。

[HLT24b] Tuomas Hakoniemi、Nutan Limaye 和 Iddo Tzameret。“函数式下界代数证明中的函数式下界：对称性、提升与障碍”。载于：第 *56* 届计算理论年度美国计算机协会研讨会。STOC 2024。加拿大不列颠哥伦比亚省温哥华，加拿大：计算机协会，2024 年，第 1396–1404 页。 ISBN：9798400703836。 DOI：10.1145/3618260.3649616。 URL：https://doi.org/10.1145/3618260.3649616（引自第2、5页）。

[HS65] Juris Hartmanis 和 Richard E. Stearns。《关于算法的计算复杂性》。算法》。载于：美国数学会汇刊117（1965年5月），第285–306页。 ISSN：0002-9947。 DOI：10.2307/1994208 （引自第1页）。

[Has86] J Hastad。《小深度电路近乎最优的下界》。载于：会议录发表于第十八届 *ACM* 计算理论年度研讨会。STOC ’86。美国加利福尼亚州伯克利：计算机协会，1986 年，第 6–20 页。 ISBN：0897911938。 DOI：10.1145/12130.12132。 URL：https://doi.org/10.1145/12130.12132（引自第1页）。

[Juk12] Stasys Jukna。布尔函数复杂度：进展与前沿。《The-理论计算机科学。第 1–2 章综述香农下界和卢潘诺夫匹配上界，由此得出非一致电路规模层级。施普林格，2012 年。 ISBN：978-3-642-24507-7（引自第 1 页）。

[LST21] Nutan Limaye、Srikanth Srinivasan 和 S´ebastien Tavenas。“针对低深度代数电路的超多项式下界”。载于：*2021 IEEE 第 62 届计算机科学基础年会（FOCS）*论文集。2021 年，第 804–814 页。 DOI： 10.1109/FOCS52979.2021.00083 （引用于第 3–5、 10、 14、 15页）。

[LST25] Jiaqi Lu、Rahul Santhanam 和 Iddo Tzameret。*$AC^0[p]$-Frege* 无法高效地证明常深度代数电路下界很难。技术报告 TR25-134。计算复杂性电子研讨会（ECCC），9月。2025年。 URL： https://eccc.weizmann.ac.il/report/2025/134/ （引自第 1 页）。

[Raz04] Ran Raz。“多线性- $NC_1 \neq$ 多线性- NC_2”。载于：第*45*届年度会议论文集 *IEEE*计算机科学基础研讨会. FOCS '04. 美国：IEEE 计算机学会，2004年，第344–351页。 ISBN：0769522289。 DOI：10.1109/FOCS.2004.42。 URL：https://doi.org/10.1109/FOCS.2004.42（引自第3、7、16页）。

[RY08] Ran Raz 和 Amir Yehudayoff：《平衡句法多线性算术电路》。载于：计算复杂性 17.4（2008年12月），第515–535页。 ISSN：1420-8954. DOI： 10.1007/s00037-008-0254-0。 URL： https://doi.org/10.1007/s00037-008-0254-0（引用于第3、7、16、18页）。

[RY09] Ran Raz 和 Amir Yehudayoff。《常深度多线性电路的下界与分离》。英文。载于：计算复杂性 18.2（2009年6月），第171–207页。 ISSN：1016-3328。 DOI： 10.1007/s00037-009-0270-8 （引用于第7页）。

[ST21] Rahul Santhanam 和 Iddo Tzameret。“迭代下界公式：一种对角化方法，探讨证明复杂度”。载于：美国计算机协会第 *53* 届年度 *SIGACT* 计算理论研讨会（*STOC 2021*）。ECCC TR21-138；期刊版本发表于 *SIAM* 计算机杂志，2025年。美国计算机协会，2021年，第 234–247 页。 DOI： 10.1145/3406325.3451010（引自第1页）。

[Sha49] Claude. E. Shannon。 “双端开关电路的综合”。载于： *The Bell System* 技术期刊 28.1 (1949)，第 59–98 页。 DOI: 10.1002/j.1538-7305.1949.tb03624.x(引自第1页）。

[西普瑟 83] 迈克尔·西普瑟。“博雷尔集与电路复杂度”。载于：第十五届计算理论年度美国计算机协会研讨会。STOC '83。纽约市，美国：计算机协会，1983年，第61–69页。 ISBN：0897910990。 DOI： 10.1145/800061.808733。 URL：https://doi.org/10.1145/800061.808733（引文见第1页）。

[SHI65] Richard E. Stearns、Juris Hartmanis 和 Philip M. Lewis II。“存储层次结构受限计算”。收录于：第六届年度开关电路理论与逻辑设计研讨会（*FOCS*）。IEEE，1965年，第179–190页。 DOI： 10.1109/FOCS.1965.11（引自第1页）。

A 反驳提升的子集和的复杂度

设 $F(\mathbf{x}、\mathbf{z}) = \sum_{i<j\in[n]} z_{i,\ j}x_ix_j - \beta$是提升的子集和实例，其中 $\beta \in \Theta(n^3)$。显然，这是一个不可满足实例。FSTW [中使用了该实例21]，以证明多线性公式 IPS 的规模下界IPSLIN′。本文进一步分析反驳该实例的难度。我们证明，在一个标准的复杂性假设下，对该实例的反驳必须具有较高的复杂度。具体而言，我们证明如下结果。

引理 A.1. 若 $F(\mathbf{x}、\mathbf{z})$ 存在多项式规模的多线性 IPSLIN′ 反驳，则 VP $=$VNP。

这使得我们的困难实例在定理 1.7 中颇具意义。一方面，我们得到了与 [FSTW21], 中同样强的下界；另一方面，我们也为该实例的函数式反驳得到了一个相当好的上界。

为了证明该引理，我们先介绍一些记号和预备知识。令 $V \subseteq [n]$ 并令$K_V = \{(i、\ j) \mid i、\ j \in V、\ i < j\}$。令 $e = (i、\ j)$ 表示集合 K_V中的一个有序对，则我们用 z_e 表示$z_{i、\ j}$。

引理 A.2 （[B¨ur98]）。令 $C_\ell(\mathbf{x}、\mathbf{z})$ 为如下定义的团多项式 *ws.*

$$C_\ell(\mathbf{x},\mathbf{z}) = \sum_{V\subseteq[n],|V|=\ell} \prod_{e\in K_V} z_e \prod_{i\in V} x_i$$

$C_{n/2}(\mathbf{x}、\mathbf{z})$ 是 VNP 完全[7]的。

现在我们可以证明引理 A.1。

引理 *A.1* 的证明。我们引入一些记号。我们用 $\binom{[n]}{2}$ 表示集合 $\{(i、\ j) \mid i、\ j \in [n]、\ i < j\}$。令（不含提升的）子集和实例为

$$f(\mathbf{z}) = \sum_{(i,j)\in\binom{[n]}{2}} z_{i,j} - \beta = 0$$

对于 $\beta > n^2$

。（这个实例与 [FSTW21第 5]节中的子集和实例相同，只是重新标记了元素。）在[FSTW21命题 B.1], 中，他们给出了其多线性函数式反驳的显式描述，即精确计算了多项式 $g(\mathbf{z})$，使得

$$g(\mathbf{z}) = \frac{1}{\left(\sum_{(i,j)\in\binom{[n]}{2}} z_{i,j} - \beta\right)}, \qquad \text{for every } \mathbf{z} \in \{0,1\}^n.$$

他们证明，对于任意 $k \in [n]$，每个函数式反驳 $f(\mathbf{z})$ 都可以表示为次数为 k 的初等对称多项式的线性组合。更准确地说，他们证明了

[7] 来自 [¨ 98] $C_\ell(\ ) =$ Bur的团多项式与我们这里的多项式略有不同。具体来说，它是$\sum_{V\subseteq[n]} \prod_{e\in K_V} z_e$。不过，通过代入上面的多项式，我们可以得到这个多项式。

$$g(\mathbf{z}) = \sum_{k=0}^{n} \alpha_k \cdot \sum_{\substack{S \subseteq \binom{[n]}{2} \\ |S|=k}} \prod_{(i,j)\in S} z_{i,j}, \tag{4}$$

其中 α_k 是一个非零常数，只取决于 k 和 β。
现在，我们首先将输入实例改为 $F(\mathbf{x}, \mathbf{z}) = \sum_{(i,j)} z_{i,j} x_i x_j$，其中求和遍历集合 $\binom{[n]}{2}$。由于 $F(\mathbf{x}, \mathbf{z})$ 可以通过单项式代换 $z_{i,j} \mapsto z_{i,j} x_i x_j$从 $f(\mathbf{z})$ 得到，因此很容易看出， $F(\mathbf{x}, \mathbf{z})$ 的函数式反驳可以通过单项式代换从 $f(\mathbf{z})$ 的反驳中得到。这是因为我们只需在布尔立方体上保持反驳。这样的单项式代换可能会产生非多重线性多项式。令 $\mathsf{ml}[\cdot]$ 表示以下映射，该映射定义在一组变量（例如 $\mathbf{y}$）上的单项式上：$\mathsf{ml}\left[\prod_i y_i^{a_i}\right] = \prod_i y_{,i}^{\min\{a_i}$ $^{1\}}$。该映射线性扩展，并且可以定义为从 $\mathbb{F}[\mathbf{y}] \to \mathbb{F}[\mathbf{y}]$ 到任意多项式环$\mathbb{F}[\mathbf{y}]$的映射。

令 $G(\mathbf{x}、\mathbf{z})$ 表示 $F(\mathbf{x}、\mathbf{z})$的唯一多线性反驳。那么，利用公式（4）可得

$$G(\mathbf{x}, \mathbf{z}) = \sum_{k=0}^{n} \alpha_k \cdot \sum_{S \subseteq \binom{[n]}{2}, |S|=k} \mathsf{ml}\left[\prod_{(i,j)\in S} z_{i,j} x_i x_j\right]$$

假设我们认为 $F(\mathbf{x}、\mathbf{z})$ 具有多项式规模的 $\mathrm{IPS}_{\mathrm{LIN}'}$ 反驳。这意味着存在一个多项式规模的多线性电路，计算 $G(\mathbf{x}、\mathbf{z})$。我们进一步通过插值分离出 $\mathbf{z}$ 变量中的次数为 $\binom{n/2}{2}$的部分，并通过另一次插值分离出 $\mathbf{x}$ 变量中的次数为 n 的部分。显然，该电路计算出的多项式等于 $C_{n/2}(\mathbf{x}、\mathbf{z})$（相差一个系数的缩放）。假设 $\mathrm{VP} \neq \mathrm{VNP}$，这就产生了矛盾。■