arXiv:2304.11325v1 [cs.CC] 22 Apr 2023

有界顶层扇入深度 4 电路的确定性恒等式测试范式*

Pranjal Dutta† Prateek Dwivedi‡ Nitin Saxena†

摘要

多项式恒等式测试（PIT）是一个基础计算问题。Agrawal 和 Vinay（FOCS 2008）提出的著名深度 4 归约结果，使针对深度 4 电路的多项式恒等式测试成为一项引人注目的研究课题。计算形式为 $\sum_{i=1}^{k}\prod_j n$ 元、次数为 d 的多项式 ^{ij} 的受限深度 4 电路，其中 $_{ij} \leq \delta$，称为 $\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}$ 电路。进一步限制 g^{ij} 为单变量多项式之和，可得到 $\Sigma^{[k]}\Pi\Sigma\wedge$ 电路。关于常数 k 的 $\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}$ 以及 δ、 $\Sigma^{[k]}\Pi\Sigma\wedge$ 的特殊情形，大多仍未解决；过去二十年间，它们催生了许多重要思想。例如，Dvir 和 Shpilka（STOC 2005）、Kayal 和 Saxena（CCC 2006），以及 Saxena 和 Seshadhri（FOCS 2010 和 STOC 2011）提出的深度 3 思路。此外，还有 Beecken、Mittmann 和 Saxena（ICALP 2011）、Saha、Saxena 和 Saptharishi（Comput.Compl. 2013）、Forbes（FOCS 2015），以及 Kumar 和 Saraf（CCC 2016）提出的深度 4 思路。另外，Kayal 和 Saraf（FOCS 2009）、Shpilka（STOC 2019），以及 Peleg 和 Shpilka（CCC 2020、STOC 2021）提出了几何 Sylvester-Gallai 思路。最近，Limaye、Srinivasan、Tavenas（FOCS 2021）在下界方面取得突破，并据此为常数深度电路构造出了亚指数时间的 黑盒 多项式恒等式测试算法。本文解决了两个基础的相关开放问题。

我们给出了 $\Sigma^{[}$首个 多项式时间的多项式恒等式测试（PIT），用于$^{k]}\Pi\Sigma\wedge$。我们还为 $\Sigma^{[k]}\Pi\Sigma\wedge$ 和 $\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}$ 分别给出了首个 准多项式时间黑盒 多项式恒等式测试。三个算法的一个关键技术要点是，对数导数及其幂级数如何将顶层Π-门变换为 $\wedge$。

关键词 多项式恒等式测试、命中集、深度 4 电路。

2012 年 ACM 学科分类 计算理论 $\rightarrow$ 代数复杂性理论。

致谢 Pranjal 得到了“基于格密码学的基础理论”项目的资助，该项目由 NUS-NCS 网络安全联合实验室提供资金支持。Pranjal 的大部分工作是在访问印度理工学院坎普尔分校计算机科学与工程系期间完成的，并获得了 Google 博士奖学金的资助。Nitin 感谢 DST (SJF/MSA-01/2013-14)、SERB (CRG/2020/000045) 和 N. Rama Rao 教席提供的资金支持。

*预备版本发表于 36th 计算复杂性会议（CCC），2021年。 [DDS21a]

†新加坡国立大学计算学院。电子邮箱：duttpranjal@gmail.com

‡印度理工学院坎普尔分校计算机科学与工程系。电子邮箱： {pdwivedi,nitin}@cse.iitk.ac.in

目录

1 引言：PIT及其他 2

1.1 主要结果：绕道至三种确定性PIT的解析方法 3 1.2 相关模型的既有工作 4 1.3 技术与动机 7 1.3.1 DiDI技术 8 1.3.2 雅可比矩阵再度登场 8

2 预备知识 8

2.1 记号与定义 8 2.2 代数复杂性理论基础 9

3 白盒多项式恒等式测试

$\Sigma^{[k]}\Pi\Sigma\wedge$ 12 3.1 算法 20

4 深度4电路的黑盒多项式恒等式测试 20

4.1 $\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}$ 22 的多项式恒等式测试

4.2 $\Sigma^{[k]}\Pi\Sigma\wedge$ 26 的多项式恒等式测试

5 结论 27

1 引言：多项式恒等式测试及其延伸

代数电路是布尔电路自然的代数类比，其逻辑运算被替换为底层域上的 $+$ 和 $\times$ 运算。对代数电路的研究构成了代数复杂性这一庞大研究领域，其主要由 Valiant [Val79] 开创（并加以形式化）。代数复杂性中的一个核心问题是算法设计问题，即多项式恒等式测试（PIT）：给定一个域 $\mathbb{F}$ 上的代数电路 $\mathcal{C}$ 以及输入变量 $x_1, \ldots, x_n$，确定 $\mathcal{C}$ 是否计算出恒等于零的多项式。PIT 已在其他算法问题中得到广泛应用，并与之建立了诸多联系。相关例子包括：在图 [Lov79, MVV87, FGT19]，中寻找完美匹配的算法、素性测试 [AKS04]，、多项式因式分解 [KSS14, DSS22]，、多项式等价性 [DDOS14]，、重构算法 [KS06, Shp09, KS09]，以及代数自然证明的存在性 [CKR+20, KRST22]。此外，高效设计 PIT 算法与证明强下界有着内在联系 [HS80, Agr05, KI04, DSY10, FSV18, CKS18, DST21]。有趣的是，PIT 也出现在复杂性理论中的许多基础性结果中，例如 IP $=$ PSPACE [Sha92, LFKN92]，、PCP定理 [ALM+98, AS98]，，以及旨在实现 P类 $\neq$ NP类 [Mul12b, Mul12a, Gro15, JKY16] 的宏大几何复杂性理论（GCT）计划。

关于多项式恒等式测试问题，大致可以在两种设置下进行讨论。在 白盒设置中，我们可以查看电路的内部连线；而在 黑盒 设置中，我们

只能在给定定义域中的某些点对电路进行求值。针对这一问题，有一种非常简单的随机化算法——从足够大的定义域中随机选取一个点，并在该点对多项式进行求值。以极高的概率，非零多项式的求值结果将非零；这被广为人知地称为多项式恒等式引理 [Ore22，DL78，Zip79，Sch80]。如何去随机化这一算法，长期以来一直是一个悬而未决的问题。

多年来，人们仅知道针对计算稀疏多项式的深度-2电路的黑盒恒等性测试 [BOT88、KS01]。Agrawal 和 Vinay [AV08]的一项出人意料的结果表明，仅对深度 4 电路进行黑盒恒等式测试的完全去随机化（ΣΠΣΠ）就已经意味着对一般多项式恒等式测试问题的近乎完全去随机化。近期的深度约简结果 [Koi12、GKKS16], 以及自举现象[AGS19、KST19、GKSS22和20] 表明，即使是对非常受限的深度 4 电路（甚至 深度-3电路）进行多项式恒等式测试，也会对一般电路的多项式恒等式测试产生非常有趣的影响。这些结果使得深度 4 电路的恒等式测试成为一项极具意义的研究方向。

一次性完成三种多项式恒等式测试。 秉承同样的理念，我们在此解决三个重要且尚未解决的多项式恒等式测试问题。对于有界个单变量多项式之和的乘积之和电路 [SSS13，开放问题 2]，我们给出了首个确定性的多项式时间白盒多项式恒等性测试算法。此外，我们还为同一类电路给出了一个准多项式时间黑盒算法。这些电路记作 $\Sigma^{[k]}\Pi\Sigma\wedge$，并计算形如 $\Sigma_{i\in[k]}\Pi_j\left(g^{ij1}(x_1)+\cdots+g^{ijn}(x_n)\right)$ 的多项式。

> $\Sigma^{[k]}\Pi\Sigma\wedge$ 电路的白盒多项式恒等式测试可在多项式时间内完成，黑盒多项式恒等式测试则可在准多项式时间内完成。

一种类似的技术还可以为有界次数稀疏多项式之积的有界个和电路提供准多项式时间的黑盒多项式恒等式测试算法。它们记为 $\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}$（其中 k 和 δ 可以达到 $\mathrm{poly}(\log(s))$，其中 s 为电路规模）。

> $\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}$ 电路的黑盒多项式恒等式测试可在准多项式时间内完成。

$\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}$ 电路计算的多项式具有以下形式 $\Sigma_{i\in[k]}\Pi_j g^{ij}(\boldsymbol{x})$，其中 度$(g^{ij}) \leq \delta$。即使 $\delta = 2$ 也是一个棘手的未解决问题 [KS16，开放问题 2]。过去几年中，这一模型受到了广泛关注，并催生了许多重要成果 [PS20，PS21，GOS22，OS22]。

1.1 主要结果：绕道探讨三种多项式恒等式测试

尽管已有一些尝试来解决 $\Sigma^{[k]}\Pi\Sigma\wedge$上的多项式恒等式测试问题，但对于$k \geq 3$，即使在白盒设置下，高效的多项式恒等式测试仍然悬而未决，参见[SSS13、开放问题 2]。我们的第一个结果针对这一问题，设计了一种多项式时间算法（参见算法1）。在这一过程中，我们发现了一种基于解析方法而非理想的新技术，并将其称为DiDI。全文中，我们将在 $\mathbb{F} = \mathbb{Q}$上开展研究，不过所有结果对大特征域同样成立。

定理 1.1（白盒 $\Sigma^{[k]}\Pi\Sigma\wedge$ 多项式恒等式测试）。存在一种确定性的白盒 $s^{O(k7^k)}$ 时间多项式恒等式测试算法，可用于在 $\mathrm{x}]$ 上的规模为 s 的 $\Sigma^{[k]}\Pi\Sigma\wedge$ 电路。

备注。

1. 情形 $k \leq 2$ 可以通过调用 [SSS13，定理 5.2] 来解决；但 $k \geq 3$ 仍未解决。2. 我们的技术必然会使指数随k呈指数级增长。特别是，当$k = \Theta(\log s)$时，设计一种高效的时间算法将很有意义。3. 目前尚不清楚现有技术能否为 $\Sigma^{[k]}\Pi\Sigma\mathrm{M}_2$ 电路提供多项式恒等式测试；其中 $\Sigma\mathrm{M}_2$ 表示由计算出的双元单项式之和，并将其输入顶层乘积门。

接下来，我们转向黑盒设置，并讨论两个感兴趣的模型，即——$\Sigma^{[k]}\Pi\Sigma\wedge$和 $\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}$，其中$k$，$\delta$ 均为常数。我们的工作建立在针对无界顶层扇入的先前思路之上：(1) 雅可比矩阵 [ASSS16]，；(2) 已知的针对 $\Sigma\wedge\Sigma\wedge$和 $\Sigma\wedge\Sigma\Pi^{[\delta]}$ [GKS17 的黑盒多项式恒等式测试。对于15] ，我们采用解析方法，通过幂级数进行处理，这种方法出人意料地将顶层 Π门化为 $\wedge$门。

定理 1.2（黑盒深度 4 多项式恒等式测试）。

$_{T}^{(a)}$ 存在一个 这里有一个运行时间为 $s^{O(k\log_{\text{对数}} s)}$ 的黑盒多项式恒等式检验算法，适用于规模为 s 的 $\Sigma^{[k]}\Pi\Sigma\wedge$ 电路，其变量范围为 $\mathbb{F}[x]$ 。（b）存在一个 T 这里有一个运行时间为 $s^{O(\delta^2 k\log s)}$ 的黑盒多项式恒等式检验算法，适用于规模为 s、定义在 $\mathbb{F}[$ 上的 $\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}$ 电路 $\boldsymbol{x}]$.

备注。

1. 定理 1.2 (b) 的 依赖关系更优，但对 k 的依赖更差，相较于s而言，优于定理 1.1。即使 k 达到 $\delta =$ 多项式(对数s)，我们的结果仍能在准多项式时间内完成。2. 定理 1.2 (a) 优于定理 1.2 (b)，因为 $\Sigma\wedge\Sigma\wedge$ 的算法速度快于 $\Sigma\wedge\Sigma\Pi^{[\delta]}$。3. 即使对于 $\Sigma^{[3]}\Pi\Sigma\wedge$ 和 $\Sigma^{[3]}\Pi\Sigma\Pi^{[3]}$ 模型，我们仍未解决关于多项式时间黑盒问题。

1.2 相关模型的先前工作

在过去二十年中，针对有界深度代数电路的受限类（例如“局部”有界独立性、有界读取/出现次数、有界变量）的恒等式测试涌现出大量研究成果。关于具有有界顶层扇入的深度为 3 的电路（称为 $\Sigma^{[k]}\Pi\Sigma$-电路）的多项式恒等式测试，已有许多研究成果。Dvir 和 Shpilka [DS07] 给出了首个针对 $k = O(1)$ 的准多项式时间确定性白盒算法，该算法采用基于秩的方法，最终促使 Karnin 和 Shpilka [KS11] 设计出黑盒设置下复杂性相同的算法。Kayal 和 Saxena [KS07] 给出了首个多项式时间算法。随后，[SS11、SS12、SS13、ASSS16] 系列研究推广了该模型，并在乘积多项式的代数秩有界时给出了$n^{O(k)}$时间算法。注意

在白盒设置下，我们的算法为顶层扇入有界的深度-3电路给出了一个运行时间为 poly(s) 的多项式恒等式测试算法。此外，其对顶层扇入的依赖是指数级的。在黑盒设置下，我们的算法以准多项式时间 poly(s) 解决顶层扇入有界的深度-3电路的多项式恒等式测试问题，因此与已知的多项式时间算法相比并未带来任何加速。不过，我们的算法确实提出了一种不同于已知方法的多项式恒等式测试思路。

在受限类深度 4 电路的多项式恒等式测试方面，也取得了一些进展。[KMSV13], 提出了一种针对多线性 $\Sigma^{[k]}\Pi\Sigma\Pi$-电路的准多项式时间黑盒多项式恒等式测试算法，随后在 [SV18] 中将其进一步改进为一个运行时间为 $n^{O(k^2)}$ 的确定性算法。当每个乘法门中不可约因子的代数秩以及底层扇入均有界时，[BMS13, KS16] 给出了一种准多项式时间黑盒多项式恒等式测试算法。其他一些有趣的限制，例如变量数较少的乘积之和，以及更多结构性限制也得到了利用，参见 [FS13, ASS13, For15, Muk16, KS17]。通过关联几何，针对顶层和底层扇入有界的深度-4电路也取得了一些进展，参见 [Gup14, Shp19, PS20]。事实上，最近， [PS21] 针对 $\Sigma^{[3]}\Pi\Sigma\Pi^{[2]}$-电路提出了一种多项式时间黑盒多项式恒等式测试算法。

模型	Time	Ref.
$\Sigma^{[k]}\Pi^{[d]}\Sigma$	多项式（n, d^k）	[SS12]
多线性 $\Sigma^{[k]}\Pi\Sigma\Pi$	$\mathrm{poly}(n^{O(k^2)})$	[SV18， ASSS16]
$\Sigma\Pi\Sigma\Pi$ 超越次数有界	poly（s^{trdeg}）	[BMS13]
$\Sigma^{(k)}\Pi\Sigma\Pi^{[d]}$ 局部超越次数有界	QP(n)	[KS17]
$\Sigma^{[3]}\Pi\Sigma\Pi^{[2]}$	poly(n, d)	[PS21]
$\overline{\Sigma^{[k]}\Pi\Sigma\wedge}$	秒$_{O(k\cdot 7^k\cdot \text{对数 对数})}$	[DDS21b]
$\overline{\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}}$	$s_{O(\delta^2\cdot k\cdot 7^k\cdot \text{对数 } s)}$	[DDS21b]
$\Sigma\Pi\Sigma\Pi$	次指数级(n)	[LST21]
白盒 $\Sigma^{[k]}\Pi\Sigma\wedge$	$s^{O(k7^k)}$	本工作。
$\Sigma^{[k]}\Pi\Sigma\wedge$	<escape>$s^{O(k\log \text{日志 } s)}$</escape>	本文工作。
$\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}$	$s^{O(\delta^2\, k\log s)}$	本文工作。

表1：与 $\Sigma\Pi\Sigma\Pi$ 电路相关的多项式恒等式测试算法的时间复杂度比较

作者最近将其新颖的 DiDI技术推广到深度为 4 的电路的“边界多项式恒等式检验”问题 [DDS21b]。具体而言，他们分别为 $\overline{\Sigma^{[k]}\Pi\Sigma\wedge}$ 和 $\overline{\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}}$ 给出了一个 $s_{O(k\cdot 7^k\cdot \log\, logs)}$ 时间和 $s_{O(\delta^2\cdot k\cdot 7^k\cdot \log s)}$ 时间的黑盒多项式恒等式检验算法。根据定义，边界复杂度类刻画了精确的复杂度类，因此，边界多项式恒等式检验结果似乎涵盖了我们在本文中给出的结果。然而，这里的白盒多项式恒等性测试算法比他们的准多项式时间黑盒算法高效得多。此外，与他们呈指数级的依赖关系相比，黑盒多项式恒等式测试算法的时间复杂度对k 和 δ 的依赖关系更优。最后，

本文中的证明更加简单，因为我们不必处理边界复杂度类中多项式的无穷小近似。最近，Dutta 和 Saxena [DS22]证明了有界深度 3 电路的指数间隙扇入层级定理，该定理同样基于对 *DiDI*技术的更精细 推广。

Limaye、Srinivasan 和 Tavenas 的一项突破性成果 [LST21] 给出了常数深度电路的第一个超多项式下界。他们的下界结果与 [CKS18] 的“困难性与随机性”权衡结果相结合，得到了第一个针对一般深度 4 电路的确定性黑盒多项式恒等式测试算法，该算法对所有实数 $\epsilon > 0$ 的运行时间为 $O(n^{\epsilon}$s。他们的结果是针对深度 4 电路的首个亚指数时间多项式恒等式测试算法。此外，与他们的算法相比，我们的准多项式时间黑盒算法和多项式时间白盒算法快得多。

已知技术的局限性。人们只在附加限制下研究深度 4 多项式恒等式测试，这主要是因为现有技术的适用范围有限：这些技术是针对特定模型量身定制的，无法推广。例如，先前的方法处理的是 $\delta = 1$（即底层为线性多项式）或$k = 2$ （通过因式分解，[SSS13]）。而将$k = 2$ 改为 3，或将$\delta = 1$ 改为 2（即从“线性”变为“二次”），就已经需要采用本质上不同的方法。

白盒 $\Sigma^{[k]}\Pi\Sigma\wedge$ 模型推广了 [KS07] 著名的有界顶层扇入深度为 3 的电路 $\Sigma^{[k]}\Pi\Sigma$；但其中国剩余定理（CR）方法失去了适用性，因此甚至无法解决稍微更一般的模型。黑盒设置中也涉及类似的“认证路径”思想，见 [SS12]，可以将其视为一般化的 CR 方法。该方法构造了一个理想 I，使得 $f \neq 0$ 模 I，并最终通过常变量线性映射保留这一性质。由于理想 I 的生成元非线性增加，保留这一性质变得更加困难（对 $\Sigma^{[k]}\Pi\Sigma\wedge$ 和 $\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}$而言都是如此）。直观而言，通过基于理想的途径扩大 δ，会引向 Gröbner 基方法（其运行时间关于 n 为双指数级）[Vas04]。我们知道，即使是由 3 个生成元（类似地，$k = 4$）构成的理想，也已足以涵盖整个理想成员问题[Sap19b]。

用于解决 $\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}$ 的代数几何方法已在 [BMS13、Gup14、Muk16、Guo21]中得到探索。满足某种西尔维斯特–伽莱构形的族（称为 SG 电路）是更难的情形；据猜想，其超越次数为常数 [Gup14，猜想 1]。非 SG 电路对应的情形中，非零性认证路径问题可归约为根理想非成员关系问题 [GS20]。这本质上是一个簇问题，可以利用代数几何工具设计多项式时间黑盒多项式恒等式测试。事实上，最近 Guo [Guo21] 通过构造显式的簇规避子空间族，给出了一个 s^{δ^k} 时间的多项式恒等式测试。遗憾的是，理想非成员关系并非如此；这种情形使问题更难解决 $\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}$。从这个角度看，根理想成员关系很好地解释了为何直观的 $\Sigma^{[k]}\Pi\Sigma$ 方法无法推广到 $\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}$。

有趣的是，Forbes [For15] 利用移位偏导数技术，为 $\Sigma\wedge\Sigma\Pi^{[\delta]}$ 找到了准多项式时间的多项式恒等式测试算法；但如果将 $\wedge$门替换为 Π，这种方法会直接失效（因为“测度”会变得过大）。[Sax08] 的对偶技巧通过将其转换为只读无关紧要算术分支程序（ROABP），彻底解决了 $\Sigma\wedge\Sigma\wedge$的白盒多项式恒等式测试问题；但该方法不适用于

我们的顶层带有 ΠΠ门的模型（这是由于 Waring 秩和 ROABP宽度都很大）。从先验角度看，我们的模型与 ROABP 不可比，因此也无法期待 ROABP 著名的多项式恒等式测试算法 [FS13、FSS14、GKS17] 能发挥作用。

同样，直接应用 [ASSS16]中的雅可比矩阵和认证路径技术并不适用于我们的模型，因为很难为常变量归约构造出忠实映射。Kumar 和 Saraf [KS16] 关键地利用了所计算的多项式具有较低的单变量次数这一性质（因此可以调用 [DSY10] ）；而在 [KS17] 中，他们利用了顶层 ΠΠ-门以下所计算多项式的低代数秩。这两种性质对我们的模型一般都不成立。最近，Peleg 和 Shpilka [PS21] 通过关联几何（例如涉及“二次”多项式的 Edelstein-Kelly定理），解决了 $k = 3, \delta = 2$ 的 [Gup14, Conj. 1] ，从而给出了针对 $\Sigma^{[3]}\Pi\Sigma\Pi^{[2]}$ 的多项式时间黑盒多项式恒等式测试。即使推广到“三次”多项式（$\delta = 3 = k$），该方法似乎也相当难以推广。

针对其他模型的多项式恒等式测试。 许多受限模型已有黑盒多项式恒等式测试算法。例如，只读代数分支程序相关模型 [RS05、 JQS10、 AGKS15、 GKS17、 GKST17、 FSS14、 AFS+18]、对数变量电路 [FGS18、 BS21], 以及非交换模型 [GGOW16、LMP19]。

1.3 技术与动机

这两个证明都是解析性的，因为它们使用了对数导数及其幂级数展开，从而极大地变换了相应的模型。第一个证明具有归纳性，而第二个证明则是更直接的一次性证明。在这两种情况下，我们本质上都归约到广为人知的楔形模型；这些模型具有无界的顶层扇入，但已知可以对其进行多项式恒等式测试。这种归约出人意料，而且颇具“力量”。

我们所使用的解析工具，通过形式幂级数环 $R[[x_1, \ldots, x_n]]$ (简写为 $R[[x]]$) 出现在代数和复杂性理论中，参见 [Niv69、Sin19、DSS22]。环 $R[[x]]$ 的优点很多，它们通常源于逆元恒等式：$(1 - x_1)^{-1} = \sum_{i \geq 0} x_1^i$；该恒等式在 $R[x]$，中没有意义，但在 $R[[x]]$ 中成立。其他使用的解析工具受到朗斯基行列式（线性相关）[KPT15、定理 7] [KKPS15],雅可比矩阵（代数依赖）[BMS13、ASSS16、PSS18], 以及对数导数算子 $\mathrm{dlog}_{z_1}(f) = (\partial_{z_1} f)/f$ 的启发。

我们将使用除法运算符（例如，$R(z_1)$，其中 R 是某个环）。然而，除法并非免费的，因为它要求在整个过程中相对于 z_1 具有可逆性（再次使我们落入 $R[[z_1]]$。对于电路类 C,D ，我们定义类

$$\mathcal{C}/\mathcal{D} := \{f/g \mid f \in \mathcal{C}, \mathcal{D} \ni g \neq 0\}.$$

类似地， $\mathcal{C} \cdot \mathcal{D}$ to 表示分别取乘积的类。

1.3.1 DiDI技术

在定理 1.1 中，我们引入了一种设计多项式恒等式测试算法的新颖技术，该技术通过对输入电路归纳地应用两种基本运算，将其约化为一个更易处理的模型。假设我们希望测试 $\sum_{i\in[k]}T_i$? $= 0$，其中每个 T_i 均可由 ΠΣ∧计算。其核心思想是用 T_k 对其进行除法，得到 $1 + \sum_{i\in[k-1]} T_i/T_k$，然后再进行求导，将扇入约化至 $k - 1$，从而得到 $\sum_{i\in[k-1]} \mathcal{T}_i$。自然地，这些运算促使我们在分式环（例如，某个环 R 上的 $R(z_1)$）中开展工作；此外，由于 $\mathcal{T}_i$ 不再能由简单的 ΠΣ∧ 电路计算，这些运算也使模型发生了扭曲。然而，通过仔细的解析分析，我们证明了在约化后的模型中，非零性得以保持。随后，我们重复这一过程，直至达到 $k = 1$，同时维持有助于我们将非零性保持到最后的不变量。最后，我们通过证明约化模型的恒等式测试可以利用已知的多项式恒等式测试算法完成，从而结束证明。

1.3.2 雅可比矩阵再显威力

在定理 1.2 中，我们利用最初在 [BMS13] 中引入、随后在 [ASSS16] 中深入研究的雅可比多项式的强大作用，统一已知的多项式恒等式测试算法并设计新的算法。假设我们希望测试 $\sum_{i\in[k]}$ T_i ?$= 0$，其中 $T_i \in \Pi\Sigma\Pi^{[\delta]}$（分别为 ΠΣ∧）。我们将雅可比矩阵 $J(T_1,\ldots,T_r)$ 与 $T_1,\ldots,T_r$ 的代数独立性联系起来，并假设这些多项式构成 T_i 的一个超越基。我们设计一个降变量线性映射 Φ，它保持 $T_1,\ldots,T_r$ 的代数独立性，并证明对于任意 C：$C(T_1,\ldots,T_k) = 0 \iff C(\Phi(T_1),\ldots,\Phi(T_k)) = 0$。这种映射在 [ASSS16] 中被称为“忠实”映射。映射 Φ 最终为 $T_1 + \ldots + T_k$ 提供一个命中集，因为我们将问题归约为对一个仅含“少量”（大致等于 k 个）变量的多项式进行多项式恒等式测试，从而得到一个拟多项式时间算法。

2 预备知识

在证明结果之前，我们先介绍贯穿全文所使用的一些假设和记号。$\boldsymbol{x}$ 表示$(x_1,\ldots,x_n)$。$[n]$ 表示 $\{1,\ldots,n\}$。

2.1 记号与定义

- **对数导数**。在环 R 和变量y上，对数导数 $\mathrm{dlog}_y : R(y) \to R(y)$ 定义为 $\mathrm{dlog}_y(f) := \partial_y f/f$; 其中，$\partial_y$ 表示关于变量y的偏导数。对数导数的一个重要性质是，它在乘积上具有可加性

  as
  $$\mathsf{dlog}_y(f\cdot g) = \frac{\partial_y(f\cdot g)}{f\cdot g} = \frac{(f\cdot\partial_y g + g\cdot\partial_y f)}{f\cdot g} = \mathsf{dlog}_y(f) + \mathsf{dlog}_y(g).$$
  我们将这种效应称为乘积的线性化。

• **电路规模**。 稀疏度 $\mathrm{sp}(\cdot)$ 表示非零单项式的数量。在本文中，它是电路规模的一个参数。具体而言，规模$(g_1 \cdots g_s) = \sum_{i\in[s]} (\mathrm{sp}(g_i) + \deg(g_i))$，对于 $g_i \in \Sigma\wedge$ (分别为 $\Sigma\Pi^{[\delta]}$)。在白盒设置中，我们还将电路的位复杂度（即连线中所用常数的位复杂度）纳入规模参数。电路的一些复杂性参数包括深度 （层数）、语法次数 （任意节点所计算的多项式的最大次数）以及扇入 （节点的最大输入数量）。

• **命中集**。 点集 $\mathcal{H} \subseteq \mathbb{F}^n$ 称为一类 $\mathcal{C}$ 个变量的n元多项式的命中集，如果对于任意非零多项式$f \in \mathcal{C}$，都存在一个点属于 $\mathcal{H}$，使得f在该点取非零值。$T(n)$时间的命中集表示该命中集可在$T(n)$时间内生成，其中输入规模为n。

• **赋值**。 赋值是一个映射 $\mathrm{val}_y : \mathrm{R}[y] \to \mathbb{Z}_{\geq 0}$，定义在环 R 上，满足 $\mathrm{val}_y(\cdot)$ 被定义为整除该元素的 y 的最大幂次。它可以通过定义 $\mathrm{val}_y(p/q) := \mathrm{val}_y(p) - \mathrm{val}_y(q)$，将其轻松扩展到分式域 $\mathrm{R}(y)$；此时它可以为负值。

• **域**。 我们将底层域记为 $\mathbb{F}$，并假设其特征为 0。我们的所有结果也适用于其他域（例如 $\mathbb{Q}_p, \mathbb{F}_p$）在 大 特征下的情形（见第 3-4 节中的备注）。

• 雅可比矩阵。多项式组 $\mathrm{f} = \{\mathrm{f1}, \ldots, \mathrm{fm}\}$ 在 $\mathbb{F}[\mathrm{x}]$ 上的雅可比矩阵定义为矩阵 $\mathcal{J}\mathrm{x(f)} := \left(\partial \mathrm{xj}(\mathrm{fi})\right)_{\mathrm{m}\times\mathrm{n}}$。设 $\mathrm{S} \subseteq \mathrm{x} = \{\mathrm{x1}, \ldots, \mathrm{xn}\}$ 且 $|\mathrm{S}| = \mathrm{m}$。那么，多项式 JS(f) 表示 $\mathcal{J}$ x(f) 的子式（即子矩阵的行列式），该子矩阵由与 S 中变量对应的列构成。

2.2 代数复杂性理论基础

关于代数复杂性理论基础的详细讨论，我们建议读者参阅 [SY10, Sax09, Mah13, Sax14, Sap19a]。这里我们将正式陈述一些多项式恒等式测试结果以及电路的性质，以供后文参考。

平凡多项式恒等性测试算法

对于一般的任意电路，最简单的多项式恒等式测试算法源于多项式恒等式引理[Ore22, DL78, Zip79, Sch80]。当变量数量较少时，例如$O(1)$，该算法就非常高效。

引理 2.1 (平凡多项式恒等性测试)。对于一类具有 n 个变量、单变量次数为 $< d$ 的多项式 $f \in \mathbb{F}[\boldsymbol{x}]$，存在一种确定性多项式恒等式测试算法，其运行时间为 $O(d^n)$。

稀疏多项式

稀疏多项式恒等式测试是检验单项式数量有界的多项式是否恒等为零。关于稀疏多项式恒等式测试已有大量研究，感兴趣的读者可参阅 [BOT88、KS01] 及其中的参考文献。关于稀疏多项式恒等式测试的多项式时间击中集的证明，参见 [Sax09，定理 2。1]。

定理 2.2 (稀疏多项式恒等式测试映射 [KS01])。 设 $p(x) \in \mathbb{F}[x]$ 的单变量次数至多为 d，稀疏度至多为 m。则存在 $1 \leq r \leq (mn\log d)^2$,，使得

$$p(y, y^d, \ldots, y^{d^{n-1}}) \neq 0, \bmod y^r - 1.$$

如果 p 可由规模为 s 的 ΣΠ 电路计算，则存在一种确定性算法，可在时间 多项式(s,m) 内测试其是否为零多项式。

事实上，如果能高效地测试稀疏多项式的恒等性，那么也能高效地测试稀疏多项式乘积的恒等性。我们将其形式化如下：

引理 2.3 ([Sap13] 引理 2.3)。 对于一类 n 元、次数为 d 的多项式 $f \in \mathbb{F}[x]$，若其可由规模为 s 的 ΠΣΠ 计算，则存在一种确定性多项式恒等式测试算法，运行时间为 多项式(s,d)。

集合 $\mathcal{H} \subseteq \mathbb{F}^n$ 称为一类多项式的命中集 $\mathcal{C} \subseteq \mathbb{F}[x]$,，如果对于所有 $g \in \mathcal{C}$

$$g \neq 0 \iff \exists \boldsymbol{\alpha} \in \mathcal{H} : g(\boldsymbol{\alpha}) \neq 0.$$

在文献中，多项式恒等式测试与命中集密切相关，因为这两个概念已被证明是等价的（参见引理 3.2.9 和 3.2.10 [对于14]）。注意，集合 $\mathcal{H}$ 对该类中的每个多项式都有效。有时我们会使用这样的集合来替代多项式恒等式测试算法。

引理 2.4 （ΠΣ∧的命中集）。 对于一个由规模为 s 的 ΠΣΠ 计算的 n 元、次数为 d 的多项式类中的多项式 $f \in \mathbb{F}[x]$，存在一个规模为 $\mathrm{poly}(s,d)$ 的显式命中集。

代数分支程序（ABP）

ABP 是一个分层有向无环图，包含 $q+1$ 层顶点 $V_0, \ldots\ldots, V_q$，具有一个源点 a 和一个汇点 b，其中图中的所有边仅从 a 指向 V_0,，从 V_{i-1} 指向 V_i （对于任意 $i \in [q]$,），以及从 V_q 指向 b。边的权重是 单变量多项式。若 ABP 计算多项式

$$f(\boldsymbol{x}) = \sum_{p \in \mathsf{paths}(a,b)} \prod_{e \in p} W(e),$$

其中 W(e) 表示边 e 的权重。若 $|V_i| \leq w$, $\forall i \in \{0, \ldots\ldots, q\}$，则该代数分支程序的宽度为 w。等价地，代数分支程序计算的多项式可写为 $A^T(\prod_{i\in[q]} D_i)B$，其中 A、B $\in \mathbb{F}^{w\times 1}[x]$,，且 $D_i \in \mathbb{F}^{w\times w}[x]$,，其各项均为单变量多项式。建议感兴趣的读者参阅 [SY10、Mah13]，以了解更详细的讨论。

定义 2.5 （只读一次无关紧要算术分支程序（只读代数分支程序））。如果一个代数分支程序称为只读无关紧要

代数分支程序（只读代数分支程序），当其边权是在不同层上不同的变量的单变量多项式。形式化地说，存在集合 $[q]$ 上的一个排列 π，使得第 i 个矩阵 D_i 的各项都是变量 $x^{\pi(i)}$ 上的单变量多项式，也就是说，它们属于多项式环 $\mathbb{F}[x_{\pi(i)}]$。

如果对于变量的每一种排列 σ，都存在一个变量顺序为 σ、宽度为 {w} 的只读代数分支程序来计算多项式 $f(x)$，那么称多项式 $f(x)$可由任意阶的宽度为 {w} 的只读代数分支程序计算。在白盒设置中，任意阶只读代数分支程序的恒等式测试已经完全解决。

定理 2.6 (定理 2.4 [RS05])。对于由规模为 s 的只读代数分支程序计算的 n元多项式，可以构造一个规模为 $O(s^5 + s \cdot n^4)$ 的命中集。

关于只读代数分支程序的黑盒多项式恒等式测试，也已有不少结果 [FS13、FSS14、GKS 17]。目前已知的最佳算法可在准多项式时间内运行。

定理 2.7 (定理 4.9 [GKS17])。对于由任意阶宽度为 w 的只读代数分支程序计算的 n 元、个别次数为 d 的多项式，可以构造一个规模为 $(ndw)^{O(\log\log w)}$ 的命中集。

深度 4 电路

多项式 $f(x) \in \mathbb{F}[x]$ 可由 $\Sigma\wedge\Sigma\Pi^{[\delta]}$ 电路计算，当且仅当 $f(x) = \sum_{i\in[s]} f_i(x)^{e_i}$ 其中 $\deg f_i \le \delta$。该模型下第一个非平凡的多项式恒等式测试算法由 [For15]设计。

定理 2.8 (命题 4.18 [For15])。对于由规模为 s 的 $\Sigma\wedge\Sigma\Pi^{[\delta]}$-电路计算的 n 元、次数为 $(\le d)$ 的多项式 $f(x)$，存在一个规模为 $(nd)^{O(\delta\log s)}$的 $\mathrm{poly}(n, d, \delta\log s)$显式命中集。

类似地，$\Sigma\wedge\Sigma\wedge$ 电路计算形如 $f(x) = \sum_{i\in[s]} f^{e_i}$的多项式，其中 f_i 是单变量多项式之和。利用对偶技巧 [Sax08] 以及 [RS05、GKS17],中的多项式恒等式测试结果，可以为 $\Sigma\wedge\Sigma\wedge$ 电路设计高效的多项式恒等式测试算法。

引理 2.9 ($\Sigma\wedge\Sigma\wedge$-电路的多项式恒等式测试)。设 $P \in \Sigma\wedge\Sigma\wedge$ 的规模为 s。那么，存在一个多项式(s)（分别为 $s^{O(\log\log s)}$）时间的白盒（分别为黑盒）多项式恒等式测试。

证明概要。我们证明，任何 $g(x)^e = (g_1(x_1) + \ldots + g_n(x_n))^e$，其中 $\deg(g_i) \le s$，都可以写成 $\sum_j h^{j1}(x_1)\cdots h^{jn}(x_n)$ 的形式，其中某个 $h_{j\ell} \in \mathbb{F}[x_\ell]$ 的次数至多为 es。定义 $G := (y + g_1)\cdots(y + g_n) - y^n$。在它的 e 次幂中，注意到首项系数为 $\mathrm{coef}_{y^{e(n-1)}}(G^e) = g^e$。因此，在 $e(n-1)+1$ 个点 $(y = \beta_i \in \mathbb{F})$ 上进行插值，得到

$$\mathrm{coef}_{y^{e(n-1)}}(G^e) = \sum_{i=1}^{e(n-1)+1} \alpha_i\, G^e(\beta_i)\,.$$

现在，通过二项式展开来展开 $G^e(\beta_i) = ((\beta_i + g_1)\cdots(\beta_i + g_n) - \beta_i^n)^e$（不展开内部的 n 重乘积）。顶层扇入至多为 $s\cdot(e+1)\cdot(e(n-1)+1) = O(se^2n)$。中间单变量多项式的各项次数至多为 es。因此，它可以由一个规模至多为 $O(s^2e^3n)$ 的只读代数分支程序（任意顺序）计算。

现在，如果 $f = \sum_{j\in[s]} f^{e_j}$ 由一个规模为s的 $\Sigma\wedge\Sigma\wedge$ 电路计算，那么显然，f也可以由一个（任意顺序的）只读代数分支程序计算，其规模至多为$O(s^6)$。因此，白盒多项式恒等性测试随之成立。

来自定理 2.6，而黑盒多项式恒等式测试由定理 定理 2.7得出。 □

此外， $\Sigma\wedge\Sigma\wedge$ 可以证明其对乘法封闭，即两个多项式的乘积（每个多项式都可由一个 $\Sigma\wedge\Sigma\wedge$ 电路计算）可由单个 $\Sigma\wedge\Sigma\wedge$ 电路计算。为证明这一点，我们需要一种高效的方法，利用简单的插值，将少数几个幂的乘积写成若干幂之和。代数证明见 [CCG12，命题 4。3]。

引理 2.10 （单项式的华林恒等式）。 设 $M = x_1^{b_1}\cdots x^{b_k}{}_k$，其中 $1 \le b_1 \le \ldots \le b_k$，并且单位根 $\mathcal{Z}(i) := \{z \in \mathbb{C} : z^{b_i+1} = 1\}$。则，

$$M = \sum_{\varepsilon(i)\in\mathcal{Z}(i):i=2,\cdots,k} \gamma_{\varepsilon(2),\ldots,\varepsilon(k)} \cdot (x_1 + \varepsilon(2)x_2 + \ldots + \varepsilon(k)x_k)^d \ ,$$

其中 $d := \deg(M) = b_1 + \ldots + b_k$，且 $\gamma_{\varepsilon(2),\ldots,\varepsilon(k)}$ 是标量（$\mathrm{rk}(M) := \prod_{i=2}^{k}(b_i+1)$ 个）。备注。实际上，我们不必使用 $\mathbb{F} = \mathbb{C}$。对于次数为 d^k 的单项式，我们可以扩展到一个小的扩域（至多 d），以确保 $\varepsilon(i)$ 存在。

利用上述引理，我们证明闭包结果。

引理 2.11。 令 $f_i(x, y) \in \mathbb{F}[y][x]$, 的语法次数为 $\le d_i$，由一个 $\Sigma\wedge\Sigma\wedge$ 规模为 s_i 的电路计算，其中 $i \in [k]$ （关于 x）。那么，$f_1\cdots f_k$ 具有一个规模为 $O((d_2+1)\cdots(d_k+1)\cdot s_1\cdots s_k)$ 的 $\Sigma\wedge\Sigma\wedge$ 电路。

证明。设 $\mathrm{f}_i = \sum_j \mathrm{f}^{e_{ij}}\,\mathrm{ij}$；根据假设 $\mathrm{e}_{ij} \le \mathrm{d}_i$ （根据假设）。然后利用引理 2.10，对于指标 j_1, ...j_k，$\mathrm{f}\,\mathrm{e}_1{}_{1j_1}\mathrm{j}_1 \cdots \mathrm{f}\,\mathrm{e}^{\,kj_k}\mathrm{kj}_k$ 的规模至多为 $(\mathrm{d}_2+1)\cdots(\mathrm{d}_k+1)\cdot\left(\sum_{i\in[k]}\text{规模}(\mathrm{f}^{ji})\right)$。对所有 $\mathrm{s}_1\cdots\mathrm{s}_k$ 个乘积（至多）求和，即得上界。 □

3 $\Sigma^{[k]}\Pi\Sigma\wedge$的白盒多项式恒等式测试

我们考虑一种臃肿的计算模型，它自然地推广了 $\Sigma\Pi\Sigma\wedge$ 电路，并且能够理想地运用 DiDI 技术。

定义 3.1。 对于任意环 R，若参数为 k、规模为 s，且满足 $\mathcal{C} \in \Sigma^{[k]}(\Pi\Sigma\wedge/\Pi\Sigma\wedge)\cdot(\Sigma\wedge\Sigma\wedge/\Sigma\wedge\Sigma\wedge)$，则称电路 $\mathcal{C} \in \mathrm{Gen}(k,s)$（定义在 $\mathrm{R}(x)$ 上）。若 $f = \sum_{i=1}^{k} T_i$，则它计算 $f \in \mathrm{R}(x)$，其中

- $Ti =: (Ui/Vi)\cdot(Pi/Qi)$，其中 Ui、$Vi \in \Pi\Sigma\wedge$，且 Pi、$Qi \in \Sigma\wedge\Sigma\wedge$，
- $\mathrm{size}(T_i) = \mathrm{size}(U_i) + \mathrm{size}(V_i) + \mathrm{size}(P_i) + \mathrm{size}(Q_i)$，且 $\mathrm{size}(f) = \sum_{i\in[k]}\mathrm{size}(T_i)$。

显然，所有规模为s $\Sigma^{[k]}\Pi\Sigma\wedge$ 的电路都属于 $\mathrm{Gen}(k,s)$。我们将设计一个用于 $\mathrm{Gen}(k,s)$的递归算法。

定理 定理 *1.1*的证明。 首先定义 $T_{i,0} := T_i$ 和 $f_0 := f$，其中 $T_{i,0} \in \Pi\Sigma\wedge$; $\sum_i T_{i,0} = f_0$,和 f_0 的规模为 $\le s$。假设 $\deg(f) < d \le s$；我们将参数 d 单独保留，以便之后优化复杂性。在每次递归调用中，我们处理 $\mathrm{Gen}(\cdot,\cdot)$ 电路。

作为输入情形，定义$U_{i,0} := T_{i,0}$ 以及$V_{i,0} := P_{i,0} := Q_{i,0} := 1$。我们将利用稀疏多项式乘积的命中集（参见第2.2节）来获得一个点 $\boldsymbol{\alpha} = (a_1,\ldots,a_n) \in \mathbb{F}^n$

使得对于所有 $i \in [k]$，$U_{i,0}|_{x=\alpha} \neq 0$。最终，这个求值点将有助于维持 $\Pi\Sigma\wedge$ 的可逆性。考虑

$$g := \prod_{i\in[k]} T_{i,0} = \prod_{i\in[k]} U_{i,0} = \prod_{i\in[\ell]} \sum_{j\in[n]} f_{ij}(x_j),$$

其中，$f_{ij}(x_j)$ 是次数至多为 d 的单变量多项式，且 $\ell \leq k \cdot s$。注意，$\deg g \leq d \cdot k \cdot s$，且 g 可由规模为 O(s) 的 $\Pi\Sigma\wedge$ 电路计算。调用引理 2.4 得到一个命中集 $\mathcal{H}$，然后在 $\mathcal{H}$ 的每个点上对 g 求值，以找到一个元素 $\alpha \in \mathcal{H}$，使得 $g(\alpha) \neq 0$。我们强调，在白盒设置中，所有 $U_{i,0}$ 都可直接用于求值。由于该集合的规模为 poly(s)，且每次求值需要 poly(s) 时间，这一预处理步骤将为总时间复杂性增加 poly(s) 时间。此外，我们得到具有所需性质的 $\alpha \in \mathbb{F}^n$。

为刻画非零性，考虑一个 1-1 同态 $\Phi: \mathbb{F}[x] \longrightarrow \mathbb{F}[x,z]$，使得$x_i \mapsto z \cdot x_i + a_i$，其中 a_i 是先前得到的 α 的第i 个坐标。可逆性意味着$f_0 = 0 \iff \Phi(f_0) = 0$。现在我们继续递归算法，首先将恒等式测试从顶层扇入k 降至$k-1$。注意：$k = 1$ 是平凡的。

第一步：从 k 到 $k-1$的高效归约

By a设 $\sum_{i=1}^{k} T_{i,0} = f_0$ 和 $T_{k,0} \neq 0$。对两边应用 Φ，然后相除并求导 e:

$$\begin{aligned}
\sum_{i\in[k]} T_{i,0} = f_0 &\iff \sum_{i\in[k]} \Phi(T_{i,0}) = \Phi(f_0) \\
&\iff \sum_{i\in[k-1]} \frac{\Phi(T_{i,0})}{\Phi(T_{k,0})} + 1 = \frac{\Phi(f_0)}{\Phi(T_{k,0})} \\
&\implies \sum_{i\in[k-1]} \partial_z\left(\frac{\Phi(T_{i,0})}{\Phi(T_{k,0})}\right) = \partial_z\left(\frac{\Phi(f_0)}{\Phi(T_{k,0})}\right) \\
&\iff \sum_{i=1}^{k-1} \frac{\Phi(T_{i,0})}{\Phi(T_{k,0})} \cdot \mathrm{dlog}_z\left(\frac{\Phi(T_{i,0})}{\Phi(T_{k,0})}\right) = \partial_z\left(\frac{\Phi(f_0)}{\Phi(T_{k,0})}\right). \qquad (3.2)
\end{aligned}$$

下文中，除非另有说明，dlog 均表示对数微分$_z$。定义如下：

- $R1 := \mathbb{F}[z]/\langle z^d \rangle$。注意，方程 3.2 在 $R1(x)$上成立。~
- $T_{i,1} := \Phi(T_{i,0})/\Phi(T_{k,0}) \cdot$ 对数微分$(\Phi(T_{i,0})/\Phi(T_{k,0}))$，$\forall i \in [k-1]$。
- $f_1 := \partial_z(\Phi(f_0)/\Phi(T_{k,0}))$，在 $R1(x)$上。

可定义性 $T_{i,1}$ 和 f_1。 </style}很容易看出，这些都是定义良好的项。这里，我们强调，我们并不将 $T_{i,1}$ 精确地计算或存储为一个分式（其中 z 的次数为 $< d$）；相反，它被计算为 $\mathbb{F}(z,x)$ 中的一个元素，其中 z 是一个形式变量。形式上，我们

~计算 $T_{i,1} \in \mathbb{F}(z,\boldsymbol{x})$，使得 $T_{i,1} = T_i$,1 在 $\mathrm{R}_1(\boldsymbol{x})$ 上。我们跟踪 z 在 T_i,1 中的次数。因此，$\sum_{i\in[k-1]} T_{i,1} = f_1$，在 $\mathrm{R}_1(\boldsymbol{x})$ 上。

“当且仅当”条件。为了证明我们的 DiDI 一步归约到了 Gen(k $-1,\cdot$) 的恒等式测试，我们需要一个 $\Longleftrightarrow$ 条件。到目前为止，等式 3.2 在 R_1(x) 上是单向成立的。注意，$\mathrm{f}_1 \neq 0$ 蕴含 $\mathrm{val}_z(\mathrm{f}_1) < \mathrm{d} =: \mathrm{d}_1$。根据假设，$\Phi(\mathrm{T}_k,0)$ 在 R_1(x) 上可逆。此外，$\mathrm{f}_1 = 0$ 在 R_1(x) 上，这意味着 –

1. 或者，$\Phi(\mathrm{f}_0)/\Phi(\mathrm{T}_k,0)$ 不含 z。则 $\Phi(\mathrm{f}_0)/\Phi(\mathrm{T}_k,0) \in \mathbb{F}$(x)，进一步可知它属于 $\mathbb{F}$，这是因为映射 Φ（不含 z 蕴含不含 x，只需代入 z $= 0$）。另外注意，$\mathrm{f}_0, \mathrm{T}_{k,0} \neq 0$ 蕴含 $\Phi(\mathrm{f}_0)/\Phi(\mathrm{T}_k,0)$ 是 $\mathbb{F}$ 中的非零元素。因此，只需检查 $\Phi(\mathrm{f}_0)|_{z=0}$ 是否为非零。

2. 或者，$\partial_z(\Phi(f_0)/\Phi(T_k,0)) = z^{d_1} \cdot p$ 其中 $p \in \mathbb{F}(z,\boldsymbol{x})$ 使得 $\mathrm{val}_z(p) \geq 0$。通过简单的幂级数展开，可以证明$p \in \mathbb{F}(x)[[z]]$。

引理 3.3 (赋值)。设 $f \in \mathbb{F}(\boldsymbol{x},\boldsymbol{y})$ 满足 $\mathrm{val}_y(f) \geq 0$。那么，$f \in \mathbb{F}(\boldsymbol{x})[[\boldsymbol{y}]] \cap \mathbb{F}(\boldsymbol{x},\boldsymbol{y})$。

证明概要。设 f $=$g/h，其中 g、h $\in \mathbb{F}$[x, y]。现在，val_y(f) ≥ 0，这意味着 val_y(g) $\geq \mathrm{val}_y$(h)。令 val_y(g) $= \mathrm{d}_1$，且 val_y(h) $= \mathrm{d}_2$，，其中 $\mathrm{d}_1 \geq \mathrm{d}_2 \geq 0$。写作 g $= \mathrm{y}^{d_1} \cdot \tilde{}\mathrm{g}$，h $= \mathrm{y}^{d_2} \cdot \tilde{}$ h。写作，$\tilde{}$h $= \mathrm{h}_0 + \mathrm{h}_1\,\mathrm{y} + \mathrm{h}_2\,\mathrm{y}^2 +$。..... $+ \mathrm{h}_d\,\mathrm{y}^d$，其中 d 为某个值。注意 $\mathrm{h}_0 \neq 0$。因此，

$$\begin{aligned} f &= y^{d_1-d_2} \cdot \tilde{g}/(h_0 + h_1\,y + \ldots + h_d\,y^d) \\ &= y^{d_1-d_2} \cdot (\tilde{g}/h_0) \cdot (1 + (h_1/h_0)\,y + \ldots + (h_d/h_0)\,y^d)^{-1} \in \mathbb{F}(\boldsymbol{x})[[y]]\,. \end{aligned}$$

最后一个结论由幂级数环中的逆元恒等式得出。 □

因此，$\Phi(f_0)/\Phi(T_k,0) = z^{d_1+1} \cdot q$ 其中 $q \in F(\boldsymbol{x})[[z]]$, 即。

$$\Phi(f_0)/\Phi(T_{k,0}) \in \langle z^{d_1+1} \rangle_{\mathbb{F}(\boldsymbol{x})[[z]]} \implies \mathrm{val}_z(\Phi(f_0)) \geq d+1,$$

一个矛盾。

反之，显然$f_0 = 0$ 蕴含$f_1 = 0$。因此，我们证明了以下内容

$$\sum_{i\in[k]} T_{i,0} \neq 0 \text{ over } \mathbb{F}[\boldsymbol{x}] \Longleftrightarrow \sum_{i\in[k-1]} T_{i,1} \neq 0 \text{ over } \mathrm{R}_1(\boldsymbol{x}),\ \text{or},\ 0 \neq \Phi(f_0)|_{z=0} \in \mathbb{F}\,.$$

最终，我们证明，$\mathrm{R}_1(\boldsymbol{x})$ 上的 $T_{i,1} \in (\Pi\Sigma \wedge / \Pi\Sigma\wedge) \cdot (\Sigma\wedge\Sigma\wedge / \Sigma\wedge\Sigma\wedge)$，其规模仅有多项式级膨胀（命题 3.6）。因此，上述电路属于 $\mathrm{R}_1(\boldsymbol{x})$ 上的 $\mathsf{Gen}(k-1,\cdot)$，我们对其递归处理，最终得到恒等式测试。接下来的步骤会稍微复杂一些：

归纳步骤

假设我们处于第j步（$j \geq 1$）。我们的归纳假设为——

1. $\sum_{i\in[k-j]} T_{i,j} = f_j$，定义在 $\mathrm{R}j(\boldsymbol{x})$ 上，其中 $\mathrm{R}j := \mathbb{F}[z]/\langle z^{d_j}\rangle$，对于 $dj < d$，且 $T_{i,j} \neq 0$。2. $\mathrm{val}_z(T_{i,j}) \geq 0, \forall i \in [k-j]$。

3. 非零保持当且仅当条件

$$f \neq 0, \text{over } \mathbb{F}[\boldsymbol{x}] \iff f_j \neq 0, \text{ over } \mathsf{R}_j(\boldsymbol{x}), \quad \text{or} \bigvee_{i=0}^{j-1} ((f_i/T_{k-i,i})|_{z=0} \neq 0, \text{over } \mathbb{F}(\boldsymbol{x}))$$

4. 此处，$\mathrm{T}_{i,j} =: (\mathrm{U}_{i,j}/\mathrm{V}_{i,j}) \cdot (\mathrm{P}_{i,j}/\mathrm{Q}_{i,j})$，其中 $\mathrm{U}_{i,j}$、$\mathrm{V}_{i,j} \in \Pi\Sigma\wedge$ 以及 $\mathrm{P}_{i,j}$、$\mathrm{Q}_{i,j} \in \Sigma\wedge\Sigma\wedge$ 均属于 $\mathrm{R}_j[\mathrm{x}]$。可以将它们看作由 $\mathbb{F}(\mathrm{z}, \mathrm{x})$ 计算得到，同时跟踪其次数。不失一般性，假设 $\mathrm{val}_z(\mathrm{T}_{k-j,j})$ 在所有 $\mathrm{T}_{i,j'}$中最小。

5. $U_{i,j}|_{z=0}, V_{i,j}|_{z=0} \in \mathbb{F}\setminus\{0\}$.

像之前一样，我们继续进行，不再进一步应用同态。注意，假设 3 中的“或条件”与$j = 0$情形类似，只是没有 Φ：这是因为$\Phi(f_0)|_{z=0} \neq 0 \iff \Phi(f_0/T_k, 0)|_{z=0} \neq 0$。该条件只是将导数与常数项分离开来。

高效从$k-j$到$k-j-1$的归约。 令 $\mathrm{val}_z(T_{i,j}) =: v_{i,j}$，对所有$i \in [k-j]$均成立。注意

$$\min_i \mathrm{val}_z(T_{i,j}) = \min_i \mathrm{val}_z(P_{i,j}/Q_{i,j}) = v_{k-j,j}$$

由于 $\mathrm{val}_z(U_{i,j}) = \mathrm{val}_z(V_{i,j}) = 0$（否则我们重新排序）。我们指出，在$j$步中，对所有$i$均有 $0 \leq v_{i,j} < dj$；上界是严格的，否则$T_{i,j} = 0$ 将成为 $\mathrm{R}i(x)$上的。

与第一步类似，我们用具有最小 val 的$T_{k-j,j}$ 进行除法，然后得到：

$$\begin{aligned} \sum_{i\in[k-j]} T_{i,j} = f_j &\iff \sum_{i\in[k-j-1]} T_{i,j}/T_{k-j,j} + 1 = f_j/T_{k-j,j} \\ &\implies \sum_{i\in[k-j-1]} \partial_z(T_{i,j}/T_{k-j,j}) = \partial_z(f_j/T_{k-j,j}) \\ &\iff \sum_{i=1}^{k-j-1} T_{i,j}/T_{k-j,j} \cdot \mathsf{dlog}(T_{i,j}/T_{k-j,j}) = \partial_z(f_j/T_{k-j,j}) \end{aligned} \tag{3.4}$$

定义如下：

- $\mathrm{R}j_{+1} := \mathbb{F}[z]/\langle z d_{j+1}\rangle$，其中$dj_{+1} := dj - vk\text{–}j, j - 1$。∼
- $Tij_{+1} := Tij/Tk\text{–}jj \cdot$对数微分$(Tij/Tk\text{–}jj)$，$\forall i \in [k-j-1]$。

• $f_{j+1} := \partial_z(f_j/T_{k-j,\ j})$，在 $\mathrm{R}_{j+1}(\boldsymbol{x})$。

我们再次强调，我们并不直接计算 $\tilde{T}_{i,j+1}$ 模 $z^{d_{j+1}}$；相反，我们将其作为 $\mathbb{F}(z,\boldsymbol{x})$ 中的一个分式来计算，其中 z 是形式变量。形式地，我们计算 $T_{i,j+1} \in \mathbb{F}(z,\boldsymbol{x})$，使得 $\tilde{T}_{i,j+1} = T_{i,j+1}$ 在 $\mathrm{R}^{j+1}(\boldsymbol{x})$ 上成立。我们跟踪 $T_{i,j+1}$ 中 z 的次数。接下来，我们将证明，所作的所有归纳假设在第 j^{th} 步中同样成立。

假设（1）：$\mathrm{T}_{i,j+1}$ 和 f^{j+1} 的可定义性。根据最小赋值假设，可知 $\mathrm{val}(\mathrm{f}) \geq \mathrm{v}_{k-j,j}$，因此 $\mathrm{T}_{i,j+1}$ 和 f^{j+1} 在 $\mathrm{R}^{j+1}(\mathrm{x})$ 上都有良好定义。注意，公式 3.4 在 $\mathrm{R}^{j+1}(\mathrm{x})$ 上成立，因为 $\mathrm{d}^{j+1} < \mathrm{d}^{j}$（因为，无论模 z^{d_j} 成立什么恒等式，模 $\mathrm{z}^{d_{j+1}}$ 也必然成立）。因此，我们必有 $\sum^{k-j-1}_{\mathrm{i}=1} \mathrm{T}_{i,j+1} = \mathrm{f}^{j+1}$ 在 $\mathrm{R}^{j+1}(\mathrm{x})$ 上成立，从而证明归纳假设（1）。

假设 (2): 赋值的正性。由于我们除以最小赋值，根据定义，立即得到 $\mathrm{val}_z(T_{i,j+1}) \geq 0$，从而证明了该假设。此外，我们声称在 DiDI 中计算最小赋值很容易。为此，回顾赋值的定义

$$\min_i \mathrm{val}_z(P_{i,j}/Q_{i,j}) = \min_i(\mathrm{val}_z(P_{i,j}) - \mathrm{val}_z(P_{i,j})).$$

因此，对于最小赋值，我们计算所有 $i \in [k-j]$ 对应的 $\mathrm{val}_z(P_{i,j})$ 和 $\mathrm{val}_z(Q_{i,j})$。

下面这个重要引理表明，由 $\Sigma\wedge\Sigma\wedge$ 电路计算的多项式 $f(\boldsymbol{x},y) \in \mathbb{F}[\boldsymbol{x},y]$，的 y^e 系数，可以由一个小型 $\Sigma\wedge\Sigma\wedge$ 电路计算。

引理 3.5 (系数提取)。设 $f(\boldsymbol{x},y) \in \mathbb{F}[y][\boldsymbol{x}]$ 由一个规模为 s、次数为 d 的 $\Sigma\wedge\Sigma\wedge$ 电路计算。那么，$\mathrm{coef}_{y^e}(f) \in \mathbb{F}[\boldsymbol{x}]$ 可以由一个规模为 $O(sd)$ 的小型 $\Sigma\wedge\Sigma\wedge$ 电路在 $\mathbb{F}[\boldsymbol{x}]$ 上计算。

证明概要。设，$f = \sum_i \alpha_i \cdot g^{e_i}$。显然，$e_i \leq s$ 且 $\deg_y(f) \leq d$。因此，写作 $f = \sum_{i=0}^{d} f_i \cdot y^i$，其中 $f_i \in \mathbb{F}[\boldsymbol{x}]$。我们可以在 $d+1$ 个互异点 $y \in \mathbb{F}$ 上进行插值，并得出结论：f_i 具有一个规模至多为 $\Sigma\wedge\Sigma\wedge O(sd)$ 的电路。 □

根据 引理 3.5，我们知道 $\mathrm{coef}_{z^e}(P_{i,j})$ 和 $\mathrm{coef}_{z^e}(Q_{i,j})$ 都属于 $\Sigma\wedge\Sigma\wedge$ 上的 $F[\boldsymbol{x}]$。我们可以跟踪 z 的次数，并由此进行插值，找出使计算所得系数满足 $\neq 0$ 的最小 $e < d^j$，从而得到相应的 val。

假设 (3): "当且仅当"条件。上述 公式 3.4 开创了从 $k-j$ 项和式约化到 $k-j-1$ 的方法。但我们需要一个 $\Longleftrightarrow$ 条件，以便高效地约化恒等式测试。若 $f_{j+1} \neq 0$，则 $\mathrm{val}_z(f^{j+1}) < d^{j+1}$。此外，$f_{j+1} = 0$ 属于 $\mathrm{R}^{j+1}(\boldsymbol{x})$ 蕴含——

1. 或者，$f_j/T_{k-j,j}$ 与 z 无关。这意味着它属于 $\mathbb{F}(\boldsymbol{x})$。现在，若 $f_0 \neq 0$ 确实成立，那么根据归纳假设（因为它们在 $\mathrm{R}^j(\boldsymbol{x})$ 上均非零），计算得到的 $T_{i,j}$ 以及 f^j 在 $\mathbb{F}(z,\boldsymbol{x})$ 上都必须非零。然而，

$$\left(\frac{T_{i,j}}{T_{k-j,j}}\right)\Big|_{z=0} = \left(\frac{U_{i,j}\cdot V_{k-j,j}}{U_{k-j,j}\cdot V_{i,j}}\right)\Big|_{z=0} \cdot \left(\frac{P_{i,j}\cdot Q_{k-j,j}}{P_{k-j,j}\cdot Q_{i,j}}\right)\Big|_{z=0}$$

$$\in \mathbb{F} \cdot \left(\frac{\Sigma\wedge\Sigma\wedge}{\Sigma\wedge\Sigma\wedge} \right).$$

因此，

$$\frac{f_j}{T_{k-j,j}} \in \sum \mathbb{F} \cdot \left(\frac{\Sigma\wedge\Sigma\wedge}{\Sigma\wedge\Sigma\wedge} \right) \in \left(\frac{\Sigma\wedge\Sigma\wedge}{\Sigma\wedge\Sigma\wedge} \right).$$

这里关键地使用了 $\Sigma\wedge\Sigma\wedge$ 在乘法下是封闭的（引理 2.11）。因此，这个恒等式测试可以在 多项式时间内完成（引理 2.9）。有关详细的时间复杂度和计算，请参见 命题 3.6 及其后续段落。

2. 或者， $\partial_z(\mathrm{f}i/\mathrm{T}_{k-j,j}) = \mathrm{z}^{d_{j+1}} \cdot \mathrm{p}$，其中 $\mathrm{p} \in \mathbb{F}(\mathrm{z}, \mathrm{x})$ s.t. $\mathrm{val}_z(\mathrm{p}) \geq 0$。通过简单的幂级数展开，可以得出 $\mathrm{p} \in \mathbb{F}(\mathrm{x})[[\mathrm{z}]]$ （引理 3.3）。因此，可以得出

$$\frac{f_j}{T_{k-j,j}} \in \left\langle z^{d_{j+1}+1} \right\rangle_{\mathbb{F}(\boldsymbol{x})[[z]]} \implies \mathsf{val}_z(f_j) \geq d_j,$$

即 $f_j = 0$，在 $\mathrm{R}i(\boldsymbol{x})$ 上。

反之，$f_j = 0$，在 $\mathrm{R}i(\boldsymbol{x})$ 上，意味着

$$\begin{aligned} \mathsf{val}_z(f_j) \geq d_j &\implies \mathsf{val}_z\left(\partial_z\left(\frac{f_j}{T_{k-j,j}}\right)\right) \geq d_j - v_{k-j,j} - 1 \\ &\implies f_{j+1} = 0, \text{ over } \mathsf{R}_{j+1}(\boldsymbol{x}). \end{aligned}$$

因此，我们已经证明 $\sum_{i\in[k-j]} T_{i,j} \neq 0$ 在 $\mathrm{R}i(\boldsymbol{x})$ 上当且仅当

$$\sum_{i\in[k-j-1]} T_{i,j+1} \neq 0 \text{ over } \mathsf{R}_{j+1}(\boldsymbol{x}) \text{ , or, } 0 \neq \left(\frac{f_j}{T_{k-j,j}}\right)\Big|_{z=0} \in \mathbb{F}(\boldsymbol{x}) .$$

因此归纳假设（3）成立。

假设 (4)：规模分析。 我们将证明，$T_{i,j+1} \in (\Pi\Sigma \wedge /\Pi\Sigma\wedge) \cdot (\Sigma\wedge\Sigma\wedge/\Sigma\wedge\Sigma\wedge)$在 $\mathrm{R}i^{+1}(\boldsymbol{x})$上，其规模仅发生多项式级膨胀。设 $\mathsf{size}(T_{i,j}) \leq sj$，其中 $i \in [k-j]$, 且$j \in [k]$。注意，根据假设，$s_0 \leq s$。

命题 3.6 (最终规模)。 $T_{1,k-1} \in (\Pi\Sigma \wedge /\Pi\Sigma\wedge) \cdot (\Sigma\wedge\Sigma\wedge/\Sigma\wedge\Sigma\wedge)$ 规模为 $s^{O(k7^k)}$，在 $\mathsf{R}_{k-1}(\boldsymbol{x})$上。

证明。 步骤$j = 0$ 和 $j > 0$ 略有不同，这是因为 Φ。不过，使用幂级数的主要思路相同，最终可证明 $\mathsf{dlog}(\Sigma\wedge) \in \Sigma\wedge\Sigma\wedge$。

我们首先处理 $\mathrm{j} = 0$。令 $\mathrm{A} - \mathrm{z} \cdot \mathrm{B} = \Phi(\mathrm{g}) \in \Sigma\wedge$，其中 $\mathrm{A} \in \mathbb{F}$ 且 $\mathrm{B} \in \mathrm{R}_1[\mathrm{x}]$。注意，由于映射 Ψ，$\mathrm{A} \neq 0$。此外，$\mathsf{size}(\mathrm{B}) \leq \mathrm{O}(\mathrm{d} \cdot \mathsf{size}(\mathrm{g}))$，因为形如 x^e 的单个单项式可以生成 d $+1$个单项式。在 $\mathrm{R}_1(\mathrm{x})$ 上，

$$\mathsf{dlog}(\Phi(g)) = -\frac{\partial_z(B\cdot z)}{A(1-\frac{B}{A}\cdot z)} = -\frac{\partial_z(B\cdot z)}{A} \cdot \sum_{i=0}^{d_1-1} \left(\frac{B}{A}\right)^i \cdot z^i . \tag{3.7}$$

B^i 有一个平凡的 $\wedge\Sigma\wedge$-电路，其规模为 $O(d \cdot size(g))$。此外， $\partial_z(B \cdot z)$ 有一个规模至多为 $O(d \cdot size(g))$ 的 $\Sigma\wedge$-电路。利用华林恒等式（引理 2.10），可得每个 $\partial_z(B \cdot z) \cdot (B/A)^i \cdot z^i$的规模在 $R_1(x)$ 上为 $O(i \cdot d \cdot size(g))$。对 $i \in [d_1 - 1]$ 求和，总规模至多为 $O(d_1^2 \cdot d \cdot size(g)) = O(d^3 \cdot size(g))$，因为 $d_0 = d_1 = d$。

对于第j步，我们强调，次数可能大于d。假设$T_{i,j}$ 的分母和分子（各自属于 $\mathbb{F}[x,z]$）的语法次数不超过D^j（如上所见，它不是 d^j；这样可以避免在每一步进行模计算的麻烦）。当然，$D_0 < d \leq s$。

对于 $j > 0$，公式 3.7 中的上述求和是在 $R^j(x)$ 上进行的。然而，相应的 A 和B 的次数可能是 D^j （可能大于 d^j）。因此，幂级数展开后的总体规模将为 $O(D_j^2 \cdot d \cdot$规模$(g))$。

利用引理 3.8，我们可以证明 $\text{dlog}(P_{i,j}) \in \Sigma\wedge\Sigma\wedge/\Sigma\wedge\Sigma\wedge$ （$Q_{i,j}$ 的情况类似）的规模为 $O(D_j^2 \cdot s^j)$。此外，$\text{dlog}(U_{i,j} \cdot V_{k-j,j}) \in \sum \text{dlog}(\Sigma\wedge)$，即 dlog 作用于 $\Sigma\wedge$ 上的结果之和（因为对数微分可以将乘积线性化）；并且可以通过上述形式计算。因此，$\text{dlog}(T_{i,j}/T_{k-j,j})$ 是 4 个 $\Sigma\wedge\Sigma\wedge/\Sigma\wedge\Sigma\wedge$ 之和，其规模至多为 $O(D_j^2 s^j)$，以及 1 个规模为 $O(D_j^2 d^j s^j)$ 的 $\Sigma\wedge\Sigma\wedge$ （由上述幂级数计算得到）。[注意：我们将来自 $\text{dlog}(\Sigma\wedge)$ 的 $\Sigma\wedge\Sigma\wedge$ 表达式合并求和了]。此外，每个分母和分子（即 $\Sigma\wedge\Sigma\wedge/\Sigma\wedge\Sigma\wedge$）的语法次数均为 $O(D^j)$。我们利用华林恒等式（引理 2.11），将这 4 个表达式（每个都是 $\Sigma\wedge\Sigma\wedge/\Sigma\wedge\Sigma\wedge$）合并并表示为一个 $\Sigma\wedge\Sigma\wedge/\Sigma\wedge\Sigma\wedge$，其规模膨胀为 $O(D_j^{12} s_j^4)$；此时语法次数膨胀至 $O(D^j)$。最后，我们加上剩余的 $\Sigma\wedge\Sigma\wedge$ 电路（规模为 $O(D_j^3 s^j)$，次数为 $O(dD^j)$），得到 $O(s_j^5 D_j^{16} d)$。为了对此进行上界估计，我们需要理解次数上界 D^j。

最后，我们需要将$T_{i,j}/T_{k-j,j} \in (\Pi\Sigma\wedge/\Pi\Sigma\wedge) \cdot (\Sigma\wedge\Sigma\wedge/\Sigma\wedge\Sigma\wedge)$相乘，其中每个$\Sigma\wedge\Sigma\wedge$ 都是两个规模为s^j、语法次数为D^j的 $\Sigma\wedge\Sigma\wedge$ 表达式的乘积；将它们合并在一起会产生$O(D^j \cdot s_j^2)$的膨胀。因此，将其与上文 dlog 计算得到的 $\Sigma\wedge\Sigma\wedge/\Sigma\wedge\Sigma\wedge$ 表达式相乘，会产生$s^{j+1} = s^7 \cdot D^{O(1)}{}_j \cdot d$的规模膨胀。

计算$T_{i,j}/T_{k-j,j}$ 会使语法次数缓慢增长；这一增长远小于规模膨胀。如前所述，dlog 计算中的次数膨胀为$O(dD^j)$，而清除四个表达式时，膨胀仅为$O(D^j)$。因此，$D^{j+1} = O(dD^j) \implies D^j = d$。

关于规模的递归为 $s^{j+1} = s_j^7 \cdot d^{O(j)}$。利用 $d \leq s$ 我们可推得，$s^j = (sd)^{O(j \cdot 7^j)}$。特别地，$s_{k-1}$，经过 $k-1$ 步后的规模为 $s^{O(k \cdot 7^k)}$。这一计算定量地确立了归纳假设（4）。

□

假设（5）：的可逆性-电路。 对于可逆性，我们要强调，dlog 计算在此处发挥着关键作用。在下面的引理中，我们声称，作用 $\text{dlog}(\Sigma\wedge\Sigma\wedge) \in \Sigma\wedge\Sigma\wedge/\Sigma\wedge\Sigma\wedge$ 的规模为多项式规模。

引理 3.8 （求导）。设 $f(x, y) \in \mathbb{F}[y][x]$ 由一个规模为 s、次数为 d 的 $\Sigma\wedge\Sigma\wedge$ 电路计算得到。那么，$\partial_y(f)$ 可以由一个规模为 $O(sd^2)$ 的小型 $\Sigma\wedge\Sigma\wedge$ 电路计算得到，该电路在 $\mathbb{F}[y][x]$ 上运行。

证明概要 *h.* 引理 3.5 表明，每个f_e 都有规模为$O(sd)$ 的电路，其中$f = \sum_e f_e y^e$。Doi ng

对每个$e \in [0,d]$，这会导致$O(sd^2)$的膨胀。 □

类似地，考虑对 $\Pi\Sigma\wedge$的作用。我们知道 对数微分 将乘积加性地分配，因此只需处理 对数微分$(\Sigma\wedge)$；并且我们在前面的 命题 3.6 中看到，$\mathrm{dlog}(\Sigma\wedge) \in \Sigma\wedge\Sigma\wedge$ 具有多项式规模。假设这些条件成立，我们可将其简化为

$$\frac{T_{i,j}}{T_{k-j,j}} = \frac{U_{i,j}\cdot V_{k-j,j}}{V_{i,j}\cdot U_{k-j,j}} \cdot \frac{P_{i,j}\cdot Q_{k-j,j}}{Q_{i,j}\cdot P_{k-j,j}},$$

及其对数微分。因此，利用公式 3.4，$U_{i,(j+1)}$ 增长为$U_{i,j}\cdot V_{k-j,j}$ （$V_{i,(j+1)}$也同样如此）。这也意味着：$U_{i,(j+1)}|_{z=0} \in \mathbb{F}\setminus\{0\}$，从而证明该假设。

最终时间复杂度

上述证明实际上表明，$\mathrm{T1}_{,k-1}$ 属于$\mathrm{R}_{k-1}(\mathrm{x})$上的$\mathrm{Gen}(1, \mathrm{s}^{O(k\cdot 7^k)})$；并且z的次数上界（在 $\mathbb{F}[\mathrm{z},\mathrm{x}]$，上保持分母和分子“原位”）为$\mathrm{D}_{k-1} = \mathrm{d}^{O(k)}$。由于$\mathrm{R}_{k-1}(\mathrm{x})$，我们不能直接使用组成的简单模型的恒等式检验算法。此外，利用假设（2）和引理 3.3，我们知道$\mathrm{T1}_{,k-1} \in \mathbb{F}(\mathrm{x})[[\mathrm{z}]]$，因此只需对幂级数的第一项进行恒等式测试：$\mathrm{T1}_{,k-1}|_{z=0}$ 在 $\mathbb{F}(\mathrm{x})$上。注意，假设（5）保证 $\Pi\Sigma\wedge$ 部分在 $\mathrm{z} = 0$ 求值时保持非零；然而，$\Sigma\wedge\Sigma\wedge/\Sigma\wedge\Sigma\wedge$ 可能未定义。为此，我们跟踪分子和分母关于z的次数，如上面的讨论所示，它们将具有多项式上界。我们可以轻松地进行插值并消去z的幂，使其成立。基本上，这表明要测试$\mathrm{T1}_{,k-1}$，我们需要测试$\mathrm{z}^e\cdot\Sigma\wedge\Sigma\wedge$ 在 $\mathbb{F}[\mathrm{x}]$ 上，其中$\mathrm{e} \geq 0$，这是由于正赋值所致。利用引理 2.9，$\Sigma\wedge\Sigma\wedge$的白盒多项式恒等性测试可在多项式时间内完成；利用引理 2.1，在适当的次数上界下可以测试z^e。上述证明是构造性的：我们显式地从$\mathrm{U}_{i,j}$计算出$\mathrm{U}_{i,j+1}$（以及其他项）。将所有内容连接起来，我们得出这一部分可在$\mathrm{s}^{O(k7^k)}$时间内完成。

剩下的工作是检验归纳假设的$z = 0$部分（3）；它可能会在$j = k-1$之前很早就提前终止递归。正如前面提到的，在这种情况下，我们只需对 $\Sigma\wedge\Sigma\wedge$ 进行多项式恒等式测试。在第j步，当代入$z = 0$时，每个$T_{i,j}$ 的规模至多为s^j （按定义）。我们需要对一个更简单的模型进行多项式恒等式测试：$\sum^{[k-j]} \mathbb{F}\cdot(\Sigma\wedge\Sigma\wedge/\Sigma\wedge\Sigma\wedge)$。我们可以化简并将其表示为单个 $\Sigma\wedge\Sigma\wedge/\Sigma\wedge\Sigma\wedge$ 表达式；其规模膨胀为$s^{O(k-j)_j} \leq (sd)^{O(j(k-j)7^j)}$。由于这种情况可能会提前终止递归，为了界定最终时间复杂度，我们需要考虑使指数最大的j。

引理 3.9。设 $k \in \mathbb{N}$，且 $h(x) := x(k-x)7^x$。那么，$\max^{i\in[k-1]} h(i) = h(k-1)$。

证明概要。求导得到 $h'(x) = (k-x)7^x - x7^x + x(k-x)(\log 7)7^x = 7^x\cdot[x^2(-\log 7) + x(k\log 7 - 2) + k]$。它在

$$x = \left(\frac{k}{2} - \frac{1}{\log 7}\right) + \sqrt{\left(\frac{k}{2} - \frac{1}{\log 7}\right)^2 - \frac{k}{\log 7}}\,.$$

因此，h 在整数 $x = k - 1$处达到最大值。 □

因此，$\max_{j\in[k-1]} j(k-j)7^j = (k-1)7^{k-1}$。最后，使用 引理 2.9 进行基本情形的白盒多项式恒等性测试。因此，最终时间复杂度为 $s^{O(k\cdot 7^k)}$。

这里我们还要指出，在 $z = 0$ 代换 $\Sigma\wedge\Sigma\wedge/\Sigma\wedge\Sigma\wedge$ 中可能未定义。不过，我们会跟踪分子和分母的 z 次数，正如上文讨论的那样，它们将被多项式有界。我们可以轻松地进行插值并消去 z 的幂，使其能够正常工作。

位复杂度。 可以常规地证明，位复杂度确实如我们所声称的那样。初始时，给定电路的位复杂度为 s。主要的膨胀来自 对数微分-计算，其导致多项式规模膨胀。还要指出，使用 引理 2.11 (使用 引理 2.10) 时，我们 可能 需要扩张到次数至多为 $s^{O(k)}$ (这是由于 $\varepsilon(i)$ 以及相应的常数 $\gamma_{\varepsilon(2),\ldots,\varepsilon(k)}$，但它们仍然是 $s^{O(k)}$-位）。此外，定理 2.2 和 引理 2.9 的计算会使位复杂度发生多项式膨胀。证明至此完成。

□

备注。1. 上述方法不能（在多项式时间内）为 $\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}$ 提供白盒多项式恒等式测试，因为我们不知道 $\Sigma\wedge\Sigma\Pi^{[\delta]}$ 的多项式时间白盒多项式恒等式测试。然而，上述方法确实表明，$\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}$ 的白盒多项式恒等式测试可归约为 $\Sigma\wedge\Sigma\Pi^{[\delta]}$ 的白盒多项式恒等式测试，且归约是多项式时间的。

2. DiDI 技术可用于为一般的膨胀模型 Gen(k,s)提供白盒多项式恒等式测试。3. 当特征为 $\geq d$ 时，上述证明仍然成立。这是因为对 z 求导后，非零性仍得以保留。

3.1 算法

定理 定理 1.1的白盒多项式恒等式测试（第 3 节中对此进行了讨论）如下所示，即算法 1。

注意事项：在整个算法中，需要紧凑地存储一些中间表达式。可以把它们看作关于 $\boldsymbol{x}$ 的“特殊”电路，但其系数取自函数域 $\mathbb{F}(\boldsymbol{z})$。请跟踪它们关于 z 的次数，以及以“膨胀”电路形式表示的分式规模。

4 深度 4 电路的黑盒多项式恒等式测试

我们将在本节给出定理 1.2 的证明。在详细展开之前，我们先陈述一些重要定义和引理，这些内容来自[ASSS16]，稍后将会引用。

定义 4.1 （超越次数）。 若存在非零的消去多项式A，使得 $A(T_1,, T_m) = 0$，则称多项式 $T_1,, T_m$ 在代数相关。超越次数是 $T_1,, T_m\}$ 中最大的代数无关子集 S 的大小。此时，S 称为一个超越基。

算法 1 $\Sigma^{[k]}\Pi\Sigma\wedge$-电路的白盒多项式恒等性测试算法 输入：$f = T_1 + ... + T_k \in \Sigma^{[k]}\Pi\Sigma\wedge$，一个定义在 $\mathbb{F}[x]$ 上、规模为 s 的白盒电路 输出：若 $f \equiv 0$，则输出 0；若非零，则输出 1。1：令 $\Psi : \mathbb{F}[x] \longrightarrow \mathbb{F}[z]$，为一个稀疏多项式恒等式测试映射，使用 [KS01]（定理 2.2）。将其应用于 f，并检查 $\Psi(f) ?= 0$。若非零，则输出 1。2：从 $\mathcal{H}$ 的命中集中取得一点 $\boldsymbol{\alpha} = (a_1,..., a_n) \in \mathbb{F}^n$，使得对所有 $i \in [k]$，$T_i|_{x=\boldsymbol{\alpha}} \neq 0$。并定义 $\Phi : x_i \mapsto z \cdot x_i + a_i$。按如下方式检查 $\sum_{i\in[k-1]} \partial_z(\Phi(T_i)/\Phi(T_k)) ? = 0 \mod z^{d_1}(d_1 := s)$：3：考虑 $R_1(x)$ 上的每个 $T_{i,1} := \partial_z(\Phi(T_i)/\Phi(T_k))$，其中 $R_1 := \mathbb{F}[z]/\langle z^{d_1}\rangle$。使用 dlog 计算（命题 3.6），将每个 $T_{i,1}$ 写成 $(\Pi\Sigma\wedge/\Pi\Sigma\wedge) \cdot (\Sigma\wedge\Sigma\wedge/\Sigma\wedge\Sigma\wedge)$ 的“膨胀”形式。4：对于 $j \leftarrow 1$ 到 $k-1$，执行以下操作。5：使用“除法与求导”技术，逐步降低每一步的顶层扇入。假设在第 j 步需要检查恒等式：$\sum_{i\in[k-j]} T_{i,j} ?= 0$，它定义在 $R_j(x)$ 上，其中 $R_j := \mathbb{F}[z]/\langle z^{d_j}\rangle$；每个 $T_{i,j}$ 都有一个 $(\Pi\Sigma\wedge/\Pi\Sigma\wedge) \cdot (\Sigma\wedge\Sigma\wedge/\Sigma\wedge\Sigma\wedge)$ 表示，且其中每个 $\Pi\Sigma\wedge|_{z=0} \in \mathbb{F} \setminus \{0\}$。6：计算 $v_{k-j,j} := \min_i \mathrm{val}_z(T_{i,j})$；通过重排，可令 $i = k-j$。要计算 $v_{k-j,j}$，使用系数提取（引理 3.5）和 $\Sigma\wedge\Sigma\wedge$-电路多项式恒等式测试（引理 2.9）。7：“除以”$T_{k-j,j}$，并检查 $\left(\sum_{i\in[k-j-1]} (T_{i,j}/T_{k-j,j}) + 1\right)\Big|_{z=0} ?= 0$。注意：该表达式属于 $(\Sigma\wedge\Sigma\wedge/\Sigma\wedge\Sigma\wedge)$。使用 ——(1) $\Pi\Sigma\wedge|_{z=0} \in \mathbb{F}$，以及 (2) $\Sigma\wedge\Sigma\wedge$ 在乘法下的封闭性。最后，依据引理 2.9 对其进行多项式恒等式测试。8：若其非零，则输出 1；否则，对 z 求导，并在 $R_{j+1}(x)$ 上对 $\left(\sum_{i\in[k-j-1]} \partial_z(T_{i,j}/T_{k-j,j})\right) ?= 0$ 进行“归纳”，其中 $R_{j+1} := \mathbb{F}[z]/\langle z^{d_j - v_{k-j,j}-1}\rangle$。9：再次利用 dlog（命题 3.6），证明 $T_{i,j+1} := \partial_z(T_{i,j}/T_{k-j,j})$ 在 $R_{j+1}(x)$ 上具有规模较小的 $(\Pi\Sigma\wedge/\Pi\Sigma\wedge)\cdot(\Sigma\wedge\Sigma\wedge/\Sigma\wedge\Sigma\wedge)$-电路。因此，对 $\sum_{i\in[k-j-1]} T_{i,j+1} ?= 0$ 调用该算法。10：$j \leftarrow j + 1$。11：结束循环。12：最后，$j = k - 1$。依据引理 2.9，对 $R_{k-1}(x)$ 上唯一的 $(\Pi\Sigma\wedge/\Pi\Sigma\wedge) \cdot (\Sigma\wedge\Sigma\wedge/\Sigma\wedge\Sigma\wedge)$ 电路进行多项式恒等式测试。若结果为零，则输出 0；否则输出 1。

定义 4.2 (忠实同态)。对于 $\boldsymbol{T}$，同态 $\Phi\colon \mathbb{F}[\boldsymbol{x}] \to \mathbb{F}[\boldsymbol{y}]$ 是忠实的，当且仅当超越次数$_{\mathbb{F}}(\boldsymbol{T}) =$ 超越次数$_{\mathbb{F}}(\Phi(\boldsymbol{T}))$。

之所以关注忠实映射，是因为它有助于保持恒等关系，如下述事实所示。

Fact 4.3 (定理 2.4 [ASSS16])。对于任意 $C \in \mathbb{F}[y_1, \ldots, y_m]$，$C(\boldsymbol{T}) = 0 \iff C(\Phi(\boldsymbol{T})) = 0.$

这里有一个关于雅可比矩阵的重要判据，它基本上表明该矩阵保持代数独立性。

事实 4.4 (雅可比判据)。设 $\mathbf{f} \subset \mathbb{F}[\boldsymbol{x}]$ 是一个有限的多项式集合，且其中多项式的次数至多为 d，并且超越次数$_{\mathbb{F}}(\mathbf{f}) \leq r$。若 $char(\mathbb{F}) = 0$，或 $char(\mathbb{F}) > d^r$，则超越次数$_{\mathbb{F}}(\mathbf{f})$ = 等于$\mathrm{rk}_{\mathbb{F}(x)}\mathcal{J}_{\boldsymbol{x}}(\mathbf{f})$。

雅可比判据与忠实映射为设计一种映射提供了方法；当超越次数较小时，该映射可以大幅减少变量的数量。

引理 4.5 (引理 2.7 [ASSS16])。设 $\boldsymbol{T} \in \mathbb{F}[\boldsymbol{x}]$ 是一个有限的多项式集合，其中每个多项式的次数至多为 d，且 超越次数$_{\mathbb{F}}(\boldsymbol{T}) \leq r$，并且 $char(F)$=0 or $> d^r$。设 $\Psi'\colon \mathbb{F}[\boldsymbol{x}] \longrightarrow \mathbb{F}[z]$ 满足 $\mathrm{rk}_{\mathbb{F}(x)}\mathcal{J}_{\boldsymbol{x}}(\boldsymbol{T}) = \mathrm{rk}_{\mathbb{F}(z)}\Psi'(\mathcal{J}_{\boldsymbol{x}}(\boldsymbol{T}))$。

那么，映射 $\Phi\colon \mathbb{F}[\boldsymbol{x}] \longrightarrow \mathbb{F}[z,t,\boldsymbol{y}]$，使得 $x_i \mapsto (\sum_{j\in[r]} y_j t^{ij}) + \Psi'(x_i)$，是 T 的忠实同态。

在下一节中，我们将使用这些工具证明 定理 1.2(b)。关于 定理 1.2(a) 的证明和计算非常相似。

4.1 $\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}$的多项式恒等式测试

我们解决了 解决比 $\Sigma^{[k]}\Pi\Sigma\Pi$ 更一般模型的多项式恒等式测试。

问题 4.6。设 $\{T_i \,|\, i \in [m]\}$ 为（语法）次数至多为 d、规模为 s 的电路。设 T_i's 的超越次数为 超越次数$_{\mathbb{F}}(T_1, \ldots, T_m) = k \ll s$。此外，设 $C(x_1, \ldots, x_m)$ 为一个(规模 + 次数) $< s'$的电路。为 $C(T_1, \ldots, T_m)$设计一个黑盒多项式恒等式测试算法。

显然，$\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}$ 是上述设置的一个非常特殊的情形。令 $\boldsymbol{T} := \{T_1, \ldots, T_m\}$。令$\boldsymbol{T}_k := \{T_1, \ldots, T_k\}$ 为一个超越基。对于 $T_i = \prod_j g^{ij}$，记集合 $L(T_i) := \{g_{ij} \,|\, j\}$。

我们想要找到一个显式同态 $\Psi\colon \mathbb{F}[\mathrm{x}] \to \mathbb{F}[\mathrm{x}, \mathrm{z}]$ s.t. $\Psi(\mathcal{J}_{\boldsymbol{x}}(\mathrm{T}))$ 具有一种“良好”的形式。在像中，我们适当地固定 x，从而得到一个复合映射 $\Psi'\colon \mathbb{F}[\mathrm{x}] \longrightarrow \mathbb{F}[\mathrm{z}]$s.t. $\mathrm{rk}_{\mathbb{F}(x)}\mathcal{J}_{\boldsymbol{x}}(\mathrm{T}) = \mathrm{rk}_{\mathbb{F}(z)}\Psi'(\mathcal{J}_{\boldsymbol{x}}(\mathrm{T}))$。然后，我们可以将该映射扩展为 $\Phi\colon \mathbb{F}[\mathrm{x}] \longrightarrow \mathbb{F}[\mathrm{z}, \mathrm{y}, \mathrm{t}]$s.t. $\mathrm{x}_i \mapsto (\sum_{j=1}^{k} \mathrm{y} t^{ij}) + \Psi'(\mathrm{x}_i)$，这就是保真引理 4.5。我们展示了可以使用缩放与平移映射 (Ψ) 高效构造映射 Φ；该映射最终由一个 $\Sigma\wedge\Sigma\Pi^{[\delta]}$ 电路的命中集（H′定义 Ψ'）固定。总体而言，$\Phi(\mathrm{f})$ 是一个 k + 2-变量多项式，存在一个平凡的命中集。

不失一般性，$\mathcal{J}_{\boldsymbol{x}}(\mathrm{T})$ 关于变量集 $\mathrm{x}_k = (\mathrm{x}_1, \ldots, \mathrm{x}_k)$ 是满秩的。因此，根据假设，$\mathrm{J}^{\boldsymbol{x}_k}(\mathrm{T}_k) \neq 0$（有关符号说明，请参见第 2 节）。我们希望构造一个 Ψ，使得 $\Psi(\mathrm{J}^{\boldsymbol{x}_k}(\mathrm{T}_k))$ 具有更“容易”的多项式恒等式测试。根据行列式的线性[ASSS16，公式 3.1]，，我们有以下恒等式：

行列式，以及一个简单的观察：$\partial_x\left(T_i\right) = T_i \cdot \left(\sum_j \partial_x\left(g^{ij}\right)/g_{ij}\right)$，其中 $T_i = \prod_j g^{ij}$:

$$J_{x_k}(\boldsymbol{T}_k) = \sum_{g_1 \in L(T_1), \ldots, g_k \in L(T_k)} \left(\frac{T_1 \ldots T_k}{g_1 \cdots g_k}\right) \cdot J_{x_k}(g_1, \ldots, g_k)\,. \tag{4.7}$$

同态 Ψ。 为确保所有 $g \in \bigcup_i L(T_i)$ 我们按照第 3 节中的方法进行。考虑

$$h := \prod_{i \in [k]} \prod_{g \in L(T_i)} g = \prod_{i \in [\ell]} g,$$

其中 $g \in \bigcup_i L(T_i)$ 且 $\ell \le k \cdot s$。注意，$\deg h \le d \cdot k \cdot s$，且 h 可由规模为 O(s) 的电路计算。引理 2.4 给出了相关的命中集 $\mathcal{H} \subseteq \mathbb{F}^n$，其中包含一个求值点 $\boldsymbol{\alpha} = (a_1, \ldots, a_n)$，使得 $h(\boldsymbol{\alpha}) \neq 0$，从而对于所有 $g \in \bigcup_i L(T_i)$，都有 $g(\boldsymbol{\alpha}) \neq 0$。我们强调，与前一种情况不同，在这里的黑盒设置中，我们无法单独访问 g 来验证 $\boldsymbol{\alpha}$ 是否正确。因此，我们尝试所有 $\boldsymbol{\alpha} \in \mathcal{H}$，看看哪一个有效。如果输入多项式 f 非零，则必定存在这样一个 $\boldsymbol{\alpha}$。这一搜索会带来 poly(s) 的乘法膨胀，因为 $\mathcal{H}$ 的规模为 poly(s)。

固定一个 $\boldsymbol{\alpha} = (a1, \cdots, a_n) \in \mathcal{H}$，并定义 $\Psi\colon \mathbb{F}[x] \to \mathbb{F}[x, z]$ 为 $x_i \mapsto z \cdot x_i + a_i$。记环 $R[x]$，其中 $R := \mathbb{F}[z]/\langle z^D \rangle$，且 $D := k \cdot (d-1) + 1$。由于是一一映射，Ψ 显然是一个保持非零的映射。此外，

命题 4.8。 $J_{x_k}(\boldsymbol{T}_k) = 0 \iff \Psi(J_{x_k}(\boldsymbol{T}_k)) = 0$，在 $R[\boldsymbol{x}]$ 上。

证明。由于 $\deg(T_i) \le d$，矩阵的每个元素的次数至多为 $d-1$；因此 $\deg(J_{x_k}(\boldsymbol{T}_k)) \le k(d-1) = D - 1$。于是，$\deg_z(\Psi(J_{x_k}(\boldsymbol{T}_k))) < D$。结论得证。 □

公式 4.7 意味着

$$\Psi(J_{x_k}(\boldsymbol{T}_k)) = \Psi(T_1 \cdots T_k) \cdot \sum_{g_1 \in L(T_1), \ldots, g_k \in L(T_k)} \frac{\Psi(J_{x_k}(g_1, \ldots, g_k))}{\Psi(g_1 \cdots g_k)}\,. \tag{4.9}$$

由于 T_i 的乘积扇入为 s，公式 4.9 中求和的顶层扇入 公式 4.9 至多为 s^k。接着定义，

$$\widetilde{F} := \sum_{g_1 \in L(T_1), \ldots, g_k \in L(T_k)} \frac{\Psi(J_{x_k}(g_1, \ldots, g_k))}{\Psi(g_1 \cdots g_k)}\,, \text{ over } R[\boldsymbol{x}]. \tag{4.10}$$

$\widetilde{F}$ 的良定义性。 请注意，

$$\Psi(g_i) \bmod z \neq 0 \implies 1/\Psi(g_1 \cdots g_k) \in \mathbb{F}[[\boldsymbol{x}, z]].$$

因此，RHS 是 $\mathbb{F}[[\boldsymbol{x}, z]]$ 中的一个元素；对 z^D 取模后，它属于 $R[\boldsymbol{x}]$。我们指出，与其对 z^D 做最小化约化，不如使用一个 $F \in \mathbb{F}[z, \boldsymbol{x}]$，使得 $F = \widetilde{F}$ over $R[\boldsymbol{x}]$。

此外，我们确保 z 的次数受到多项式的有界约束。

断言 4.11. 在$\mathrm{R}[\boldsymbol{x}]$, $\Psi(J^{x_k}(T_k)) = 0 \iff F = 0$。

证明概要。 这由 $\Psi(T_1 \cdots T_k)$ 在$R[\boldsymbol{x}]$中的可逆性可得。 □

命中集 H'。由 $\mathrm{J}^{x_k}(\mathrm{T}_k) \neq 0$ 以及断言 4.8-4.11，我们有 $\mathrm{F} \neq 0$在 $\mathrm{R}[\mathrm{x}]$ 上。我们希望找到 $\mathrm{H}' \subseteq \mathbb{F}^n$，使得 $\Psi(\mathrm{J}^{x_k}(\mathrm{T}_k))|_{x=\alpha} \neq 0$，其中某个 $\alpha \in \mathrm{H}'$（这将确保秩保持）。为此，我们将在下文证明，F 在 $\mathrm{R}[\mathrm{x}]$ 上有一个 $\mathrm{s}^{O(\delta k)}$-规模 $\Sigma\wedge\Sigma\Pi^{[\delta]}$-电路。接下来，定理 2.8 给出命中集 H'，耗时 $\mathrm{s}^{O(\delta^2}\mathrm{k}\log \mathrm{s})$。

断言 4.12 (规模主界)。 $F \in \mathrm{R}[\boldsymbol{x}]$ 具有大小为$(s3^{\delta})^{O(k)}$的电路。

该证明研究方程 4.10—

<escape>1. 分子 $\Psi(J^{x_k}(g_1,\ldots,g_k))$ 具有 $O(3^{\delta}2^k k!ks)$规模的 $\Sigma\wedge\Sigma\Pi^{[\delta-1]}$电路（参见 引理 4.15），并且</escape>

2. $1/\Psi(g_1\cdots g_k)$，对于 $g_i \in L(T_i)$ 具有 $(s3^{\delta})^{O(k)}$规模为 $\Sigma\wedge\Sigma\Pi^{[\delta]}$ 的电路；二者均在 $\mathrm{R}[\boldsymbol{x}]$（参见引理 4.16）。

我们需要以下两个论断来证明分子大小界。

断言 4.13。 设 $g_i \in L(T_i)$，其中 $T_i \in \Pi\Sigma\Pi^{[\delta]}$ 的规模至多为 s，则多项式 $J^{x_k}(g_1,\ldots,g_k)$可由 $\Sigma^{[k!]}\Pi^{[k]}\Sigma\Pi^{[\delta-1]}$ 规模为 $O(k!ks)$的电路计算。

证明概要。 矩阵的每个元素的次数至多为 $\delta-1$。直接展开可得 $k!$ 个顶层扇入，其中每个乘积（扇入为 k）的规模为 $\sum_i \mathrm{size}(g_i)$。由于 $\mathrm{size}(T_i) \leq s$，显然每个 $\mathrm{size}(g_i) \leq s$。因此，总规模为 $k!\cdot\sum_i \mathrm{size}(g_i) = O(k!ks)$。 □

断言 4.14。 设 $g \in \Sigma\Pi^{\delta}$，则 $\Psi(g) \in \Sigma\Pi^{\delta}$ 的规模为 $3^{\delta}\cdot\mathrm{size}(g)$ （当 $n \gg \delta$时）。

证明概要。 每个次数为 δ 的单项式 $\boldsymbol{x}^{\boldsymbol{e}}$ 可生成 $\prod_i(e_i+1) \leq ((\sum_i e_i+n)/n)^n \leq(\delta/n+1)^n$ 个单项式；由算术-几何平均不等式，as $\sum_i e_i \leq \delta$。由于 $\delta/n \to 0$，我们有$(1+\delta/n)^n \to e^{\delta}$。由于 $e<3$，上界得证。 □

引理 4.15 (分子大小)。 $\Psi(J^{x_k}(g_1,\ldots,g_k))$ 可由大小为 $O(3^{\delta}\,2^k k\;k!s) =: s_2$计算。

证明。在断言 4.13 中，我们证明了 $\mathrm{J}^{x_k}(\mathrm{g}_1,\ldots,\mathrm{g}_k) \in \Sigma^{[k!]}\Pi^{[k]}\Sigma\Pi^{[\delta-1]}$ 的规模为 $\mathrm{O(k!ks)}$。此外，对于一个 $\mathrm{g} \in \Sigma\Pi^{[\delta-1]}$，我们有 $\Psi(\mathrm{g}) \in \Sigma\Pi^{[\delta-1]}$ 的规模至多为 $3^{\delta}\cdot\mathrm{size(g)}$，在 $\mathrm{R}[\mathrm{x}]$ 上（由断言 4.14 得出）。

结合这些结果可得，$\Psi(J^{x_k}(g_1,\ldots,g_k)) \in \Sigma^{[k!]}\Pi^{[k]}\Sigma\Pi^{[\delta-1]}$，规模为$O(3^{\delta}k!ks)$。我们利用华林恒等式（引理 2.10）将 Π-门转换为 $\wedge$ 门，这会使规模增大 2^{k-1} 的倍数。因此，$\Psi(J^{x_k}(g_1,\ldots,g_k)) \in \Sigma\wedge\Sigma\Pi^{[\delta-1]}$的规模为$O(3^{\delta}\,2^k k k!s)$。 □

在下面的引理中，通过对诸如 $1/(1-a\cdot z)$ 这样的表达式进行幂级数展开，我们得出 $1/\Psi(g)$ 具有一个规模较小的 $\Sigma\wedge\Sigma\Pi^{[\delta]}$-电路，这进一步意味着 $1/\Psi(g_1\cdots g_k)$ 也具有同样性质。

引理 4.16 (分母规模)。设 $g_i\in L(T_i)$。那么，$1/\Psi(g_1\cdots g_k)$ 可以由一个规模为 $s_1:=(s3^\delta)^{O(k)}$ 的 $\Sigma\wedge\Sigma\Pi^{[\delta]}$-电路计算，其中底环为 $\mathrm{R}[\boldsymbol{x}]$。

证明。设 $g\in L(T_i)$，其中 i 为某个值。假设，$\Psi(g)=A-z\cdot B$，其中 $A\in\mathbb{F}$ 和 $B\in\mathrm{R}[x]$ 的次数为 δ，且 $\mathrm{size}(B)\le 3^\delta\cdot s$，这由断言 4.14 得出。注意，在 $\mathrm{R}[x]$ 上

$$\frac{1}{\Psi(g)}=\frac{1}{A(1-\frac{B}{A}\cdot z)}=\frac{1}{A}\cdot\sum_{i=0}^{D-1}\left(\frac{B}{A}\right)^i\cdot z^i. \tag{4.17}$$

由于 B^i 有一个平凡的 $\wedge\Sigma\Pi^{[\delta]}$-电路（在 $\mathrm{R}[x]$ 上），其规模为 $\le 3^\delta\cdot s+i$；对 $i\in[D-1]$ 求和后，总规模至多为 $D\cdot 3^\delta\cdot s+O(D^2)$。由于 $D<k\cdot d$，我们得出，$1/\Psi(g)$ 有一个规模为 $\mathrm{poly}(s\cdot k\cdot d3^\delta)$ 的电路，其底环为 $\mathrm{R}[x]$。直接相乘 k 个这样的乘积，得到上界 $(s\cdot 3^\delta)^{O(k)}$，这里用到了引理 2.11（本质上就是华林恒等式）。 □

断言 4.12 的证明。结合引理 4.15–4.16，注意到 $\Psi(J_{x_k}(\cdot)/\Psi(\cdot)$ 在 $\mathrm{R}[x]$，上具有一个规模至多为 $(s_1\cdot s_2)^2=(s\cdot 3^\delta)^{O(k)}$ 的 $\Sigma\wedge\Sigma\Pi^{[\delta]}$-电路，其中使用了引理 2.11。将至多 s^k 个项相加（根据 F 的定义），其规模仍然保持为 $(s\cdot 3^\delta)^{O(k)}$。 □

次数上界。由于 T_i 的语法次数受 d 限制，且 Ψ 保持 $\deg_{\boldsymbol{x}}=\deg_z$，我们必须有 $\deg_z(\Psi(J_{x_k}(g_1,\ldots,g_k))=\deg_x(J_{x_k}(g_1,\ldots,g_k))\le D-1$。注意，引理 4.15 实际上在 $\mathbb{F}[x,z]$ 上成立，因此不存在额外的（关于 z 的）次数膨胀。然而，由于方程 4.17，引理 4.16 中存在一些次数膨胀。

注意，方程 4.17 表明在 $\mathrm{R}[\boldsymbol{x}]$，

$$\frac{1}{\Psi(g)}=\left(\frac{1}{A^D}\right)\cdot\left(\sum_{i=0}^{D-1}A^{D-1-i}z^i\cdot B^i\right)=:\frac{p(\boldsymbol{x},z)}{q},$$

其中 $q=A^D$。我们将 $p\in\mathbb{F}[\boldsymbol{x},z]$ 和 $q\in\mathbb{F}$视为变量。注意，$\deg_z(\Psi(g))\le\delta$ 意味着 $\deg_z(p)\le\deg_z((Bz)^{D-1})\le\delta\cdot(D-1)$。

最后，记 $1/\Psi(g_1\cdots g_k)=:P_{g_1,\ldots,g_k}/Q_{g_1,\ldots,g_k}$，其定义在 $\mathrm{R}[x]$ 上。这相当于将 k 个 (p/q) 相乘；因此次数会膨胀 k 的倍数。特别地，$\deg_z(P(\cdot))\le\delta\cdot k\cdot(D-1)$ 因此，在方程 4.10 中，对 s^k 个项求和，得到一个表达式（定义在 $\mathrm{R}[x]$ 上）：

$$F=\sum_{g_1\in L(T_1),\ldots,g_k\in L(T_k)}\Psi(J_{x_k}(g_1,\ldots,g_k))\cdot\left(\frac{P_{g_1,\ldots,g_k}}{Q_{g_1,\ldots,g_k}}\right)=:\frac{P(\boldsymbol{x},z)}{Q}.$$

验证$Q\in\mathbb{F}$。z 的次数也仍有上界

$$\max_{g_i\in L(T_i),i\in[k]}\deg_z(P_{g_1,\ldots,g_k})+\delta k\le\mathrm{poly}(s).$$

利用次数界，我们最终得到$P \in \mathbb{F}[x,\ z]$作为一个 $\Sigma\wedge\Sigma\Pi^{[\delta]}$-电路（在 $\mathbb{F}(z)$上），其规模$n^{O(\delta)}$ $(s3^{\delta})^{O(k)} = 3^{O(\delta k)}s^{O(k+\delta)} =: s_{3}$。

我们希望构造一个集合 $H' \subseteq \mathbb{F}^n$，使得作用 $P(H', z) \neq 0$。利用 [For15]（定理 2.8），我们得出它具有 $s^{O(\delta \log s_3)} = s^{O(\delta^2 k \log s)}$ 规模的命中集，并且可以在类似的时间内构造出来。因此，Φ的构造随之完成，使得 $\Phi(f)$ 成为一个 $k+2$元多项式。最后，根据 Φ的定义中 y、z、t 的显然次数界，我们得到了时间复杂度为 $s^{O(\delta^2 k \log s)}$ 的黑盒多项式恒等式测试算法；定理 1.2(b) 得证。

我们也可以为一般问题给出最终的命中集。

问题的解答：问题 *4.6*。我们知道

$$C(T_1, \ldots, T_m) = 0 \iff E := \Phi(C(T_1, \ldots, T_m)) = 0.$$

由于H'可以在$s^{O(\delta^2 k \log s)}$时间内构造，因此可以轻易地为$E|_{H'}$找到命中集（它只是一个具有上述次数界的$k+2$元多项式）。最终的E命中集可以在$s'^{O(k)} \cdot s^{O(\delta^2 k \log s)}$时间内构造。

□

注释。1. 由于雅可比判据（事实 4.4）在特征为 $> d^{\text{trdeg}}$ 时成立，因此容易得出，我们的定理对所有特征为 $> d^k$ 的域都成立。

2. 上述证明给出了从 $\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}$ 电路的黑盒多项式恒等式测试到$\Sigma\wedge\Sigma\Pi^{[\delta]}$电路的高效归约。特别地，若 $\Sigma\wedge\Sigma\Pi^{[\delta]}$电路存在多项式时间击中集，则 $\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}$ 的多项式恒等式测试将属于P类。

3. 此外，DiDI-技术（定理 定理 1.1）直接给出一种黑盒算法，但其递归膨胀的复杂性（指数中的 呈指数级恶化（就 k 而言）。

4.2 $\Sigma^{[k]}\Pi\Sigma\wedge$的多项式恒等式测试

正如我们之前所指出的，定理 1.2(a) 的证明与我们在第4.1节讨论的证明类似。这里我们概述该证明，并说明一些相关的变化。与定理 1.2(b) 类似，我们推广这个定理，并对一个大得多的多项式类给出证明。

问题 4.18。设 $\{T_i \mid i \in [m]\}$ 是次数（语法意义下）至多为 d、规模为 s 的 $\Pi\Sigma\wedge$ 电路。T_i's 的超越次数为 超越次数$_{\mathbb{F}}(T_1, \ldots, T_m) =: k \ll s$。此外，$C(x_1, \ldots, x_m)$ 是一个规模为+ 次数为 $< s'$的电路。请为 $C(T_1, \ldots, T_m)$设计一种黑盒多项式恒等式测试算法。

很容易看出，$\Sigma^{[k]}\Pi\Sigma\wedge$ 是上述设定的一个非常特殊的情形。我们将采用与定理 1.2(b)中相同的思路（和记号），使用雅可比矩阵技术。主要思路是构造一个 Ψ 映射，以及相应的命中集 H'。如果 $g \in L(T_i)$，那么 size(g) $\leq$O(dn)。D（因此 R[x]）保持不变。断言 4.8–4.11 同理成立。我们将通过证明 F 在 R[x] 上有一个规模较小的 $\Sigma\wedge\Sigma\wedge$ 电路，来构造命中集 H'。

注意，对于 $\Sigma\wedge\Sigma\wedge$，断言 4.13 仍然成立（这意味着规模膨胀也相同）。然而，断言 4.14 中的规模膨胀为 O(d size(g))，因为每个单项式 x^e 只能产生 $d+1$ 个单项式。因此，类似于引理 4.16，可以证明 $\Psi(J^{x_k}(g_1,\ldots,g_k)) \in \Sigma\wedge\Sigma\wedge$，其规模为 $O(2^k k! k d s)$。类似地，引理 4.15 中的规模可以替换为 $s^{O(k)}$。因此，我们得到（类似于断言 4.12）：

断言 4.19. *$F \in R[x]$ 具有规模为 $s^{O(k)}$ 的 $\Sigma\wedge\Sigma\wedge$-电路。*

接下来，次数上界也保持不变。按照同样的步骤，不难看出，尽管 z 上的次数上界仍为多项式(ksd)。因此，$P \in \mathbb{F}[x,z]$ 具有规模为 $s^{O(k)}$ 的 $\Sigma\wedge\Sigma\wedge$-电路。

我们希望构造一个集合 $H' \subseteq \mathbb{F}^n$，使得作用$P(H',z) \neq 0$。由引理 2.9，可知它具有规模为$s^{O(k \log\log s)}$的命中集，且可在类似的时间内构造出来。因此，映射 Φ 的构造以及定理（由z-次数上界）得证。

问题 问题 *4.18*的解答。 我们知道

$$C(T_1,\ldots,T_m) = 0 \iff E := \Phi(C(T_1,\ldots,T_m)) = 0.$$

由于H'可在$s^{O(k \log\log s)}$时间内构造，因此显然可以为$E|_{H'}$找到命中集（它只是一个具有上述次数界的$k+2$-元多项式）。最终的E命中集可在$s'^{O(k)} \cdot s^{O(k \log\log s)}$时间内构造出来。

□

5 结论

本文提出了强大的 DiDI 技术，并解决了深度 4 电路多项式恒等式测试中的三个开放问题，即 $\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}$（黑盒）和 $\Sigma^{[k]}\Pi\Sigma\wedge$（白盒与黑盒）。以下是一些值得关注、需要严谨研究的问题。

1. 能否将定理 1.1 中的指数改进为$O(k)$？目前，该指数关于k呈指数增长。 2. 能否将定理 1.2(b)改进为$s^{O(\log\log s)}$（如定理 1.2(a)中那样）？ 3. 能否为 $\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}$设计一种多项式时间多项式恒等式测试？ 4. 为 $\Sigma\wedge\Sigma\Pi^{[\delta]}$ 电路设计一种多项式时间多项式恒等式测试（即顶层扇入无界）？ 5. 对于 $\Sigma^{[k]}\Pi\Sigma M_2$ 电路，能否高效地解决多项式恒等式测试问题（多项式时间/准多项式时间），其中 ΣM_2 表示二元多项式？ 6. 能否为形如 $\Sigma(1/\Sigma\wedge\Sigma)$ 或 $\Sigma(1/\Sigma\Pi)$的有理函数设计一种高效的多项式恒等式测试（对于无界顶层扇入）？

参考文献

[AFS+18] Matthew Anderson、Michael A Forbes、Ramprasad Saptharishi、Amir Shpilka 和 Ben Lee Volk。只读代数分支程序的恒等式测试与下界。ACM《计算理论汇刊》（TOCT），2018年。预备版本发表于 IEEE 31st 计算复杂性会议（CCC'16）。（第7页引用。）[AGKS15] Manindra Agrawal、Rohit Gurjar、Arpita Korwar 和 Nitin Saxena。只读代数分支程序及集合多线性电路之和的命中集。《SIAM计算杂志》，2015年。（第7页引用。）[Agr05] Manindra Agrawal。通过伪随机生成器证明下界。载于《软件技术与理论计算机科学基础国际会议》。施普林格，2005年。（第2页引用。）[AGS19] Manindra Agrawal、Sumanta Ghosh 和 Nitin Saxena。代数电路中的变量自举。《美国国家科学院院刊》，2019。预备版本发表于《计算理论研讨会》，2018年（STOC'18）。（第3页引用。）[AKS04] Manindra Agrawal、Neeraj Kayal 和 Nitin Saxena。PRIMES 属于 P。《数学年刊》，2004年。（第2页引用。）[ALM+98] Sanjeev Arora、Carsten Lund、Rajeev Motwani、Madhu Sudan 和 Mario Szegedy。证明验证与近似问题的困难性。ACM 期刊（JACM），1998年。（第2页引用。）[And20] Robert Andrews。《低特征下的代数困难性与随机性》。载于第35届计算复杂性会议（CCC 2020），2020年。（第3页引用。）[AS98] Sanjeev Arora 和 Shmuel Safra。概率性证明检验：NP类的一种新刻画。ACM 期刊（JACM），1998年。预备版本发表于 33rd计算机科学基础年度研讨会（FOCS'92）。（第2页引用。）[ASS13] Manindra Agrawal、Chandan Saha 和 Nitin Saxena。集合深度-Δ 公式的准多项式规模命中集。载于 45th 年度 ACM 研讨会论文集。

计算理论研讨会（STOC'13），第321–330页，2013年。（参见第5页。）[ASSS16] Manindra Agrawal、Chandan Saha、Ramprasad Saptharishi 和 Nitin Saxena。雅可比矩阵命中电路：击中集、深度-D 出现次数为-k公式的下界，以及深度-3、超越次数为-k的电路。《SIAM计算杂志》，2016年。预备版本发表于 44th 计算理论研讨会，2018年（STOC'12）。（参见第4、5、7、8、20和22页。）[AV08] Manindra Agrawal 和 V Vinay。《算术电路：深度四处的鸿沟》。载于《计算机科学基础》，2008年。FOCS'08。IEEE第49届年度IEEE研讨会，第67–75页。IEEE，2008年。（参见第3页。）[BMS13] Malte Beecken、Johannes Mittmann 和 Nitin Saxena。代数独立性与黑盒恒等式检验。《信息与计算》，2013年。预备版本发表于 38th 自动机、语言与编程国际研讨会（ICALP'11）。（参见第5、6、7和8页。）[BOT88] Michael Ben-Or 和 Prasoon Tiwari。稀疏多元多项式插值的确定性算法。载于 20th ACM年度计算理论研讨会论文集（STOC'88），1988年。（参见第3和10页。）[BS21] Pranav Bisht 和 Nitin Saxena。对数变量常数宽度只读代数分支程序之和的多项式时间黑盒恒等式检验。《计算复杂性》，2021年。（参见第7页。）[CCG12] Enrico Carlini、Maria Virginia Catalisano 和 Anthony V. Geramita。单项式的华林问题及互素单项式之和的解。《代数杂志》，2012年。（参见第12页。）[CKR+20] Prerona Chatterjee、Mrinal Kumar、C Ramya、Ramprasad Saptharishi 和 Anamay Tengse。论代数自然证明的存在。载于IEEE 61st 计算机科学基础年度研讨会（FOCS'20），2020年。（参见第2页。）[CKS18] Chi-Ning Chou、Mrinal Kumar 和 Noam Solomon。有界深度算术电路的困难性与随机性。载于 33rd 计算复杂性会议（CCC'18）。Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik，2018年。（参见第2和6页。）

[DDOS14] Zeev Dvir、Rafael Mendes De Oliveira 和 Amir Shpilka。测试移位下多项式的等价性。载于《自动机、语言与编程国际研讨会》。施普林格，2014年。（参见第2页。）[DDS21a] Pranjal Dutta、Prateek Dwivedi 和 Nitin Saxena。有界顶层扇入四层电路的确定性恒等式测试范式。载于第36届计算复杂性会议（CCC 2021）论文集，2021年。（参见第1页。）[DDS21b] Pranjal Dutta、Prateek Dwivedi 和 Nitin Saxena。揭开三层代数电路边界的奥秘。第62届IEEE计算机科学基础年度研讨会论文集（FOCS 2021），2021年。（参见第5页。）[DL78] Richard A. Demillo 和 Richard J. Lipton。关于代数程序测试的概率性注记。《信息处理快报》，1978年。（参见第3和9页。）[DS07] Zeev Dvir 和 Amir Shpilka。具有两次查询的局部可解码码，以及深度为3的电路的多项式恒等式测试。《SIAM计算杂志》，2007年。（参见第4页。）[DS22] Pranjal Dutta 和 Nitin Saxena。分离边界：近似三层电路的扇入层级指数差距定理。载于2022年IEEE第63届计算机科学基础年度研讨会（FOCS），2022年。（参见第6页。）[DSS22] Pranjal Dutta、Nitin Saxena 和 Amit Sinhababu。发现根：因式分解下代数类的一致闭包结果。《ACM学报》，2022年。预备版本发表于第50届ACM计算理论研讨会（STOC 2018）。（参见第2和7页。）[DST21] Pranjal Dutta、Nitin Saxena 和 Thomas Thierauf。大规模平方和蕴含电路困难性与去随机化。载于第11届理论计算机科学创新会议（ITCS 2021）论文集，2021年。（参见第2页。）[DSY10] Zeev Dvir、Amir Shpilka 和 Amir Yehudayoff。有界深度算术电路的困难性与随机性之间的权衡。《SIAM计算杂志》，2010年。预备版本发表于第40届ACM计算理论研讨会（STOC 2008）。（参见第2和7页。）

[FGS18] Michael A Forbes、Sumanta Ghosh 和 Nitin Saxena。迈向对数变量电路的黑盒恒等式测试。载于第45届自动机、语言与编程国际研讨会（ICALP 2018）论文集，2018年。（参见第7页。）[FGT19] Stephen Fenner、Rohit Gurjar 和 Thomas Thierauf。二分图完美匹配属于准NC。《SIAM计算杂志》，2019年。预备版本发表于 48th ACM计算理论年会（STOC'16）论文集。（参见第2页。）[For14] Michael A. Forbes。只读一次无视代数分支程序的多项式恒等式测试。博士论文，麻省理工学院，剑桥，马萨诸塞州，美国，2014年。（参见第10页。）[For15] Michael A Forbes。通过移位偏导数进行确定性整除性测试。载于 56th 计算机科学基础年会（FOCS'15）论文集，2015年。（参见第4、5、6、11和26页。）[FS13] Michael A Forbes 和 Amir Shpilka。非交换及只读一次无视代数分支程序的准多项式时间恒等式测试。载于 54th计算机科学基础年会（FOCS'13），2013年。（参见第5、7和11页。）[FSS14] Michael A Forbes、Ramprasad Saptharishi 和 Amir Shpilka。任意顺序的多线性只读一次代数分支程序的命中集。载于 46th ACM计算理论年会（STOC'14）论文集，2014年。（参见第7和11页。）[FSV18] Michael A Forbes、Amir Shpilka 和 Ben Lee Volk。简洁击中集及证明代数电路下界的障碍。《计算理论》，2018年。预备版本发表于第51届ACM计算理论年会（STOC 2019）。（参见第2页。）[GGOW16] Ankit Garg、Leonid Gurvits、Rafael Oliveira 和 Avi Wigderson。非交换有理恒等式测试的确定性多项式时间算法。载于 57th计算机科学基础年会（FOCS'16），2016年。（参见第7页。）[GKKS16] Ankit Gupta、Pritish Kamath、Neeraj Kayal 和 Ramprasad Saptharishi。算术电路：深度三处的鸿沟。《SIAM计算杂志》，2016年。预备版本发表于第54届IEEE计算机科学基础年会娱乐国际研讨会论文集。

（FOCS 2013）。（参见第 3 页。）[GKS17] Rohit Gurjar、Arpita Korwar 和 Nitin Saxena。《常数宽度及任意阶只读一次无关算术分支程序的恒等式测试》。《计算理论》，2017年。预备版本发表于第 31 届年度计算复杂性会议（CCC 2016）。（参见第 4、7 和 11 页。）[GKSS22] Zeyu Guo、Mrinal Kumar、Ramprasad Saptharishi 和 Noam Solomon。《基于代数困难性的去随机化》。《SIAM计算杂志》，2022年。预备版本发表于第 60 届 IEEE 计算机科学基础研讨会（FOCS 2019）。（参见第 3 页。）[GKST17] Rohit Gurjar、Arpita Korwar、Nitin Saxena 和 Thomas Thierauf。《只读一次无关算术分支程序之和的确定性恒等式测试》。《计算复杂性》，2017年。预备版本发表于第 30 届年度计算复杂性会议（CCC 2015）。（参见第 7 页。）[GOS22] Abhibhav Garg、Rafael Oliveira 和 Akash Kumar Sengupta。《二次多项式的鲁棒根式 Sylvester-Gallai 定理》。发表于第 38 届国际计算几何研讨会（SoCG 2022），2022年。（参见第 3 页。）[Gro15] Joshua A Grochow。《通过几何复杂性理论统一已知下界》。《计算复杂性》，2015年。预备版本发表于 IEEE 第 29 届计算复杂性会议（CCC'14）。（参见第 2 页。）[GS20] Abhibhav Garg 和 Nitin Saxena。《黑盒根式成员性、零点定理和超越次数的特殊情形算法》。发表于《国际符号与代数计算研讨会论文集》，2020年。（参见第 6 页。）[Guo21] Zeyu Guo。《簇规避子空间族》。发表于第 36 届计算复杂性会议（CCC 2021），2021年。（参见第 6 页。）[Gup14] Ankit Gupta。《深度 4 多项式恒等式测试的代数几何技术及簇的 Sylvester-Gallai 猜想》。发表于《计算复杂性电子学术讨论会》（ECCC），2014年。（参见第 5、6 和 7 页。）

[HS80] Joos Heintz 和 Claus-Peter Schnorr。测试易于计算的多项式。载于 12th 年度 ACM 计算理论研讨会（STOC'80）论文集，1980年。（第 2 页引用。）[JKY16] A Grochow Joshua、D Mulmuley Ketan 和 Qiao Youming。VP 与 VNP 的边界。载于第 43 届自动机、语言与编程国际研讨会（ICALP 2016）论文集，2016年。（第 2 页引用。）[JQS10] Maurice Jansen、Youming Qiao 和 Jayalal Sarma。π-有序代数分支程序的确定性黑盒恒等式测试。载于 IARCS 软件技术与理论计算机科学基础年度会议（FSTTCS 2010），2010年。（第 7 页引用。）[KI04] Valentine Kabanets 和 Russell Impagliazzo。去随机化多项式恒等式测试意味着证明电路下界。《计算复杂性》，2004年。预备版本载于 35th 年度 ACM 计算理论研讨会（STOC'03）论文集。（第 2 页引用。）[KKPS15] Neeraj Kayal、Pascal Koiran、Timoth´ee Pecatte 和 Chandan Saha。低次单变量多项式幂和的下界。载于自动机、语言与编程国际研讨会（ICALP'15），2015年。（第 7 页引用。）[KMSV13] Zohar S Karnin、Partha Mukhopadhyay、Amir Shpilka 和 Ilya Volkovich。有界顶层扇入深度4多线性电路的确定性恒等式测试。《SIAM计算杂志》，2013年。预备版本载于42^{nd} ACM 计算理论研讨会（STOC'10）论文集。（第 5 页引用。）[Koi12] Pascal Koiran。算术电路：深度四处的鸿沟进一步扩大。《理论计算机科学》，2012年。（第 3 页引用。）[KPT15] Pascal Koiran、Natacha Portier 和 S´ebastien Tavenas。关于实数 τ-猜想的朗斯基行列式方法。《符号计算杂志》，2015年。（第 7 页引用。）[KRST22] Mrinal Kumar、C. Ramya、Ramprasad Saptharishi 和 Anamay Tengse。如果 VNP 很难，那么关于它的方程也同样困难。载于第 39 届理论计算机科学国际研讨会

方面（STACS 2022），2022年。（第 2 页引用。）[KS01] Adam R Klivans 和 Daniel Spielman。多元多项式的高效随机性恒等式测试。载于 33rd 年度 ACM 计算理论研讨会（STOC'01）论文集，2001年。（第 3、10 和 21 页引用。）[KS06] Adam Klivans 和 Amir Shpilka。算术电路受限模型的学习。《计算理论》，2006年。预备版本载于 16th 年度学习理论会议（COLT'03）。（第 2 页引用。）[KS07] Neeraj Kayal 和 Nitin Saxena。深度 3 电路的多项式恒等式测试。《计算复杂性》，2007年。预备版本载于 21st 计算复杂性会议（CCC'06）。（第 4 和 6 页引用。）[KS09] Zohar S Karnin 和 Amir Shpilka。有界顶层扇入广义深度-3算术电路的重构。载于 24th 年度 IEEE 计算复杂性会议（CCC'09）。IEEE，2009年。（第 2 页引用。）[KS11] Zohar S Karnin 和 Amir Shpilka。有界顶层扇入广义深度-3算术电路的黑盒多项式恒等式测试。《Combinatorica》，2011年。预备版本载于 23rd 年度 IEEE 计算复杂性会议（CCC'08）。（第 4 页引用。）[KS16] Mrinal Kumar 和 Shubhangi Saraf。少变量多项式乘积之和：下界与多项式恒等式测试。载于 31st 计算复杂性会议（CCC 2016），LIPIcs。Schloss Dagstuhl - Leibniz-Zentrum f¨ur Informatik，2016年。（第 3、5 和 7 页引用。）[KS17] Mrinal Kumar 和 Shubhangi Saraf。具有局部低代数秩的算术电路。《Theory Comput.》，2017年。预备版本载于 31st 计算复杂性会议（CCC'16）。（第 5 和 7 页引用。）[KSS14] Swastik Kopparty、Shubhangi Saraf 和 Amir Shpilka。多项式恒等式测试与确定性多元多项式因式分解的等价性。载于 IEEE 29th 计算复杂性会议（CCC'14）。IEEE，2014年。（第 2 页引用。）

[KST19] Mrinal Kumar、Ramprasad Saptharishi 和 Anamay Tengse。《代数电路击中集的近乎最优自举》。载于 30th 年度 ACM-SIAM离散算法研讨会论文集，第639–646页，2019年。（第3页引用。）[LFKN92] Carsten Lund、Lance Fortnow、Howard Karloff 和 Noam Nisan。《交互式证明系统的代数方法》。ACM 期刊（JACM），1992。（第2页引用。）[LMP19] Guillaume Lagarde、Guillaume Malod 和 Sylvain Perifel。《非交换计算：下界与多项式恒等式测试》。Chic. J. Theor. Comput. Sci.，2019。（第7页引用。）[Lov79] L´aszl´o Lov´asz。《论行列式、匹配与随机算法》。载于《计算理论基础》（FCT'79），1979年。（第2页引用。）[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》。已被 62nd 年度计算机科学基础研讨会（FOCS）接收，2021年，2021年。（第5页和第6页引用。）[Mah13] Meena Mahajan。《代数复杂性类》。CoRR，2013年。预印本见 arXiv:1307.3863。（第9页和第10页引用。）[Muk16] Partha Mukhopadhyay。《深度4恒等式测试与诺特正规化引理》。载于《俄罗斯国际计算机科学研讨会》（CSR'16）。施普林格，2016年。（第5页和第6页引用。）[Mul12a] Ketan D Mulmuley。《几何复杂性理论 V：多项式恒等式测试黑盒去随机化与诺特正规化引理去随机化之间的等价性》。载于 IEEE 第53届计算机科学基础年度研讨会（FOCS'12）。IEEE，2012年。（第2页引用。）[Mul12b] Ketan D Mulmuley。《迈向P与NP问题的GCT计划》。ACM 通讯，2012年。（第2页引用。）[MVV87] Ketan Mulmuley、Umesh V. Vazirani 和 Vijay V. Vazirani。《匹配与矩阵求逆一样容易》。Comb.，1987年。预备版本发表于 19th

ACM计算理论研讨会年会（STOC’87）。（参见第2页。）[Niv69] Ivan Niven。《形式幂级数》。The American Mathematical Monthly，1969年。（参见第7页。）.[Ore22] Øystein Ore。《关于高阶同余》。Norsk Mat. Forenings Skrifter，1922年。（参见第3页和第9页。）[OS22] Rafael Oliveira 和 Akash Kumar Sengupta。《三次多项式的根式 Sylvester-Gallai 定理》。载于2022年 IEEE第63届计算机科学基础年会（FOCS），第212–220页，2022年。（参见第3页。）[PS20] Shir Peleg 和 Amir Shpilka。《二次多项式的广义 Sylvester-Gallai 型定理》。载于计算复杂性会议（CCC’20）。Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik，2020年。（参见第3页和第5页。）[PS21] Shir Peleg 和 Amir Shpilka。《通过二次多项式的 Edelstein-Kelly 型定理实现电路的多项式时间确定性恒等式测试算法》。载于 ACM计算理论研讨会年会（STOC’21），2021年。（参见第3、5和7页。）[PSS18] Anurag Pandey、Nitin Saxena 和 Amit Sinhababu。《正特征域上的代数独立性：新判据及其在局部低代数秩电路中的应用》。计算复杂性，2018年。预备版本发表于国际数学基础研讨会（MFCS’16）。（参见第7页。）[RS05] Ran Raz 和 Amir Shpilka。《非交换模型中的确定性多项式恒等式测试》。计算复杂性，2005年。预备版本发表于 IEEE计算复杂性年会（CCC’04）。（参见第7页和第11页。）[Sap13] Ramprasad Saptharishi。《多项式恒等式测试与下界的统一方法》。博士论文，博士论文，金奈数学研究所，2013年。（参见第10页。）[Sap19a] Ramprasad Saptharishi。《算术电路复杂性中的下界综述》。GitHub综述，2019年。（参见第9页。）

[Sap19b] Ramprasad Saptharishi。私人通信，2019年。（参见第 6 页。）[Sax08] Nitin Saxena。对角电路恒等式测试与下界。载于《自动机、语言与编程国际研讨会》（ICALP'08），第 60–71 页。施普林格，2008年。（参见第 6 页和第 11 页。）[Sax09] Nitin Saxena。多项式恒等式测试的进展。EATCS 通报，2009年。（参见第 9 页和第 10 页。）[Sax14] Nitin Saxena。多项式恒等式测试的进展——II。载于《计算复杂性展望》。施普林格，2014年。（参见第 9 页。）[Sch80] Jacob T Schwartz。用于验证多项式恒等式的快速概率算法。《ACM 期刊》（JACM），1980年。（参见第 3 页和第 9 页。）[Sha92] Adi Shamir。交互式证明系统= 多项式空间。《ACM 期刊》（JACM），1992年。（参见第 2 页。）[Shp09] Amir Shpilka。具有两个乘法门的深度为 3 的算术电路的插值。《SIAM计算杂志》，2009年。预备版本发表于 39th ACM年度计算理论研讨会论文集（STOC 2007）。（参见第 2 页。）[Shp19] Amir Shpilka。二次多项式的 Sylvester-Gallai 型定理。载于 51st ACM SIGACT 年度计算理论研讨会论文集（STOC'19），第 1203–1214 页，2019年。（参见第 5 页。）[Sin19] Amit Kumar Sinhababu。复杂性中的幂级数：代数依赖、因子猜想与 VP 的闭包的命中集。博士论文，博士论文，印度理工学院坎普尔分校，2019年。（参见第 7 页。）[SS11] Nitin Saxena 和 Comandur Seshadhri。深度为 3 的恒等式的近乎最优秩界。《SIAM计算杂志》，2011年。预备版本发表于24^{th} IEEE计算复杂性会议（CCC'09）。（参见第 4 页。）[SS12] Nitin Saxena 和 Comandur Seshadhri。顶层扇入有界的深度为 3 的电路的黑盒恒等式测试：域并不重要。《SIAM计算杂志》，

2012年。预备版本，发表于第 43rd 届 ACM 计算理论研讨会（STOC'11）。（参见第 4、5 和 6 页。）[SS13] Nitin Saxena 和 Comandur Seshadhri。从 Sylvester-Gallai 配置到秩界：改进的深度为 3 的电路黑盒恒等式测试。ACM 期刊（JACM），2013年。预备版本，发表于第 51st 届 IEEE 计算机科学基础研讨会（FOCS'10）。（参见第 4 页。）[SSS13] Chandan Saha、Ramprasad Saptharishi 和 Nitin Saxena。一个关于深度为 3 的恒等式测试、稀疏分解与对偶性的案例。计算复杂性，2013年。（参见第 3、4 和 6 页。）[SV18] Shubhangi Saraf 和 Ilya Volkovich。深度为 4 的多线性电路的黑盒恒等式测试。Combinatorica，2018年。预备版本，发表于43^{rd} 届 ACM 计算理论研讨会论文集（STOC'11）。（参见第 5 页。）[SY10] Amir Shpilka 和 Amir Yehudayoff。算术电路：近期成果与未决问题综述。Now Publishers Inc，2010。（参见第 9 和 10 页。）[Val79] Leslie G Valiant。代数中的完备性类。载于第 11th 届 ACM 计算理论研讨会论文集（STOC'79），1979年。（参见第 2 页。）[Vas04] Wolmer Vasconcelos。交换代数与代数几何中的计算方法。2004年。（参见第 6 页。）[Zip 79] Richard Zippel。稀疏多项式的概率算法。载于国际符号与代数计算研讨会论文集，EUROSAM '79，1979年。（参见第 3 和 9 页。）