arXiv:2602.09302v1 [cs.CC] 10 Feb 2026

概率多项式时间推理理论

Lijie Chen* Jiatu Li† Igor C. Oliveira‡ Ryan Williams§

2026年2月11日

摘要

在这项工作中，我们提出了一种新的有界算术理论，记作 APX_1, ，旨在将理论计算机科学中常用的一大类概率论证形式化。在合理假设下，APX_1 严格弱于此前提出的框架，例如 Je$\check{\mathrm{r}}$´abek 在开创性工作中（2007年）引入的理论 APC_1。从计算角度看，APX_1 与近似计数以及去随机化中的核心问题——prBPP 与 prP 问题——密切相关，而 APC_1 则与对偶弱鸽巢原理以及具有指数电路复杂度的布尔函数的存在性相关。

引入 APX_1 的一个重要动机是，其较弱的公理揭示了更精细的证明论结构，使其成为多个研究方向的自然框架，包括复杂性猜想的不可证性以及随机化下界的逆向数学。特别是，我们为 APX_1构建的框架，能够提出关于在 $deterministic$可行数学中 prBPP =prP 的可证明性的精确问题。由于有界算术中的 P 与 NP 问题的（不可）证性长期以来一直是该领域的核心主题，我们预计这一研究方向会特别引人关注。

我们的技术贡献包括：从较弱的公理出发，为概率推理建立全面的基础；在 APX_1, 中形式化理论计算机科学中的非平凡结果；并针对其中可证明为全定义的 TFNP 问题建立专门的见证定理。作为对形式化理论计算机科学中相关命题所需的最小证明论强度进行分析的副产品，我们解决了一个开放问题：关于在 PV_1,中 AC^0 下界的可证明性。Razborov（1995年）、Kraj´ı$\check{\mathrm{c}}$ek（1995年）以及 M¨uller 和 Pich（2020年）此前都曾研究过这一问题。

*加州大学伯克利分校。电子邮箱： lijiechen@berkeley.edu

†麻省理工学院。电子邮箱： jiatuli@mit.edu。本研究得到美国国家科学基金会资助，项目编号为 CCF 2420092。

‡华威大学。电子邮箱： igor.oliveira@warwick.ac.uk。本研究部分得到英国研究与创新署前沿研究保障基金 EP/Y007999/1 以及华威大学离散数学及其应用中心（DIMAP）的资助。§麻省理工学院。电子邮箱： rrw@mit.edu。作者访问新泽西州普林斯顿高等研究院期间完成了本研究的部分工作。本材料基于美国国家科学基金会资助的研究，资助项目编号为 DMS-2424441（高等研究院）和 CCF-2420092（麻省理工学院）。

目录

1 引言 1 1.1 概述.1 1.2 主要贡献.4 1.2.1 APX_1 理论.4 1.2.2 APX_1 中的概率推理.6 1.2.3 APX_1中的理论计算机科学.7 1.2.4 APX_1, 的见证、相对强度及 prBPP =prP 的可证明性.8 1.2.5 随机化与平均情形下界的逆数学.10 1.3 技术.11 1.3.1 APX_1中的概率推理：“从逐点到整体”技巧（第 1.2.2 节） 12 1.3.2 电路下界的可证明性（定理 1.6 和 1.7）.13 1.3.3 见证定理（定理 1.9）.14 1.4 相关工作.15

2 理论的形式化定义17

2.1 记号.172.2 APX 理论APX .19APX 的模型APX .20一阶理论APX_1 .22

3 APX 中的概率推理$_1$ 23

3.1 近似计数的一致性 .233.1.1 近似计数的全局一致性 .243.1.2 近似计数的置换对称性 .253.1.3 近似计数的存在性引理 .263.1.4 具体电路的近似计数 .27

3.2 近似期望及其基础理论 .29

3.2.1 随机变量与近似期望的定义 .293.2.2 近似期望的基本性质 .303.2.3 期望的平均论证.323.2.4 补集.343.2.5 期望的线性性 .34

3.3 概率不等式.35

3.3.1 并集界.353.3.2 马尔可夫不等式.363.3.3 方差与切比雪夫不等式.373.3.4 两两独立性与方差.39

3.4 独立性 性、误差缩减与集中界.4

23.4.1 显式独立性.423.4.2 乘法原理.433.4.3 单边错误陈述的误差缩减.463.4.4 Chernoff（Log n）随机变量的切尔诺夫界.47

4 理论计算机科学 计算机科学中的APX_1 4 9

4.1 姚期智的区分器到预测器转换 .504.2 Schwartz-Zippel引理 .524.3 线性哈希 .544.4 针对以下类别中奇偶性的下界 AC^0 电路 .554.4.1 限制的确定性子集选择 .564.4.2 APX中的平均情形下界 APX_1 .59

4.4.3 PV中的最坏情形下界PV_1 .634.5 Blum-Luby-Rubinfeld 线性测试 .654.5.1 两个有用引理 .66
4.5.2 BLR 线性测试的完备性 .684.5.3 多数纠正的正确性 .694.5.4 BLR 线性测试的可靠性 .71

5 APX 的见证定理与相对强度$_1$ **73**
5.1 APX 中可证明全定义的 TFNP 问题$_1$ .73 5.1.1 一个 TFZPP 问题：Refuter(Yao).73 5.1.2 与 LossyCode 的联系.74 5.1.3 见证定理.75 5.2 与 PV_1的关系：prBPP $=$prP 是否可行证明？.76 5.3 与 APC_1的关系.77 5.3.1 一个上界：APC_1 扩展 APX_1 .78 5.3.2 条件分离：APC_1 可能比 APX_1 更强.78 5.3.3 一个开放问题：是否存在更多分离？.79 5.4 预测器提取引理：引理 5.6 的证明.79 5.5 用 NW(C, Δ) 模拟 P(C, Δ)：定理 5.9 的证明 .84 5.6 APX_1 的 KPT 见证定理：定理 5.12 的证明 .86

6 随机化与平均情况下界的逆向数学 **86**
6.1 收缩鸽巢原理的变体 .876.2 单向通信下界 .886.3 通信复杂度的主要等价性结果 .896.3.1 压缩蕴含通信上界：(12) $\Rightarrow$ (4) .906.3.2 从通信上界压缩：(1) $\Rightarrow$ (5).916.3.3 压缩的伸长归约：(2) $\Rightarrow$ (3) .92
6.3.4 最坏情形到平均情形归约：(4) $\Rightarrow$ (1) .94

1 引言

1.1 概述

有界算术扩展了传统的复杂性理论：它不仅刻画算法所需的计算资源（例如运行时间或电路规模），还刻画证明其正确性的复杂性。通过在统一框架中整合计算复杂性与证明复杂性，它为理论计算机科学中的基础问题开辟了新的视角。该领域历史悠久（参见[HP93、Kra95、CN10、Kra19] 及其中的参考文献），并借助新的形式化 [BKKK20、Gay24、Kha24、AAdRK25]；不可证性结果 [PS21、LO23、ABM23、CLO25、CRT25、Tha25]；与TFNP的联系 [LLR24], 复分析 [Jeˇr23], 逆向数学 [CLO24、AT25], 复杂性下界 [GC25、CKK+25]，以及命题证明复杂性 [Kra25]；还有在密码学中的应用 [JJ22、JKLV24、JKLM25、JJMP25], 等进展而重新获得发展势头。关于背景以及与算法和复杂性理论的联系，我们推荐参阅 [Bus97、Oli25]。

两种核心且受到广泛研究的理论是 Cook 的 PV_1 [Coo75、KPT91] （另见 [Kra19、Li25]）以及 Jeˇr´abek 的 APC_1 [Jeˇr04、Jeˇr05、Jeˇr07a]。理论 PV_1 将多项式时间推理形式化，并涵盖算法与复杂性中的许多经典结果。由于随机化算法是否通常能够去随机化尚不明确，PV_1 并不适合用于概率推理或分析随机化算法。理论 APC_1 通过加入对偶弱鸽巢原理 dWPHP(PV)，扩展了 PV_1，从而为概率推理和随机化构造提供了一个方便的框架。特别是，APC_1 （及其温和扩展）足以将若干非平凡结果形式化，包括图问题中随机化算法的正确性 [LC11], 、多项式恒等式测试 [AT25], 以及电路下界 [MP20]。然而，APC_1 的公理可能强于必要程度：许多值得关注的结果或许能够在一个更弱、且更接近 PV_1的理论中得到证明。

有具体理由认为，APC_1 的强度会超过概率多项式时间推理所需的最低强度。一方面，APC_1 与 dWPHP(PV) 以及指数电路复杂度函数的存在性相关；从计算角度看，这类函数的显式构造（即电路下界）是一种广泛使用的去随机化假设，其强度可能高于 prBPP 的去随机化（参见例如 [For01、Gol11、CT23]）。另一方面，即使 prBPP = prP 可通过“可行”的证明得到，APC_1 也不一定会坍缩为 PV_1；事实上，在合理的密码学假设下，APC_1严格强于 PV_1 [ILW23]。

寻找一种较弱的理论，同时仍能支撑理论计算机科学中广泛使用的各类概率论证，这一目标受到若干因素的推动：

- 复杂性理论猜想的不可证性。这一领域的核心目标之一，是找出既能形式化复杂性理论中现有工具、又适合开展不可证性研究的框架。APC_1 很可能严格强于PV_1 根据 [ILW23], ，即使prBPP = prP，其见证函数通常也无法变为确定性的，这使不可证性论证变得复杂，并带来重大挑战（参见例如 [LO23、CKKO21]）。尤其是，引入强原理dWPHP(PV) 是将复杂性下界的不可证性从PV_1 [PS21]扩展到APC_1 [LO23]的主要障碍。

- 带概率推理的有界逆向数学。 受近期进展（如[CLO24、AT25] （相关背景另见 [CN10] ））的启发，我们可以尝试对算法和复杂性理论进行系统的逆向数学研究，按照所用公理对“概率证明”进行分类。同样，这也表明，可以根据随机化算法的正确性证明的复杂性对其进行分类，以补充通过空间复杂度（例如参见 [Nis92]）或电路复杂性（例如参见 [AW89]）进行的标准分类。这一视角对于去随机化可能颇具启发性，具体而言，就是基于正确性证明的证明复杂性进行去随机化。由于 dWPHP(PV) 本身就很强，APC_1 对于比 dWPHP(PV) 弱的精细对应关系而言，是一种过于强大的基础理论。

- 密码学中的正确性证明。Jain 和 Jin [JJ22] 及后续论文 [JKLV24、JKLM25,

JJMP25、MDS25] 探讨了PV_1及其与命题证明的联系，以帮助构造 $i\mathcal{O}$ 及其他密码学原语，强调证明某些陈述的逻辑复杂性可能在密码系统及其效率中发挥重要作用。特别是，[JJMP25、JKLM25] 高度依赖于带有PV_1 正确性证明的密码学原语。然而，现有工作通常考虑“完美正确性”，因为PV_1 无法原生地讨论近似计数和随机性，而APC_1 对于这一目的而言似乎既过强又不便。

- 概率陈述的可行可证明性。人们自然会精确表述 $\mathsf{prBPP} = \mathsf{prP}$ 及相关问题的可证明性的可行概念。然而，即便对 $\mathsf{prBPP} = \mathsf{prP}$ 作可行表述也并非平凡，因为它似乎首先要求在该理论内部定义概率计算。鉴于 $\mathsf{P} = \mathsf{NP}$ 在 PV_1 中的（不）可证明性长期以来一直是有界算术的核心问题（参见例如 [CK07、Oli25]），这一方向对于推进随机化计算与数学证明之间相互作用的研究具有重要潜力。

这些考量指向一个共同目标：设计一个用于在可行数学中推理概率与随机化构造的最小理论。

贡献概述。 我们提出一个在强意义上对应于“概率多项式时间推理”的理论。我们的主要概念性与技术性贡献如下：

1. **理论 APX_1 及其相对强度。** 我们引入 APX_1，，确立其基本性质，并发展核心概率工具。该理论扩展了 PV_1，并且在如下意义上包含于 APC_1，：它在 APC_1 语言中的所有推论在 APC_1 中也都可证。此外，在合理假设下，APX_1 严格弱于 APC_1。

2. **高级形式化。** 我们在 APX_1 中形式化了算法与复杂性领域的若干非平凡结果，包括布卢姆-卢比-鲁宾菲尔德线性测试、Schwartz-Zippel引理[1]，以及关于奇偶性的平均情况 AC^0 下界。此外，作为对有界算术中 AC^0电路进行精细分析的副产品，我们给出了一个相匹配的 PV_1最坏情形下界。后一个形式化处理了 Razborov Raz95]，Krajíˇcek [Kra95第15节2],以及 M¨uller-Pich MP20],提出的问题，而该问题此前仅在更强的理论中得到解决。

3. **量身定制的见证定理。** 我们证明，APX_1 中可证明全定义的 NP 关系可确定性地归约到一个自然的 TFZPP 问题[2] —— Refuter(Yao)，该问题由我们提出。此外，若 $\mathsf{prBPP} = \mathsf{prP}$，则 APX_1 具有确定性多项式时间见证。

4. **可行去随机化。** 借助新的框架，我们提出了对这一基本问题的自然形式化：$\mathsf{prP} = \mathsf{prBPP}$ 是否可行证明？换言之，是否存在关于一般去随机化的确定性可行证明？

5. **随机性的逆向数学。** 最后，我们展示 APX_1 可作为发展平均情况下界和随机化下界之逆向数学的合适基础理论，这里通过研究随机化通信协议及其通信复杂性来加以说明。

在更详细地介绍我们的结果之前，我们先补充一些背景和上下文。

在 dWPHP(PV) 中同时用于 APC_1。 为什么 APC_1，迄今为止已知能够形式化概率和随机化算法的最弱理论，却似乎强于必要程度？通过考察 APC_1 [Je˘r04、Je˘r05、Je˘r07a]，的构造，我们发现引入 dWPHP(PV) 有两个不同的原因。

[1]值得注意的是，Schwartz-Zippel引理的标准证明（例如，参见 [AB09，引理 A.36]）目前尚不知能否在 APC_1 中形式化。在本工作中，我们在 APX_1 中形式化了 Atserias 和 Tzameret [AT25] 提出的一种替代证明。[2]若对于每个输入 x，至少有逆多项式比例的字符串 y 是有效解，即 $R(x,y) = 1$，则称 TFNP 问题 $R(x,y)$ 属于 TFZPP。显然，TFZPP 问题存在简单的零错误随机算法，能够在多项式时间内运行。

- 首先，它被用于实现近似计数。Jeˇr´abek [Jeˇr04] 证明，dWPHP(PV) 能够证明存在一个指数级难的布尔函数；通过在理论 PV_1中形式化 Nisan-Wigderson 伪随机生成器 [NW94] 某种形式的正确性，我们可以用这个难布尔函数实例化该伪随机生成器，从而近似计算电路的接受概率。

- 其次，它还可作为计数原理，用于推导组合学和概率论中的工具，包括容斥原理、并界和切尔诺夫界 [Jeˇr07a，第 2]节。

第一种作用似乎不可或缺，因为近似计数是概率多项式时间算法形式化的基础。然而，作为一种计数原理，dWPHP(PV)似乎过于强大，许多应用并不需要它。

Remark 1.1（dWPHP的计算方面）。为了补充背景，dWPHP(PV) 断言，对于任意函数 f，若其由电路实现，且其陪域远大于其定义域，例如 $f\colon \{0,1\}^n \to \{0,1\}^{n+1}$，则陪域中存在一个没有原像的字符串。该原理的计算方面，即给定函数 f后寻找这样一个字符串的搜索问题，近来引起了计算复杂性领域的关注（综述见 [Kor25]）。这个问题如今称为 *Range AvoidanceProblem* [KKMP21、Kor21、RSW22], ; 在合理假设下，已知即使对于非确定性搜索算法，该问题也很难 [ILW23、CL24]。

在APX_1中公理化近似计数。由于 dWPHP(PV) 在 APC 中承担两项关键功能，因此构建一个更弱的理论并非易事——必须找到一种放宽计数原理的方法，同时不牺牲形式化近似计数的能力。

我们的方法事后看来相当自然：将近似计数置于基础地位，使之成为核心原始概念，而不是从诸如 dWPHP(PV)[Jeˇr04、Jeˇr05、Jeˇr07a]等更强的原理推导出来。我们以PV_1 为基础理论，直接引入一个旨在执行近似计数的预言机，并用适当的公理对其加以约束。通过这种方法，我们将近似计数的概念与计数原理分离开来。

主要的技术挑战在于选择一组合适的公理。这些公理应足够强大，以支持我们开展高级形式化、证明逆向数学结果，并有望得到理论计算机科学中的更多结果。同时，公理集又应尽可能精简。这两个相互矛盾的目标使得选择合适的公理颇为困难；事实上，甚至无法先验地确定，是否存在一组无需诉诸 dWPHP(PV) 变体的有限公理。

或许令人意外的是，我们提炼出了四条简单直观的公理，足以实现我们的所有结果；其中唯一非平凡的公理刻画了近似计数预言机的“局部”行为。可以说，这使 APX_1 成为概率多项式时间推理最小理论的一个合理候选。

Remark 1.2（去随机化的最小假设）。猜想 prBPP $\subsetneq$prP 是去随机化中的核心问题。Impagliazzo、Nisan 和 Wigderson 的著名结果 [NW94, IW97] 在 E $\not\subseteq$ i.o.-SIZE$[2^{\Omega(n)}]$这一合理的最坏情况电路下界假设下，给出了肯定答案。反过来，已知去随机化结果也能推出较弱的电路下界，例如 NTIME$(n^{\omega(1)}) \not\subseteq$ P/poly （参见 [IKW02, Wil14, Tel19]）。然而，长期以来，一个开放问题是：在 [NW94, IW97] 中使用的强电路下界，是否 *necessary* 能用于证明 prBPP $=$ prP。事实上，已有大量进展表明，去随机化可能 *not* 需要强电路下界（参见 [For01, Gol11, CT21]）。此外，近期还发现了若干关于 prBPP $=$ prP 的 *characterizations* 结果 [LP22, Kor22, CT23, CTW23, LPT24], , 其动机是理解去随机化所需的 *minimal* 假设。

我们旨在提出一种 *minimal theory* 足够强大的理论，以便对概率多项式时间算法开展有意义的可行证明。具体而言，我们提供证据表明，dWPHP(PV) 以及困难布尔函数的存在性——它们是 Jeˇr´abek 的理论 APC_1 [Jeˇr04、Jeˇr05、Jeˇr07a], 的基础——对于概率多项式时间推理的最小理论而言，或许并非必需。

从某种意义上说，我们的结果试图在证明复杂性的背景下回答一个类似的问题

1.2 主要贡献

现在，我们将详细阐述我们的贡献及其影响。

1.2.1 APX 理论

如上所述，我们不从更强的组合原理推导概率（如 APC_1通过 dWPHP(PV)），而是直接将近似计数公理化。我们的目标是构造一种较弱的理论：在其中，任何可有效定义的事件[3] 的概率都可以命名，并且可以在允许加性松弛的情况下进行推理，同时保持较低的证明论强度。

为此，我们引入一阶有界算术理论 APX_1, ，其核心原语是一个近似计数函数 P。直观地说，给定一个作用于 n 个输入位的布尔电路 C 以及一个精度参数 Δ，项 $\mathsf{P}(C, \Delta)$ 返回一个 $[0,1]$ 中的有理数，该数在加性误差 $1/|\Delta|$ 范围内近似于 C 的接受概率，其中 $|\Delta|$ 表示输入参数 Δ 的位长。为方便起见，我们通常写作 $\mathsf{P}_\delta(C)$，而不是 $\mathsf{P}(C, \Delta)$，其中 $\delta = 1/|\Delta|$。

APX_1, 的等式核心称为 APX，它是在 Cook 的等式理论 PV 上加入预言机符号 P（新语言记作 PV(P)）及其支配公理而得到的。APX_1 则是 APX 通常的一阶闭包，即 APX 方程的全称闭包，以及标准的 PV 风格的记号归纳。

> *Remark* 1.3（PV 与 PV_1）。PV [Coo75] 是一种等式理论，其预期模型是 $\mathbb{N}$，其中基本符号（如 0、 $+$和 $\times$）按通常方式解释。其语言为每个多项式时间算法 $f\colon \mathbb{N}^k \to \mathbb{N}$ （对任意固定的 k）都包含一个函数符号；这些符号及其定义公理由 Cobham 对多项式时间函数的刻画给出。该理论包含一个形式化二分搜索的归纳方案，特别是，它证明了无量词公式（即多项式时间谓词）的归纳法。标准的一阶扩展是 PV_1 [KPT91]。尽管 PV_1 的形式化定义相当技术性，但该理论具有稳健性：不同的表述会导出相同的定理。例如，PV_1 有一种等价的公理化方式，无需使用 Cobham 定理 [Je˘r06]；或者，也可以将其表述为 Buss 的理论 S^1_2 [Bus86] 中所有可证明的 $\forall\Sigma^b_1$- 句子的集合。简要概述可参阅 [Oli25]，详细介绍可参阅 [Li25]。

APX_1 定义的一个关键方面是采用约束 P_δ行为的“局部”条件，这些条件共同确保所需的“全局”行为，即 P_δ 对任意输入电路的接受概率进行近似，误差不超过加性误差项 δ。APX_1 的整套概率机制（随机变量、期望、尾界等）都建立在以下公理之上。

APX_1 约束 P 的公理。所有公理都是全称 PV(P)-方程；下面的 $\beta^{-1} \in \mathsf{Log}$ 是一个可自由使用的“松弛”参数，用于吸收常见的有限精度效应。[4] 我们以非正式的方式概述这些陈述；正式版本见第 2 节。

- **基本公理。** 对于任意布尔电路 C和 Δ，值 $\mathsf{P}(C, \Delta)$ 是 $[0,1]$ 中的一个有理数（以 PV 编码），并且所有 PV(P) 可证方程都成立。再结合 $\mathsf{P}(C, \Delta)$ 的输出长度界，即可确保能够按任意指定精度进行近似计数。

- **边界公理。** 如果 C 在语法上是常元（不读取任何输入），那么 $\mathsf{P}_\delta(C) \in \{0,1\}$ 与 C的输出位一致。因此，P 在平凡情形下是精确的 。

- **精度一致性。**对于任意两个精度 δ_1, δ_2 以及电路 C,

$$\left|\mathsf{P}_{\delta_1}(C) - \mathsf{P}_{\delta_2}(C)\right| \;\le\; \delta_1 + \delta_2 + \beta.$$

[3]换言之，存在一个多项式规模布尔电路 C，使得对于事件 $E \subseteq \{0,1\}^m$， $C(x) = 1$ 当且仅当 $x \in E$。[4]表达式 $\beta^{-1} \in \mathsf{Log}$ 是有界算术中用于表示以下含义的标准记号：对于某个变量 y， $\beta = 1/|y|$，其中 $|y|$ 是 y的位长。

因此，要求更高的精度只会使报告的概率改变指定错误参数之和（至多为 β）。

- **局部一致性**。 如果 C 至少有一个输入位，且 $\mathsf{Fix}_b(C)$ 表示将最右侧输入位固定为 $b \in \{0,1\}$ 后得到的电路，那么

$$\left| \mathsf{P}_\delta(C) \;-\; \tfrac{1}{2}\big(\mathsf{P}_\delta(\mathsf{Fix}_0(C)) + \mathsf{P}_\delta(\mathsf{Fix}_1(C))\big) \right| \;\le\; 2\delta + \beta.$$

  因此， C 所报告的接受概率（允许有 β 的加性松弛）等于固定一个新的随机位后所报告概率的平均值。此举旨在刻画在均匀超立方体上计数的预期语义。[5]

实践中，可以将 APX_1 视为在 PV_1 的基础上扩展而成的理论：加入符号 P 及其支配公理，并在语言 PV(P) 中加入对无量词公式的归纳法。其余内容——例如随机变量、期望、并集界等——都将在 APX_1 内通过该语言和公理引入并推导得出。

近似计数在 APX_1 中的可靠性。 我们称一个 PV-标准模型（即 $\mathbb{N}$），其中函数符号 P 被解释为任意正确的近似计数函数（返回一个与真实值相差不超过 $\pm 1/|\Delta|$ 的有理数，且对语法上为常值的电路给出精确值），为 APX_1 的 标准模型。一个简单但核心的结果表明，这些模型恰好就是 满足这些公理的模型（“容许模型”），从而保证预期解释下的语义可靠性，并在底层模型为 $\mathbb{N}$ 时，为近似计数提供正确的公理化（见第 2.3 节）。

APX_1 的最小性。 我们认为，APX_1 是概率多项式时间推理的最小理论的一个良好候选。从数学角度来看，这并非一个形式化断言。然而，上述公理似乎接近于能够一致地定义和运算可行描述事件的近似概率的最弱可用基础理论。具体而言：

- 任何关于概率多项式时间算法进行推理的理论都应能够定义这些算法的接受概率。这要求具备带有加性误差的近似计数能力，即符号 P。

- 由于基本公理和边界公理只是对预言机 P 的相当语法化的承诺，我们预计它们是可用的。可以说，精度一致性公理断言 P 在不同精度参数下的一致性，也应该是可用的。注意，这三个公理并不充分，因为人们可以轻易地指定一个平凡且错误的多项式时间函数，使得这些公理在 PV_1 中可证。

- 因此，我们使用局部一致性公理 来刻画 P 的正确性——它表明，近似计数预言机能够通过一项简单的统计检验，而该检验在整个证明过程中会进行三次查询。我们认为，很难利用一个可能无法通过此检验的预言机来进行有实质意义的近似计数；因此，这条公理似乎也是必要的。

关于其最小性的另一项证据是，APX_1 在计算意义上，函数符号P 与电路接受概率问题(CAPP)相对应，后者是prBPP 的完全问题（例如，参见 [Vad12]）。相比之下，范围规避问题对应于dWPHP(PV)，与 APC_1，有关，而且即使面对非确定性算法，它也很可能是困难的 [ILW23，CL24]。

[5] $X \subseteq \{0,1\}^n$ X X_0 X_1 $X_b = \{x \in$ 换句话说，对于每个（可有效定义的）集合，由于 $X \mid x_n = b\}$ $|X| \approx |X_0| + |X_1|$ 是 与 的不相交并，其中，我们预期 。

1.2.2 APX中的概率推理[1]

我们在 APX_1 中构建一个自成一体的"概率演算"，并使用近似计数函数 P_δ。作为预备步骤，我们证明 P_δ 在可行描述的事件上表现符合预期。具体而言，APX_1 建立了以下性质（每项都允许任意小的加性松弛 $\beta^{-1} \in \mathsf{Log}$）：

- **语义不变性**。P_δ 尊重语义等价，即如果 APX_1 证明电路 C 和 D计算的是同一个函数，那么 $\left|\mathsf{P}_\delta(C) - \mathsf{P}_\delta(D)\right| \leq 2 \cdot \delta + \beta$ (引理 3.2)。
- **置换不变性**。对输入位进行置换不会显著改变P_δ的值。换言之，对于任意电路 C 以及输入位的任意置换 π，$\left|\mathsf{P}_\delta(C \circ \pi) - \mathsf{P}_\delta(C)\right| \leq 2 \cdot \delta + \beta$ (引理 3.5)。
- **通过概率方法得到存在性**。假设电路 C 所接受的字符串被视为 良好。那么，如果良好字符串足够多，即相对于精度参数 $\delta + \beta$，其比例超过 δ，则必定存在一个良好字符串（引理 3.6）。更正式地说，

$$\mathsf{APX}_1 \vdash \forall n, \delta^{-1}, \beta^{-1} \in \mathsf{Log}\ \forall C\ (\beta > 0 \wedge \mathsf{P}_\delta(C) > \delta + \beta \rightarrow \exists x \in \{0,1\}^n\ C(x) = 1).$$

- **具体电路上的一致性**。P_δ 与简单测试相符。例如，对于一个自然定义的阈值电路 $C_{<t}(x)$，其输入为 n 位，仅当 x （视为整数）小于t时才接受，$\mathsf{P}_\delta(C_{<t}) \approx t/2^n$ （见第3.1.4节）。

这些元性质确保在 APX_1 中建立的定义和不等式仅产生微小且明确受控的加性损失，同时保留预期的概率行为。

有了这些保证，我们现在引入可行随机变量。随机变量 X 由显式支撑集 $V \subseteq \mathbb{Q}$、种子长度 n和多输出采样器电路 C 指定：$\{0,1\}^n \to V$。其近似期望通过在指示布尔电路 $\{C_v\}_{v \in V}$上查询 P_δ 来定义，其中 $C_v(z)$ 当且仅当 $C(z) = v$时接受 z。换言之：

$$\mathbb{E}_\delta[X] \triangleq \sum_{v \in V} v \cdot \mathsf{P}_\delta(C_v).$$

我们注意到，存在一个 PV(P) 函数 $\mathsf{E}(V, n, C, \Delta)$，它计算由 (V, n, C) 定义的随机变量X的 $\mathbb{E}_{|\Delta|^{-1}}[X]$。具体而言，E 枚举所有 $v \in V$，构造相应的电路 C_v，查询预言机以获得 $p_v \leftarrow \mathsf{P}(C_v, \Delta)$，并输出总和 $\sum_{v \in V} v \cdot p_v$。

我们引入一种核心技术工具，它为期望的平均论证（第3.2.3节）提供了一个通用版本：给定在相同种子上定义的随机变量 X_1、……、X_m 以及系数 λ_1、……、λ_m，APX_1 可以搜索种子的一个后缀 z，使得固定该后缀后，数值 $\sum_i \lambda_i \cdot \mathbb{E}_\delta[X_i]$ 的下界近似保持不变。这一技术被反复用于在全局和逐点陈述之间转换，也是若干结果证明的基础。我们将在第1.3节更详细地介绍这一技术。

利用上述工具并结合一些额外思路，APX_1 推导出了若干标准概率不等式的近似表述。具体而言，它证明了对可行随机变量的线性组合成立的期望的线性性、适用于多项式数量事件的并集界，以及适用于非负变量并具有通常 $1/k$ 衰减率的马尔可夫不等式。[6]

Remark 1.4（示例：APX_1中的并集界；参见定理 3.20）。APX_1 证明了以下陈述。设 $n, m, \delta^{-1}, \beta^{-1} \in \mathsf{Log}$、$C_1$、……、$C_m$ 为单输出电路，且 $V = \{0,1\}$。假设 $\forall x \in \{0,1\}^n$ 和 $i \in [m]$, $C_i(x) \in V$，并令 $Y, X_1, \ldots, X_m$ 为如下定义的随机变量。

- 对于每个 $i \in [m]$，X_i 由 (V, n, C_i) 定义。
- Y由 (V, n, S) 定义，其中 $S(x) \in \{0,1\}$ 是一个电路，满足 $S(x) \leq C_1(x) \vee \cdots \vee C_m(x)$。

[6]我们注意到，一些结果会遭受近似损失，该损失取决于 $\|V\| \triangleq \sum_{v \in V} |v|$ 以及所涉及系数的大小，其中此处 $|\cdot|$ 表示绝对值。在这些量有多项式界的应用中，可以通过在应用 $\mathbb{E}_\delta[X]$时选取足够小的参数 δ 和 β 来减轻这一问题。

那么我们有 $\mathbb{E}_\delta[Y] \le \mathbb{E}_\delta[X_1] + \cdots + \mathbb{E}_\delta[X_m] + (2\delta + \beta) \cdot m$。

此外，APX_1 定义了一个近似方差$\mathrm{Var}_\delta[X] \triangleq \mathbb{E}_\delta\big[(X - \mu)^2\big]$，其中 $\mu \triangleq \mathbb{E}_\delta[X]$，并证明了形如 $\mathrm{Var}_\delta[X] \approx \mathbb{E}_\delta[X^2] - \mu^2$ 的恒等式，由此得出切比雪夫不等式的一种自然表述。APX_1 还通过近似协方差形式化了（几乎）两两独立性，并证明，对于（几乎）两两独立的变量，和的方差近似等于各变量方差之和。

最后，我们讨论独立性与集中性。我们在 APX_1 中研究显式独立性：变量由种子的互不相交部分抽样得到。在这一概念下，理论证明了乘法原理

$$\mathbb{E}_\delta[XY] \;\approx\; \mathbb{E}_\delta[X] \cdot \mathbb{E}_\delta[Y],$$

并且对于伯努利变量，还给出了一个方便的乘积界

$$\left|\mathbb{E}_\delta\Big[\textstyle\prod_{i=1}^m X_i\Big] - \prod_{i=1}^m \mathbb{E}_\delta[X_i]\right| \;\le\; 8\delta \cdot m.$$

由此可得单侧错误约简。此外，APX_1 还证明了一个切尔诺夫界，适用于 $m = O(\log n)$ 个独立同分布的伯努利随机变量之和；该界具有标准的指数尾，并且加性松弛可控。

Remark 1.5（示例：APX_1 中的单侧错误约简；见定理 3.33）。对于一个布尔电路 $C\colon \{0,1\}^n \to \{0,1\}$，令 $C^{\vee k}\colon \{0,1\}^{nk} \to \{0,1\}$ 为按 $C^{\vee k}(x_1, \ldots, x_k) \triangleq \bigvee_{i\in[k]} C(x_i)$ 定义的电路。以下陈述可在 APX_1 中证明。对于任意 n, k，$\delta^{-1}, \beta^{-1} \in \mathsf{Log}$ 和 $C\colon \{0,1\}^n \to \{0,1\}$，若 $\mathrm{P}_\delta(\neg C) \le \varepsilon$，则 $\mathrm{P}_\delta(\neg C^{\vee k}) \le (\delta + \beta + \varepsilon)^k + \delta + \beta$。

关于这些不同概念和结果如何在APX中实现的详细说明，请参见第 3 $_1$节。

1.2.3 APX_1中的理论计算机科学

如上所述，近似计数——如 APX_1 中公理化的那样——足以构建典型的概率工具集（例如存在性论证、期望的线性性、平均论证、并集界、马尔可夫不等式、切比雪夫不等式、有限独立性、误差缩减，以及适用于对数数量样本的 Chernoff 版本）。这个轻量而稳健的框架可用于形式化若干非平凡结果。我们通过对理论计算机科学不同领域中一系列有影响力的结果进行详细形式化，来说明这一点：

- 姚期智的区分器到预测器转换借助混合论证实现，这是计算伪随机性中的核心工具（见定理 4.1）；
- Schwartz-Zippel引理（如 [AT25]中所述）是关于多项式恒等式测试的代数结果，在随机性和复杂性领域有广泛应用（见定理4.4）；
- 电路复杂性中，有界深度多项式规模电路针对奇偶函数的经典下界（参见第 4.4节）；
- 次线性时间算法和性质测试中的布卢姆-卢比-鲁宾菲尔德线性测试的正确性（参见第4.5节）。

为使讨论具体化，并将我们的结果与先前工作进行对比，我们在此聚焦于对 n 位奇偶函数电路下界的形式化表示，该函数记作 $\oplus_n$。事实上，我们证明，在 APX_1 中可以证明针对深度为 d 的布尔电路（AC^0_d）的更强平均情况 下界。

定理 1.6（平均情况 AC^0 下界，适用于 $\oplus_n$ 在 APX_1中。 对于所有常元 k、$d \ge 1$，都存在一个常元 $n_0 \ge 1$，使得 APX_1 证明以下陈述。令 n、δ^{-1}、$\beta^{-1} \in \mathsf{Log}$、 $n > n_0$，以及

C： $\{0,1\}^n \to \{0,1\}$ 是一个大小至多为 n^k 的AC^0_d 电路。令 T_C： $\{0,1\}^n \to \{0,1\}$ 为这样一个电路：给定 $x \in \{0,1\}^n$，当且仅当 $C(x) = \oplus_n(x)$ 时输出1 。那么

$$\mathsf{P}_\delta(T_C) \leq \frac{1}{2} + \frac{1}{n^k} + \delta + \beta. \tag{1.1}$$

主要的技术挑战在于避免使用“基于编码的计数论证”（鸽巢原理的变体），因为这类论证在APX_1，中不可用，例如 Razborov 证明切换引理时所用的方法 [Raz95]。相反，我们的证明建立在 Furst、Saxe 和 Sipser 的一种技术之上 [FSS84]。这一方法由[AAI+01] 进一步改进（另见 [Agr01]），他们给出了一个确定性多项式时间算法，输出切换引理所提供的适当限制。我们的贡献之一是证明，在 [AAI+01] 中，该算法的正确性可以在APX_1内得到确立。结合上述概率工具和其他思想，便可得到平均情况下界APX_1。

作为我们改进后的证明论框架的推论，并经过一些额外工作，我们可以从上述形式化中提取出一个在较弱理论 PV_1 中成立的最坏情况下界。

定理 1.7（最坏情况 AC^0 下界，适用于 $\oplus_n$ 在 PV_1中）。对于所有常元 k、$d \geq 1$，都存在一个常元 $n_0 \geq 1$，使得 PV_1 证明以下陈述：对于每个 $n \in \mathsf{Log}$、$n > n_0$ 和 AC^0_d 电路C： $\{0,1\}^n \to \{0,1\}$ 其大小至多为 n^k，都存在一个字符串 $x \in \{0,1\}^n$，使得 $C(x) \neq \oplus_n(x)$。

此前对有界深度电路最坏情况奇偶函数下界的形式化，需要更强的理论。具体而言， [MP20] 和 [Kra95] 在$\mathsf{APC}_1 = \mathsf{PV}_1 + \mathsf{dWPHP(PV)}$ 中形式化了不同的证明，而[Raz95] 则在PV_1 中进行，但处于LogLog 范围——即使用 n双重对数阶的参数——因此证明可以处理指数规模的对象（详情参见 [MP20] ）。

这些形式化进一步印证了这样一种直觉：算法与复杂性理论中的相当一部分结果，已经可以在PV_1 或其温和扩展中得到刻画；因此，证明不可证性结果将具有重大意义（相关讨论见 [Oli25]）。

在下文第1.3 节中，我们将详细阐述定理1.6 和定理1.7的证明。有关这些及其他形式化的更多细节，请参见第4节。

1.2.4 见证、APX_1, 的相对强度及$\mathsf{prBPP} =_{\mathsf{pr}}$的可证明性 P

我们现在讨论理论 PV_1, APX_1，与 APC_1，之间的关系，以及它们与 prBPP 与 prP 问题的联系。我们还引入一个名为 Refuter(Yao) 的新计算问题，并为 APX_1 中 $\forall\Sigma^b_1$(PV) 的推论（即 APX_1 中可证明全定义的 TFNP 问题）提供一个量身定制的见证定理。

APX_1 与 APC_1。根据构造，在 PV_1 中可证的每个句子也是APX_1的一个定理。还可以证明，如果 φ 是 PV_1 语言中的一个句子（即不含近似计数符号 P），且可在 APX_1, 中证明，那么它也可在 APC_1 中证明（参见推论 5.10）。这意味着，除语言上的差异外（即 APC_1 没有符号 P），APX_1 是APC_1的一个子理论。[7]

另一方面，在合理的计算假设下，存在一些可在 APC_1中证明、但无法在 APX_1 中证明的句子（参见推论5.14）。[8] 这是通过改编 [ILW23]中的一种技术得到的。换言之，PV_1 包含于 APX_1, 中，而 APX_1 很可能严格弱于 APC_1。

随后，一个基本的研究方向是确定 APX_1 是否强于 PV_1,；这一问题与 prBPP 与 prP 问题密切相关，也关系到理解随机性在可行证明中的作用。

[7]事实上，存在一个称为 HARD^A [Jeˇr07a] 的 APC_1 保守扩张，它以更强的意义包含 APX_1 ——符号 P 可以由 HARD^A 中的一个项模拟，使得关于 P 的所有公理都可被证明（见定理 5.9）。[8]更正式地说，在存在不可区分混淆且 coNP 不被 NP 无限多次包含的条件下，存在一个 $\forall\Sigma^b_2$(PV) 句子可在 APC_1 中证明，却无法在 APX_1，中证明（见推论 5.14）。

PV_1 与 APX_1 以及可行去随机化。 从元数学的角度来看，一个自然的问题是，prBPP = prP 是否能在诸如 PV_1 这样的弱算术理论中（不）得到证明。一个关键障碍在于形式化：PV_1 的语言专为确定性多项式时间函数设计，而 prBPP =prP 这一命题则涉及对指数规模空间中电路接受概率的量化。我们提出以下问题。

开放问题 1. 是否存在一个 PV 函数符号 $\mathsf{P}(C, \Delta)$，使得基本、边界、精度一致性和局部一致性公理（第1.2.1节）可在 PV_1中证明?

目前看来，要无条件地给出肯定答案并不现实，因为这将立即推出 $\mathsf{prBPP}_{\sim} = \mathsf{prP}$，这是由近似计数公理的可靠性以及 P 的多项式运行时间所致（见定理 2.5）。直观地说，这相当于给出了关于该坍缩的确定性多项式时间证明。目前尚不清楚肯定答案还是否定答案更为可信。

~~P/poly 的自然性质，即假设存在对 PV 函数的~~ 一种较弱的可能性是，即使不存在这样的 PV 函数的近似计数预言机 $\tilde{\mathsf{P}}$ 仍可能对基本语言中的确定性陈述是保守的。形式化地说：

开放问题 2. APX_1 对于 PV_1是保守的吗？等价地说，在 APX_1 中可证明的 PV 语言中的每个一阶句子，是否都已经有一个在 PV_1中的证明?

若开放问题 1 得到肯定答案，则这里也会得到肯定答案。开放问题 2 与 prBPP =prP 之间的关系似乎不可比较。如果 prBPP =prP 成立，但只能通过非可行证明来证明，那么 APX_1 不一定是 PV_1上的保守扩张。反过来，即使 APX_1 是 PV_1，上的保守扩张，我们也不清楚能否推出 prBPP =prP。总的来说，我们关注计算的去随机化与证明的去随机化之间的关系。尽管目前还无法给出明确答案，但我们认为这些问题至关重要，值得进一步研究。关于 APC_1 与 PV_1背景下的相关问题，请参阅 [Kra25]及其参考文献。

APX_1的见证定理：归约到 Refuter(姚期智)。 有界理论的一个关键特征是具备适当的见证定理，对应于某些计算问题（例如，参见[Bus86、KPT91]）。我们将某个（全）搜索问题单独列出，作为一项关键计算任务，用于为 $\forall\Sigma^b_1$(PV)的推论生成见证APX_1。

Refuter(Yao)：一个实例固定以下参数：输入长度 n、多重集大小 m、预测器电路描述大小 s以及优势 $\delta > 0$。输入是一个预测器生成器，也就是一个电路

$$G\colon \{0,1\}^{nm} \to [n] \times \{0,1\}^s$$

它在平坦分布 $\mathcal{D} \in (\{0,1\}^n)^m$（即由 n 位字符串构成的 m 元组）上运行时，会返回一个索引 $i \in [n]$ 和一个预测器电路 P的描述：$\{0,1\}^{i-1} \to \{0,1\}$ 其大小为 s。任何平坦分布 $\mathcal{D}$都是一个解，只要写作 $(i, P) = G(\mathcal{D})$，

$$\Pr_{x \leftarrow \mathcal{D}}\big[P(x_{<i}) = x_i\big] < \tfrac{1}{2} + \delta.$$

因此，解 $\mathcal{D}$ 可以反驳 这一说法：G 能够为任意分布生成具有优势 δ的预测器。当参数满足 $(\delta^2/10) \cdot m \geq s + \lceil$对数 $n\rceil + 1$时，Refuter(姚期智) 属于 TFZPP；换言之，均匀随机分布很可能是一个解。这个问题称为 Refuter(姚期智)，因为 G 旨在输出一个预测器，类似于姚期智提出的标准“区分器→预测器”变换 [姚期智82]。

Remark 1.8（反驳器（姚期智）与去随机化）。注意，反驳器（姚期智）要求生成一个分布 $\mathcal{D}$，该分布相对于一个 *given* 预测器生成器 G 是不可预测的——这是一种确定性过程，试图产生一个预测器 P，用于 $\mathcal{D}$。分布 $\mathcal{D}$ 不必相对于 *all small circuits*是伪随机的（或等价地，不可预测的）；它只需欺骗特定的生成器 G。这可以视为构造 *targeted pseudorandom generators*的一种特例，而该任务已知是prBPP-完全的（参见 [Gol11、CT21、LPT24]）。

我们针对 APX_1 的可证全 TFNP 问题建立如下结果。

定理 1.9 (APX_1的见证。 设 $\varphi(x,y)$ 是PV_1语言中的无量词公式。如果$\mathrm{APX}_1 \vdash \forall x\,\exists y\,\varphi(x,y)$，则存在一个从 φ 所定义的搜索问题到反驳者(姚期智) 的确定性多项式时间图灵归约，其参数满足$(\delta^2/10)\cdot m \geq s + \lceil \text{对数}\, n\rceil + 1$。

在下文第 1.3 节中，我们将概述定理 1.9的证明。

与 LossyCode 和 APC_1的关系。 回顾搜索问题 LossyCode [Kor22]的定义：给定一个压缩器电路 C： $\{0,1\}^n \to \{0,1\}^{n-1}$和一个解压器电路 D： $\{0,1\}^{n-1} \to \{0,1\}^n$，输出 x，使其满足 $D(C(x)) \neq x$。与 反驳者(姚期智) 类似，这个问题是全问题，且属于 TFZPP。

我们注意到，只要 Refuter(Yao) 的输入实例满足……，就存在一个从 Refuter(Yao) 到 LossyCode 的确定性多项式时间映射归约

$$(\delta^2/10)\cdot m \;\geq\; s + \lceil \log n\rceil + 1.$$

因此，在上述条件下，对 LossyCode 去随机化涵盖了对 Refuter(Yao) 去随机化。由于每个可由 APX_1 证明为全的 TFNP 问题都归约到 Refuter(Yao)，在上述参数条件下，它还可进一步归约到 LossyCode。

回顾一下，Wilkie（未发表）和 Thapen [Tha02] （参见 [Je˘r04，命题 1。14] 和 [LPT24，定理 D。1]）证明了 LossyCode刻画了 $\forall\Sigma^b_1$-片段的APC_1。因此，这些结果梳理了两种理论的TFNP图景： LossyCode 见证了 $\forall\Sigma^b_1$-后果，而这些后果来自 APC_1, ； 而 Refuter（姚期智）则见证了APX_1的后果。

我们将在第5节回到这些主题，详细证明上述所有结果，并作进一步讨论。

1.2.5 随机化与平均情况下界的逆向数学

收缩弱鸽巢原理（rWPHP(PV)） [Je˘r07b, LLR24, CLO24] 是已知可在 APC_1, 中证明、但在 APX_1 中的可证明性仍不明确的最重要组合原理之一。回想一下，rWPHP(PV)断言：对于任意 n、$m \in \mathrm{Log}$，若满足 $m < n$ ，且对于所有（确定性）电路 C: $\{0,1\}^n \to \{0,1\}^m$ （“压缩器”）和 D: $\{0,1\}^m \to \{0,1\}^n$ （“解压器”），存在 $x \in \{0,1\}^n$ 使得 $D(C(x)) \neq x$。

换句话说，rWPHP(PV)体现了上述全搜索问题LossyCode 背后的组合原理。若能在APX_1 中证明它，APX_1 和APC_1 将证明相同的 $\forall\Sigma^b_1$(PV)句子；根据见证定理（见定理1.9），这还将意味着LossyCode 与 Refuter(姚期智)在确定性多项式时间图灵归约意义下等价。

我们研究收缩弱鸽巢原理的计数变体，并刻画它们关于 APX_1 中可证明性的等价类。我们证明，该等价类涵盖了针对随机化协议的通信复杂度下界中的某些结果，并由此确立，这些结果在基础理论 APX_1 上都等价于收缩鸽巢原理的相应变体。

rWPHP(PV) 的计数变体。我们考虑以下命题：

- 近似计数缩回弱鸽巢原理：#rWPHP$[m,\varepsilon]$。对于任意确定性压缩器—解压器对，若编码长度为 $m < n$，则有 ε比例的输入无法被正确解压。

- 随机化压缩缩回弱鸽巢原理：rrWPHP$[m,\varepsilon]$。对于一个随机化压缩器和一个确定性解压器，若编码长度为 $m < n$，则存在某个输入，使得该压缩器—解压器对的错误概率至少为 ε。

这些原则以自然的方式，利用 APX_1 所提供的概率框架加以形式化。

单向通信复杂度。 我们证明了一个等价结果，它涉及针对随机化单向协议 的通信复杂度（CC）下界，这些协议使用公共随机性 或 私有随机性。回顾一下，集合不相交函数 SetDisj(x, y) 输出 1，当且仅当对每一个索引$i \in [n]$，要么 $x_i = 0$ 要么 $y_i = 0$，亦即 x 与 y 没有共同的 1-索引。以下陈述为清晰起见以非正式方式给出，与我们的结果相关：

- 集合不相交问题的公共随机化通信复杂度下界：pub-rLB$\longrightarrow_{\text{SetDisj}}[m, \varepsilon]$。每个使用公共随机性的单向协议，若其计算 SetDisj 的通信复杂度为 m，则在某个输入对（x，y）上的错误概率至少为 ε。

- 集合不相交问题的私有随机化通信复杂度下界：priv-rLB$\longrightarrow_{\text{SetDisj}}[m, \varepsilon]$。每个使用私有随机性的单向协议，若其计算 SetDisj 的通信复杂度为 m，则在某个输入对（x，y）上的错误概率至少为 ε。

- 某个函数的公共随机化通信复杂度下界：pub-rLB$\longrightarrow_{\text{some}}[m, \varepsilon]$。对于每个 $n \in \text{Log}$，都存在 $f\colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$，使得 pub-rLB$\underset{\longrightarrow}{}^{f}[m, \varepsilon]$ 成立。
- 某个函数的私有随机化通信复杂度下界：priv-rLB$\longrightarrow_{\text{some}}[m, \varepsilon]$。对于每个 $n \in \text{Log}$，都存在 $f\colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$，使得 priv-rLB$\underset{\longrightarrow}{}^{f}[m, \varepsilon]$ 成立。

关于相应下界句子的形式化细节，我们留待第6节讨论。我们注意到，APX_1 能够证明某些具体函数存在低成本通信协议。例如，利用线性哈希，它证明等值检验存在成本为 $O(\log n)$ 的公开随机性单向通信协议。

我们可以将主要等价性结果的非正式版本表述如下。[9]

定理1.10 （主要等价性结果（非正式版）；见定理6.7）。以下命题在APX_1，中等价，其中常元 $k \geq 1$ 和 $0 < \varepsilon < 1$之间满足适当的关系，且量词置于理论之外：

(1) #收缩弱鸽巢原理$[n-1, n^{-k}]$

(2) #收缩弱鸽巢原理$[n^{\varepsilon}, n^{-k}]$

(3) rrWPHP$[n-1, n^{-k}]$

(4) rrWPHP$[n^{\varepsilon}, n^{-k}]$

(5) 公开-rLB$\underset{\longrightarrow}{}^{\text{SetDisj}}[n-1, n^{-k}]$

(6) pub-rLB$\underset{\longrightarrow}{}^{\text{SetDisj}}[n^{\varepsilon}, n^{-k}]$

(7) priv-rLB$\underset{\longrightarrow}{}^{\text{SetDisj}}[n-1, n^{-k}]$

(8) 私有-rLB$\underset{\longrightarrow}{}^{\text{SetDisj}}[n^{\varepsilon}, n^{-k}]$

(9) 公开-rLB$\underset{\longrightarrow}{}^{\text{some}}[n-1, n^{-k}]$

(10) 公共-rLB$\underset{\longrightarrow}{}^{\text{some}}[n^{\varepsilon}, n^{-k}]$

私有-rLB$\underset{\longrightarrow}{}^{\text{some}}[n-1, n^{-k}]$

私有-rLB$\underset{\longrightarrow}{}^{\text{一些}}[n^{\varepsilon}, n^{-k}]$

因此，这些陈述中有一个可在 APX_1 中证明，当且仅当定理 1.10中的每个陈述都可在 APX_1中证明。这一结果表明，APX_1 可以作为合适的基础理论，用于发展平均情况和随机化下界的逆向数学。

有关更多详情和补充讨论，请参阅第 6 节。

1.3 技术

接下来，我们概述证明中使用的一些主要技术，首先介绍一个反复使用的论证，它在 APX_1 中建立基本的概率不等式。

[9]特别是，此处给出的简化表述未考虑随机化协议所使用的随机比特数量，而该数量会影响某些陈述中的参数。

1.3.1 概率论者 在 APX_1中的推理：“从逐点到整体”技巧（第1.2.2)

我们概率推理的核心是一个简单而强大的种子固定引理，它使我们能够从全局不等式转向关于随机性的适当选定限制的逐点陈述。回顾一下，一个可行随机变量 X 由显式支撑集 $V \subseteq \mathbb{Q}$、种子长度 n和多输出电路 C指定： $\{0,1\}^n \to V$。其近似期望为

$$\mathbb{E}_\delta[X] \triangleq \sum_{v \in V} v \cdot \mathsf{P}_\delta(C_v),$$

其中， C_v 是事件 $C(x) = v$的指示电路。这是一个可由 PV(P) 计算的量。

期望的平均论证（定理 3.17）。以下结论在APX_1中成立。设X_1，……， X_m 是在相同种子上定义的、支撑集为 V的随机变量，并固定系数 λ_1，……， $\lambda_m \in \mathbb{Q}$。记作

$$\mu \triangleq \sum_{i=1}^{m} \lambda_i \, \mathbb{E}_\delta[X_i], \qquad \mu \restriction z \triangleq \sum_{i=1}^{m} \lambda_i \, \mathbb{E}_\delta[X_i \mid z],$$

其中， $X_i \mid z$ 表示将种子的后缀固定为 z 后的 X_i 。于是，对于任意期望的后缀长度 k，存在 $z \in \{0,1\}^k$ 使得

$$\mu \restriction z \;\geq\; \mu \;-\; (2\delta + \beta) \cdot \|\lambda\|_1 \cdot \|V\|_1. \tag{3.7}$$

因此，通过对种子进行部分赋值并据此条件化，可以见证 μ 的下界（允许受控的加性松弛）。

证明通过每次固定一个种子位来迭代进行。根据期望的某种局部一致性， $\mu\restriction(0\circ z)$与 $\mu\restriction(1\circ z)$的平均值接近 $\mu\restriction z$；因此，可以证明这两种扩展中至少有一种能使当前值保持在加性损失 $O(\eta\cdot\|\lambda\|_1\cdot\|V\|_1)$以内，其中 η是证明中的一个辅助参数。贪心地重复此过程 k步，即可得到一个 k位后缀，总损失为 $O(k\cdot\eta\cdot\|\lambda\|_1\|V\|_1)$。接着，通过精度平滑论证（借助精度一致性从 η 切换到 δ ），可得所述的、与 k无关的$(2\delta+\beta)$型界。贪心构造由一个 PV(P) 过程 AvgSampler 形式化地刻画。从概念上说，AvgSampler 通过调用近似计数预言机 P 来搜索良好的后缀；其正确性则通过对 k 进行关于无量词 PV(P) 公式的（多项式）归纳法来证明，这种归纳法在 APX_1 中是可用的。

> *Remark* 1.11（示例：补运算的一致性（推论 3.18）。）。设 E_1， E_2： $\{0,1\}^n \to \{0,1\}$ 是互补谓词，即 $E_1 = \neg E_2$ 是布尔电路。设 X_1， X_2 是它们的指示变量。我们在 APX_1中进行论证。给定任意的 $\beta^{-1} \in \mathsf{Log}$，我们令 $\eta \triangleq \beta/C$，其中常元足够大 C。逐点来看，对于*every full assignment* ρ 种子，利用 E_1 与 E_2 之间的关系，我们有
>
> $$\mathbb{E}_\eta[X_1 \mid \rho] + \mathbb{E}_\eta[X_2 \mid \rho] - 1 \;=\; 0.$$
>
> 令 $\lambda \triangleq (1,\ 1,\ -1)$，并考虑 $\mu \triangleq \mathbb{E}_\eta[X_1]+\mathbb{E}_\eta[X_2]-1$。应用定理 3.17并取 $k=n$，可得到一个 ρ使得 $\mu \leq \mu\restriction\rho + O(\eta)$。但根据上面的逐点恒等式， $\mu\restriction\rho$恰好为 0，因此得到 $\mathbb{E}_\eta[X_1]+\mathbb{E}_\eta[X_2]-1 = O(\eta)$。类似地，可以证明 $-\mathbb{E}_\eta[X_1] - \mathbb{E}_\eta[X_2] + 1 = O(\eta)$。通过指示函数对应将期望转换回概率，并应用标准的精度平滑论证，可以得出 P_δ 满足补运算的一致性，即
>
> $$\left|\mathsf{P}_\delta(E_1) + \mathsf{P}_\delta(E_2) - 1\right| \;\leq\; 2\delta + \beta.$$

总而言之，定理 3.17 提供了一种固定随机性、同时保留期望线性组合下界的方法。它将对每个种子都成立的等式或不等式，转化为 APX_1 中的定量全局界，其加性松弛是显式的，且仅取决于 δ、 β 以及支撑集和系数的自然 ℓ_1 范数。这一机制是推动我们许多概率不等式及第3节应用的核心引擎。

Remark 1.12. 逐位固定技巧是计算复杂性理论中的一种标准技术。例如，它用于 SAT [AB09第2节中的搜索到判定归约5]，也用于从去随机化推导电路下界 [AvM11], 等其他结果。特别是，我们的方法受到一项通过逐位"对决论证"证明 BPP $\subseteq$ 梅林—阿瑟类 $\subseteq \Sigma_2^p$ 的新证明的启发 [LPT24，引理 A10]。

1.3.2 电路下界的可证明性（定理 1.6 和1.7）

定理 1.6 给出了平均情况下奇偶函数相对于深度为 d AC^0 电路的下界，并在 APX_1，中将其形式化；而定理 1.7 给出了相应的最坏情况下界，并在较弱的理论 PV_1 中将其形式化。如上所述，难点在于避免依赖鸽巢原理（或基于鸽巢原理构建的框架）的基于编码的论证，因为这些理论中无法使用它们。第一个结果展示了 APX_1 近似概率演算如何在更复杂的情形下支持平均情况论证；第二个结果则表明，经过额外的去随机化工作，我们可以完全在 PV_1 中完成相应的最坏情况下界论证。

从整体上看，这些形式化实现了对 Furst–Saxe–Sipser [AAI+01] 随机限制方法的简化与去随机化 [FSS84], 用于证明 AC^0 电路下界。回顾一下，该论证分阶段进行，每个阶段都会固定一个合适的部分限制 ρ: $[n] \to \{0,1,*\}$ 它将 $T \triangleq \rho^{-1}(\{0,1\}) \subseteq [n]$中的所有输入变量设定好。关键在于，深度为 d 的电路 C 在受到限制时会简化 ρ，从而得到一个深度为 $C \restriction \rho$ 、规模不会大很多的电路 $d-1$；与此同时，奇偶函数仍然保持其困难性。

两个核心引理　用于规范的 ρ 推动了定理1.6 和定理1.7的证明 .

子集选择引理（引理4.8）。第一步是算法化地选择集合 $T \subseteq [n]$中的变量，并保证"窄或宽"性质：对于电路底层的每个有界宽度合取范式/析取范式 F，在固定变量 C中的变量之后， T要么已经只依赖少量文字（窄），要么包含许多由 T 支撑的互不相交子句（宽）。关键在于，这一子集选择是在PV_1 中构造出来并证明正确的，所采用的是一种精巧的势函数论证，用来模拟通过条件期望进行去随机化的方法。这使得子集的选择 $T \subseteq [n]$ 在我们的理论中是可行的，而不仅仅是存在性的。

限制选择引理（引理4.9 和4.10）。基于子集选择步骤所揭示的窄或宽结构，接下来我们为 T 中的变量选择取值，使得电路C 中的所有相关门在应用所得限制 ρ后同时得到简化。这里有两个版本，分别对应我们的两个定理：

- 在定理$_1$ 1.6的 APX*1* 设定中，我们考虑一个随机比特赋值 （引理4.9），然后通过上文介绍的 APX*1*的"从逐点到整体"的期望的平均论证，固定一组良好的值选择。这使我们能够构造一个部分限制 ρ，并得到相应的电路 $C \restriction \rho$，使其在计算奇偶性时大致保留 C 的相对优势。

- 在定理$_1$ 1.7限制更多的 PV*1* 设定中，我们对同一选择进行去随机化 （引理4.10）。同样，这通过势函数论证实现，该论证在 PV1中可行地模拟条件期望法。证明中有一个关键方面有助于形式化：相关期望最多依赖于 O 个（$\log n$）输入坐标，因此可由 PV_1 项高效计算。

在这两种设定中，电路下界通过归纳应用限制技术得到，正如该结果的标准证明一样。详细内容见第 4.4节。

新颖之处并不在于AC^0 与奇偶性之间的组合学，而在于其底层的证明论框架。APX_1 提供了精简但充分的概率基础设施，使我们能够在内部完成平均情形下界论证。在我们的证明中，这使我们能够定义并推理一致性测试器T_C （定理1.6的陈述中所述），定义并分析适当的事件，量化优势，并将其从随机限制推广到具体选择，

并跟踪迭代过程中累积的小幅加性损失——这一切都在 APX_1 内完成。

此外，这一精简的设定及其所提供的视角澄清了与较弱理论 PV_1 的边界。APX_1 框架与我们的形式化恰好隔离出何处使用了概率推理，以及何处论证纯粹是组合性的。这种分离表明哪些组成部分可以由 PV_1，中可用的基于确定性势函数的论证替换，从而指导产生我们在 PV_1 中的最坏情形形式化的改编。

1.3.3 见证定理（定理 1.9）

定理 1.9 指出，每一个在 APX_1 中可证的 $\forall\Sigma^b_1$(PV)-句子都容许到全搜索问题 Refuter(Yao) 的确定性多项式时间图灵归约，其参数满足 $(\delta^2/10)\cdot m \geq s+\lceil\log n\rceil+1$。回想一下，Refuter(Yao) 的一个实例给出一个预测器生成器 G，并要求一个平坦分布 $\mathcal{D}$，使得预测器 $(i,P)=G(\mathcal{D})$ 无法以优势 δ 预测 $\mathcal{D}$ 的第 i 位。（对于所述参数范围，Refuter(Yao) 属于 TFZPP，并可映射归约到 LossyCode。）

假设 $\mathrm{APX}_1\vdash\forall x\,\exists y\,\varphi(x,\ y)$，其中 φ 是一个无量词 PV 公式。给定长度为 n的 x，我们描述一个预测器生成器 G_x，使得在 G_x 上对 Refuter(Yao) 的一个解 $\mathcal{D}$ 允许我们计算出 y，从而 $\varphi(x,\ y)$成立。

从一个关于 $\forall x\,\exists y\,\varphi(x,y)$ 的 APX_1-证明开始，我们首先在 APX_1 的全称公理化下应用赫布兰德定理，得到有限多个 PV(P) 项 t_1、……、t_c，使得 $\bigvee_i\varphi(x,t_i(x))$成立；然后用单个项 t_φ 编码这个析取式，使等式核心 APX 能够证明 $t_\varphi(x,t_1(x)\ldots\ldots,\ t_c(x))=1$。在标准模型（第 1.2.1 节）中，这些项是针对近似计数预言机 P 的多项式时间预言机算法。

接下来，我们描述 G_x 的构造。给定一个候选平坦分布 $\mathcal{D}$（例如，定义在 n' 位字符串上，支撑集大小为 m'，其中 n'，$m'=\mathrm{poly}(n)$ 足够大），我们通过在 $\mathcal{D}$ 上进行模拟和经验计数，来处理其中任意一次对预言机 $\mathsf{P}(C,\ \Delta)$ 的调用：

$$\mathsf{P}(C,\Delta)\triangleq\Pr_{u\leftarrow\mathcal{D}}\big[C(u_{\leq\ell})\big],$$

其中 $C\colon\{0,1\}^\ell\to\{0,1\}$ 且 $\ell\leq n'$。令 $t_i^{\mathcal{D}}(x)$ 和 $t_\varphi^{\mathcal{D}}(x,\ \cdot)$ 表示由此得到的输出。注意，这些输出可以在确定性多项式时间内计算，因为 $\mathcal{D}$ 被明确给出为一个集合，其中包含 $\mathrm{poly}(n)$ 个长度为 $\mathrm{poly}(n)$ 的字符串，并且 t_φ、t_1…… t_c 均可在多项式时间内运行。

预测器提取引理（引理5.6）。关键的技术步骤指出：如果在此模拟下，APX-可证方程不成立，即 $t_\varphi^{\mathcal{D}}(x,\ \cdot)\neq 1$，那么我们就能通过算法提取出一个小型预测器 P，其大小为 s'，并且对于 $\mathcal{D}$ 中一个显式计算出的比特位置，能获得至少为 δ' 的优势，其中 $(\delta'^2/10)\cdot m'\geq s'+\lceil\log n'\rceil+1$。

从概念上讲，APX 证明断言：对于每一种 P 的解释，方程要么成立，要么某条近似计数公理（基本、边界、精度一致性、局部一致性）被违反。在我们的经验解释下，前三条公理仍然成立，因此任何失败都必须体现为局部一致性 违反，形式如下

$$\Big|\Pr_{u\leftarrow\mathcal{D}}[C(u_{\leq\ell})]-\tfrac{1}{2}\Big(\Pr_{u\leftarrow\mathcal{D}}[C(u_{<\ell}0)]+\Pr_{u\leftarrow\mathcal{D}}[C(u_{<\ell}1)]\Big)\Big|\ >\ \tfrac{2}{|\Delta|}+\tfrac{1}{|B|},$$

对于 APX 证明中产生的一个电路 C 和字符串 Δ、B。

与姚期智的区分器到预测器引理的分析类似，这种差距通过对 C 进行确定性变换，可以得到一个预测器来预测下一位；这里的“信号”并非来自区分 $\mathcal{D}$ 与均匀分布，而是来自检测不同位固定条件下经验计数的局部不一致性。因此，预测器不仅可以由区分器导出，也可以源于这样一种能力：当 $\mathcal{D}$ 被用作近似计数的随机源时，能够发现局部不一致性——这一观点或许本身也值得关注。[10]

[10]特别是，姚期智的区分器到预测器变换需要 *randomness*（除非我们有 $\mathsf{prBPP}=\mathsf{prP}$）[LPT24]。然而，从局部不一致性构造预测器是确定性的。

形式上，该引理通过证明论分析得以确立：对 APX 证明的各个步骤进行归纳，并跟踪最终所用规则中的参数（n', m', s', δ'）。

总结这一论证，对于输入 x，归约输出预测器生成器 G_x，它由引理5.6得到。注意，对于由此产生的 $\mathcal{D}$，任何解都反驳者(姚期智) 实例都无法触发成功的预测器提取，因为根据定义，G_x 无法在 $\mathcal{D}$上生成预测器。因此，给定该 $\mathcal{D}$ 反驳者实例(姚期智) 的一个解，它必定使模拟恒等式成立，即：

$$t_\varphi(x, t_1^{\mathcal{D}}(x), \ldots, t_c^{\mathcal{D}}(x)) = 1.$$

换言之，某个 $t_i^{\mathcal{D}}(x)$ 是 $\varphi(x,\ y)$ 的有效见证 y。最后，如上所述，由于 $\mathcal{D}$ 是显式的，所有模拟调用和 $t_i^{\mathcal{D}}(x)$ 都可以在确定性多项式时间内计算。

T至此，定理1.9证明的概要就完成了。详细内容请参见第 5 节。

1.4 相关工作

下面列出一些具有代表性的相关进展和参考文献，但并未穷尽所有内容。

有界算术中的概率论证。 Paris、Wilkie 和 Woods [PWW88](另见 Pudl´ak[Pud90]) 指出，许多概率论证可以通过弱鸽巢原理的变体形式化，而不必使用精确计数。Wilkie（参见 [Kra95]）较早明确指出了弱鸽巢原理与随机算法之间的联系，他证明随机多项式时间算法见证了所有 $\forall\Sigma_1^b$-后果（consequences） $\mathsf{S}_2^1 +$ dWPHP(PV)。

Ojakian [Oja04] 对组合学中的概率方法如何在有界算术中实现形式化进行了系统研究。尽管这类证明通常可以改写为纯粹基于计数的论证，但朴素的转换仍会留下指数多的对象需要计数。核心思想仍然是利用弱鸽巢原理来模拟概率计数论证，从而避免这种膨胀。形式化工作是在S_2^1 中进行的，并加入了适当的鸽巢原理变体。

Je˘r´abek [Je˘r04] 证明，在 PV_1 中，可以通过构造从一个集合到另一个集合的满射，比较两个有界 P/poly 可定义集合的大小；他用这一方法形式化了 ZPP 和 RP 中算法的描述。他进一步证明 [Je˘r04, Je˘r05]，$\mathsf{APC}_1 = \mathsf{PV}_1 +$dWPHP(PV) 足以形式化复杂的去随机化结果。在 [Je˘r07a], Je˘r´abek 提出了一个更系统的框架，特别证明了对于任何有界 P/poly 可定义集合，APC_1 都能证明存在一对适当的满射计数函数，其近似该集合的基数，误差至多为多项式级小误差。（记号 APC_1 遵循 [BKT14]的术语。）

建立在 Je˘r´abek 的框架之上，L^e [L^e14] 形式化了 APC_1 及其扩展中的更多结果，包括随机匹配算法、Lov´asz 局部引理和 Goldreich-Levin定理。在这些形式化过程中，L^e 提供了 APC_1 中概念的表述，例如 期望、马尔可夫不等式和两两独立性，这些也是我们在本项目中研究的内容。随机变量和期望在 [L^e14] 中的形式化严重依赖于 APC_1 的工具，因此不适合我们的用途。

> *Remark* 1.13。 一个具体的开放问题是在 APX_1中陈述并证明更强形式的切尔诺夫界。在这项工作中，我们证明，带有 $O(\log n)$ 个变量（即长度为 n 的字符串被视为可行）的切尔诺夫界可以在 APX_1中形式化。我们尚不清楚能否对带有 $O(n)$ 个变量的情形陈述出简洁且有意义的切尔诺夫界：其错误概率将呈指数级缩小，这可能远小于函数 P 的近似计数误差。此外，即使存在有意义的形式化，我们也不清楚现有的切尔诺夫界证明能否在 APX_1 中形式化。注意，带有 $O(n)$ 个变量的强形式切尔诺夫界可以在 Je˘r´abek 的理论 APC_1 中形式化（见 [Je˘r07a，命题 2。18]）

dWPHP(PV)的证明复杂性。已有证据表明，这些框架中贯穿始终所用的基于鸽巢原理的公理，超出了纯多项式时间理论所能证明的范围：虽然dWPHP(PV可在T_2^2, 相对化变体在S_2^2 [Rii93]中就已不可证明。如上所述，在密码学假设下，PV_1 不能证明dWPHP(PV) [ILW23]。这支撑了一种普遍看法，即PV_1

过于弱小，无法导出上述形式化中所利用的WPHP型原则。关于dWPHP(PV)及其在有界算术中的可证明性的全面研究，参见 [Kra25]。

Je$\check{\text{r}}$´abek 的近似计数工具箱包含容斥原理和强 Chernoff 型估计等一般原理，并且都已在 APC_1 中形式化。相比之下，APX_1 的发展有意从较弱的原语出发：虽然我们恢复了 Markov/Chebyshev 风格的推理、误差缩减以及其他基本概率工具，但此处并未重新证明 Je$\check{\text{r}}$´abek 最强的所有集中界。探索 APX_1 的能力极限仍是一个有趣的方向：哪些更强的概率不等式（例如完整形式的 Chernoff 不等式）在本质上超出了其公理?

超越带加性误差的近似计数。某些组合证明——例如 Ramsey 定理的证明——通常需要对稀疏集合计数，而这在我们的框架和 Je$\check{\text{r}}$´abek 的理论 APC_1中都无法实现。在我们的设定中，对于 $X \subseteq \{0,1\}^n$ 我们只能将其估计到一个加性误差范围内，该误差是 $|X|$ 的多项式比例，而这些论证要求精度达到 2^n的多项式比例以内。比 $|X|$APC更强的理论可以实现这类计数，正如$_1$, 中所发展的 [Je$\check{\text{r}}$09]所示。

在一项同期研究中，Thapen [Tha24]提出了一个框架，用于定义更强的复杂性类（例如 $\oplus$P 和 #P），该框架建立在 TFNP理论之上，其思路与我们对近似计数的公理化类似。例如，给定一个旨在计算 $\oplus$P 的预言机，Thapen 考虑了相对化的 TFNP 问题，即寻找该预言机的“局部不一致性”。需要注意的是，TFNP框架在 [Tha24]中只考虑 查询复杂度，而我们还考虑有界算术中的证明。尽管如此，鉴于两种框架的设定相似，这两个方向上的结果或许都能在各自的框架中找到对应形式。

具有显式计数的理论。 在 [Je$\check{\text{r}}$05的第 6], Je$\check{\text{r}}$´章中，abek 研究了具有显式计数的有界理论，并重新探讨了 Impagliazzo-Kapron [IK06] 用于形式化密码学推理的二阶逻辑。该逻辑采用多类型体系：一阶变量的取值范围是字符串，而类型$k > 0$ 的二阶变量取值范围是 k元（意指多项式时间）函数。具体而言，函数是二阶对象，而非语言中的函数符号。该理论包含递归计数构造，用于表示可定义有界集合的大小。

同一章还介绍了一种可行的近似计数理论，它采用基于 Kleene 逻辑的三值语义，并配备 LPF 风格蕴涵以支撑类归纳推理。计数是近似的：该语义区分解很多与解很少的情况（同时借助三值逻辑明确划定一个不确定区域）。由此得到的“Σ^b_1推论”允许进行概率多项式时间见证（见 [Je$\check{\text{r}}$05，定理 6.2。20]）。

这些理论中的计数框架与我们的框架大不相同，它们依赖于不同逻辑语境中的精确计数项或近似计数量词。详情请参阅这些文献。

有界逆向数学。 Cook 和 Nguyen [CN10] 全面阐述了有界逆向数学计划，系统地发展了有界算术理论，并介绍了关键组合结果和算法结果的形式化，旨在确定足以证明这些结果的最弱公理。

最后，关于理论计算机科学中可在有界算术中形式化的诸多结果示例，请参阅 [L$\hat{\text{e}}$14、Pic14、MP20、AT25] 及其中的参考文献。进一步研究这些形式化中哪些可以在 APX_1 中完成，将会很有意思。

致谢。 我们感谢 Jan Kraj$\acute{\text{ı}}\check{\text{c}}$ek 与我们讨论 APC_1 对 PV_1 的 $\forall\Sigma^b_1$保守性问题，并向我们介绍了一些参考文献。我们也感谢 Dimitrios Tsintsilidas 对论文早期版本提出的意见。我们还要感谢 Surya Mathialagan、Shuo Pang 和 Hanlin Ren 所进行的有益讨论。最后，感谢匿名的 STOC 评审对论文呈现方式提出的宝贵意见。

2 理论的形式化定义

本节将正式定义等式理论 APX 及其一阶对应理论 APX_1。我们假设读者对 Cook 的理论PV [Coo75]有基本了解。必要的背景知识可参见 [Kra95，第 12], [Kra19，第 12], 以及 [Li25]。

2.1 记号

基础理论 论。 令 PV(P) 表示相对于一个新的函数符号 P、并带有以下公理的理论 PV

$$\mathsf{ITR}(\mathsf{P}(C,\Delta), C\#\Delta\#\Delta) = \varepsilon$$

该公理对函数符号 P 的输出长度作出界定。直观地说，该公理表示：当字符串 C和 Δ作为输入时，函数 $\mathsf{P}(C,\Delta)$ 的输出长度至多为 $|C|\cdot|\Delta|^2$。该公理确保在标准模型中，PV(P)-项是可行函数。感兴趣的读者可参阅 [Je˘r04、Je˘r07a、Je˘r07b]，了解更多关于相对化 PV 的例子。

与 Cook 的原始记号略有不同，我们将把 PV(P) 定义为带有常量符号 ε （而不是 0）的理论，并分别用 $s_1(x)$ 和 $s_0(x)$ 替换初始函数 $s_1(x)$ 和 $s_2(x)$。其他函数 TR、$\hat{}$ ITR、 $\circ$ 和 # 的定义与 Cook 的原始定义相同。令 P 为定义在布尔字符串上的函数。相对于 P 的 PV(P) 的标准模型，记为 $\mathbb{M}$(P)，定义如下：

- 论域由所有有限长度的布尔字符串组成。
- 常量符号 ε 解释为空字符串。
- $s_b(x)$（对于 $b\in\{0,1\}$）解释为将 b 附加到字符串 x右侧的函数。
- TR(x)解释为删除 x的最右位的函数；ITR(x,y)解释为将 x删除 $|y|$ 次的函数。
- $\circ$ 解释为字符串连接，而 #(x,y)解释为将 x连接 $|y|$份的函数。$\hat{}$
- 函数符号 P 解释为 P。

由 PV 中某条规则引入的函数（即通过项引入，或通过记号上的有界递归引入）被解释为论域上满足其引入规则的唯一函数。

电路。 我们定义几个用于操作布尔电路的 PV 函数。令 IsCkt(C,z) 为 PV 函数：当 C 是一个输入长度为 $|z|$ 的电路时输出 1，否则输出 0；令 IsConst(C) 为 PV 函数：当 C 是一个不读取其输入的电路（即从输出门到输入变量之间不存在路径）时输出 1；Bool(C) 在 IsConst(C) 且 C 输出 1 时输出 1，在 IsConst(C) 且 C 输出 0 时输出 0 （否则，例如输出 ε）；$\mathsf{Fix}_b(C)$ 是一个函数，给定电路 C，输出将最右侧输入位固定为 $b\in\{0,1\}$ 后从 C 得到的电路；Eval(C,x) 是一个函数，用于计算电路 C 在输入 x 上的值。由于 PV 是一种健壮理论，可以将这些函数在 PV 中的任何直接实现视为 PV 函数。

为简单起见，我们使用以下缩写：

- 对于 $n\in\mathsf{Log}$，$C\in B_n$ 表示 IsCkt(C，1^n)，即，C是一个具有 n 个输入位的电路。此外，$\forall C\in B_n\,\varphi(C)$ 表示 $\forall C(\mathsf{IsCkt}(C,\ 1^n)\to\varphi(C))$，而 $\exists C\in B_n\,\varphi(C)$ 表示 $\exists C(\mathsf{IsCkt}(C,\ 1^n)\wedge\varphi(C))$。
- 对于电路 C，$C(x)$ 表示 Eval(C，x)。
- 我们用 Null_n 表示这样一个电路：它有 n 个输入位，不读取其输入位，并输出 0；用 True_n 表示这样一个电路：它有 n个输入位，不读取其输入位，并输出 1。

PV项与函数。如果某个 PV(P) 项的构造表明它没有调用 P-预言机，我们就称它为 PV 项。形式上，PV 项的集合是包含所有基本函数并且对 PV 中的复合和函数构造规则封闭的最小集合，也就是说：

- 基本函数 $s_i(x)$、TR(x)、ITR(x)、 $\circ(x,\ y)$ 都是 PV 项。
- 如果 t 是一个 PV项，那么由定义公理 $f_t = t$ 引入的函数 f_t 也是一个 PV 项。
- 由 PV项通过复合构造出的项是一个 PV 项。
- 如果 $g,\ h_0,\ h_1,\ k_0,\ k_1$ 是 PV项，那么由 $\Pi = (g,\ h_0,\ h_1,\ k_0,\ k_1)$ 通过记号上的有界递归构造出的函数 f_Π 是一个 PV 项。

我们称函数符号 f 为 PV函数，如果它是一个 PV项。

根据 Cook-Levin定理（形式化见 [Pic15b] ），在 PV中，PV 项可以针对任意给定的输入长度转换为多项式规模布尔电路 $n \in$Log，且其正确性可在PV中证明。同样，PV(P) 项可以针对任意给定的输入长度转换为多项式规模 P-预言机电路$n \in$Log ，并且正确性可由 PV(P) 证明。

编码约定与算术运算。 对于函数和多输出电路，在定义电路的接受概率时，我们将 ε 视为假，其他任何值都视为真。令 Bool(x) 为 PV 函数：当 x 是 ε 时输出 0，否则输出 1。

我们假设自然数以一种直接明了的方式用二进制编码。例如，可以像下面这样用二进表示法编码一个自然数： [Coo75] ，从而可以自然地定义加法、乘法和比较等基本算术运算。我们假设可以高效地验证编码，即存在一个 PV 函数符号IsNumber(x)，当 x 是一个自然数的编码时输出 1，否则输出 0，并用 $[x \in \mathbb{N}]$ 作为 IsNumber(x) 的简写。我们用 $[x]_{\mathbb{N}}$表示由 x 编码的自然数，以便明确说明将 x 解释为自然数。

可以自然地定义加法、乘法和比较等初等算术运算。此外，可以在 PV 中确立表示这些运算的 PV 函数符号的基本性质（只要运算涉及的元素数量是可行的）。

我们在 PV 中规定有理数的一种标准编码：用数对 $(x,\ y)$ 表示有理数

$$\sum_{i=1}^{|x|} x_i 2^{i-1} + \sum_{j=1}^{|y|} y_j 2^{-j}.$$

与自然数的编码类似，我们假设存在一个 PV 函数符号 IsRational(x)，用于测试 x 是否编码了一个有理数，并用 $[x \in \mathbb{Q}]$ 作为 IsRational(x) 的简写。我们用 $[x]_{\mathbb{Q}}$ 表示由 x 编码的有理数。如果上下文明确，我们也可以直接将 x 视为有理数。

数据结构与显式集合。 我们假设采用一种简单直接的编码来表示显式集合（和多重集合），即大小可行的集合，并支持选择、并、交集和成员查询等操作。一个显式集合 S 可以编码为一个包含其所有元素的列表。请注意，这不同于可行定义的集合 [Je˘r04], ，后者的大小可能不可行。讨论显式集合时，我们用 $|S|$ 表示 S 的大小，也就是 S中所含的元素个数。当 $S = \{q_1, \ldots, q_\ell\}$ 是一个有理数集时，我们用 $||S|| = \sum_{i=1}^{\ell} |q_i|$ 表示其 ℓ_1范数，即 S中各元素绝对值之和。[11]

此外，对于显式集合 S 和 PV_1，语言中的无量词公式 $\varphi(x)$，我们可以定义对 S 的全称量化，记作 $\forall x \in S : \varphi(x)$，将其作为 PV_1 中的 无量词公式；当且仅当每个元素 $x \in S$ 都满足 $\varphi(x)$（在标准模型中）时，该公式为真。这是可行的，因为 S 是显式编码的，因此存在一个简单的可行算法，给定 S 的编码后枚举 S ，并检查是否存在某个 $x \in S$ 使得 $\varphi(x)$ 为假。同样，我们可以定义对 S 的存在量化，记作 $\exists x \in S :\ \varphi(x)$。关于集合量化的所有相关推理规则

[11]虽然我们滥用记号 法并使用 $|\cdot|$ 表示长度和绝对值，但在每种语境中，其含义都很清楚 t.

在假设采用标准编码的情况下，应当能在 PV 中导出，例如：

$$(\exists_i): \quad \frac{\Gamma \vdash \varphi[y/t] \quad \Gamma \vdash t \in S}{\Gamma \vdash \exists y \in S : \varphi} \tag{2.1}$$

$$(\exists_e): \quad \frac{\Gamma \vdash \exists y \in S : \varphi \quad \Gamma, z \in S, \varphi[y/z] \vdash \psi}{\Gamma \vdash \psi} \tag{2.2}$$

其中（$\exists_i$） t是任意项，而（$\exists_e$） z必须是一个新变量，且不能出现在 Γ、 φ、 ψ、 y中。这确保了关于显式集合的大多数自然数学证明都可以轻松地在PV中形式化；参见 [Li25第 4] 章，了解更多讨论。在本文其余部分，我们将仅非正式地描述证明，并在需要时指出如何将其形式化为PV 中的证明。

2.2 理论APX

直观地说，我们将该理论定义为 PV(P) 加上一些额外公理，用以形式化 P 能以指定精度近似计算给定电路的接受概率。换言之，对于每个确定性电路 C 以及任意 Δ，P(C, Δ) 输出一个有理数的编码，且该数保证落在区间 $[p-1/|\Delta|, p+1/|\Delta|]$ 内，其中 p 表示C的接受概率。为简单起见，我们还将 P(C, Δ) 记作 $\mathsf{P}_\delta(C)$，其中 $\delta^{-1} \triangleq |\Delta| \in \mathsf{Log}$ 表示计数精度。

APX 的语言APX。APX 是一种等式理论，其语言扩展了 PV 的语言，加入了新的函数符号 P，以及所有可通过 PV 的常见函数符号引入规则（包括复合和记号上的有界递归）引入的其他函数符号。

尽管PV 是一种以字符串为对象的等式理论，但命题联结词、算术运算和算术关系（例如有理数之间的比较）都可以用具有所需性质的适当方程编码（参见例如 [Li25]）。这使我们能够表述以下公理。

APX 的公理APX。这些公理只涉及全称量化变量，因此可以表示为 PV(P) 方程：

- （基本公理）。PV(P) 中任何可证方程都是 APX 的公理。此外，$[\mathsf{P}(C, \Delta) \in \mathbb{Q}] = 1$、$\mathsf{P}(C, \Delta) \leq 1$、$0 \leq \mathsf{P}(C, \Delta)$ 都是 APX 的公理，其中“$x \leq y$”由一个适当的 PV 方程形式化，当且仅当 $[x]_{\mathbb{Q}} \leq [y]_{\mathbb{Q}}$ 时该方程成立。

- （边界公理）。对于任意 $C \in B_n$，$\mathsf{IsConst}(C) \to \mathsf{P}_\delta(C) = \mathsf{Bool}(C)$。该公理指出，语法上为常值的电路[12] 若始终输出 $b \in \{0,1\}$，则其接受概率等于 b。
- （精度一致性公理）。对于每个 $n, \delta_1^{-1}, \delta_2^{-1}, \beta^{-1} \in \mathsf{Log}$ 以及每个 $C \in B_n$，

$$|\mathsf{P}_{\delta_1}(C) - \mathsf{P}_{\delta_2}(C)| \leq \delta_1 + \delta_2 + \beta. \tag{2.3}$$

  直观地说，该公理指出，近似计数函数 P 应与不同的精度参数保持一致。

- （局部一致性公理）。对于每个 n，δ^{-1}，$\beta^{-1} \in \mathsf{Log}$ 以及每个 $C \in B_n$，

$$\left|\mathsf{P}_\delta(C) - \frac{\mathsf{P}_\delta(\mathsf{Fix}_0(C)) + \mathsf{P}_\delta(\mathsf{Fix}_1(C))}{2}\right| \leq 2 \cdot \delta + \beta. \tag{2.4}$$

  直观地说，该公理指出，近似计数函数 P 应具有自洽性，即电路 C 的接受概率应接近通过随机固定 C 最右侧输入位而得到的电路的平均接受概率。

[12]换言之，从输出门到输入变量之间不存在路径，也就是说，电路的相关部分由作用于常量输入位的布尔运算构成。

APX 的规则。 最后，该理论包含以下推导规则：

- （逻辑规则）。我们列出 PV 的逻辑规则：

  1. $t_1 = t_2 \vdash t_2 = t_1$2. $t_1 = t_2$,
  $t_2 = t_3 \vdash t_1 = t_3$3. $t_1 = t_2 \vdash t_1$
  $(x/t) = t_2(x/t)$ 4. $u = v \vdash t(x/u)$
  $= t(x/v)$

- （结构归纳规则）。设 $f_1(x,\ \vec{y})$ 和 $f_2(x,\ \vec{y})$ 是 PV(P) 函数。对于 PV(P) 函数 $g(\vec{y})$、$h_0(x,\ \vec{y},\ z)$ 和 $h_1(x,\ \vec{y},\ z)$，若以下方程对于 $j \in \{1,2\}$ 和 $i \in \{0,1\}$ 可证

$$f_j(\varepsilon, \vec{y}) = g(\vec{y}) \tag{2.5}$$
$$f_j(s_i(x), \vec{y}) = h_i(x, \vec{y}, f_j(x, \vec{y})) \tag{2.6}$$

  那么我们可以推出方程 $f_1(x,\ \vec{y}) = f_2(x,\ \vec{y})$。这条规则类似于 PV 中原有的归纳规则。直观地说，这意味着如果 f_1 和 f_2 都与由 $g,\ h_0,\ h_1$ 递归定义的函数完全相同，那么它们就是同一个函数。

Remark 2.1（嵌套概率符号）. 我们强调，函数符号 P 不接受 P-预言机电路作为输入，因此，涉及嵌套概率符号的句子，例如

$$\Pr_x[\Pr_y[\varphi(x,y)] > \varepsilon] > \delta$$

无法直接在 APX 中形式化。然而，对于输入不重叠的谓词 $\varphi(x,p)$ 和 $\psi(y)$, s, 嵌套概 率

$$\Pr_x\left[\psi\left(x, \Pr_y[\varphi(y)]\right)\right]$$

可以表示为 在 APX 中，因为我们可以定义一个 P-预言机算法，先通过调用 t 计算 $p = \Pr_y[\varphi(y)]$ he P-预言机，然后 再通过调用 P-预言机计算 $\Pr_x[\psi(x,\ p)]$ 。

Remark 2.2（初等函数与精度问题）。 在我们的形式化中，有时会用到实数上的初等函数，例如 $\sqrt{x}$、$\ln(x)$ 或 $\exp(x)$（通常涉及常元，或涉及形如 a/b 且满足 $a,\ b \in \mathsf{Log}$ 的 x ）。由于这些函数的输出可能是无理数，要在 PV 中实现它们，我们需要为每个函数额外定义一个参数，用来确定精度位数。恰当定义这些函数后，基本不等式（例如 $\exp(x) \geq 1 + x$）的适当表述可以通过直接形式化标准数学证明，在 PV 中得到证明。本文在使用这类数值和不等式时，总会留出余量，以容忍任何潜在的精度问题（例如公理中的误差项 $\beta \in \mathsf{Log}^{-1}$ ）。因此，遵循标准做法，我们不会详细说明这类函数的实际实现及其基本性质。

2.3 APX 的模型

令 $\mathbb{M}$ 为 PV 的标准模型，也就是说，论域为 $\{0,1\}^*$，ε 被解释为空字符串，而 $s_0(x)$、$s_1(x)$ 分别被解释为向 x 末尾添加 0 和 1 的函数。对于每个函数 ˆ ˆ P: $\{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$，$\mathbb{M}$(P) 是 PV(P) 的模型，其中函数符号 P 被解释为函数 ˆ P。

ˆ定义 2.3 (标准模型**)**。 令 P: $\{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$ 为任意一个正确的近似计数函数，即

ˆ1. 对于每个电路 C: $\{0,1\}^* \to \{0,1\}$ 和 $\Delta \in \{0,1\}^*$，P(C, Δ) 都会输出一个有理数 $q \in [0,1]$（的编码），且该值位于区间 $[p - 1/|\Delta|, p + 1/|\Delta|]$ 内；其中 p 是 C 的接受概率，q 的长度至多为 $|C| \cdot |\Delta|^2$；并且

2. $\hat{\mathsf{P}}(C,\Delta)$ 当输入电路 C 满足 IsConst(C) 时，输出 $\{0,1\}$ 中的正确值 .

ˆ我们称 $\mathbb{M}$(P)是 APX 的标准模型 。

ˆ ˆ**定义 2.4** （容许模型）。 设 P: $\{0,1\}^* \times \{0,1\}^* \to \{0,1\}$ 是一个函数。若 $\mathbb{M}$(P) 满足 APX 的所有公理和规则，则称其为 APX 的可容许模型 。

关键观察是，一个模型是标准模型，当且仅当它是可容许模型。该定理的证明具有很强的构造性；事实上，在 APX_1 （参见第 3 节）的基础概率论的发展过程中，类似的归纳论证多次出现。

ˆ ˆ**定理2.5.** 设 $\mathsf{P}: \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$ 是任意函数。那么， $\mathbb{M}(\mathsf{P})$ 是标准模型，当且仅当它是可容许模型。

证明。 我们只证明 ($\Leftarrow$) 方向，反向显然成立。反设， $\mathbb{M}$(P) 是可容许模型，但不是标准模型。那么存在一个电路 C: $\{0,1\}^n \to \{0,1\}$ 和$\Delta \in \{0,1\}^*$ ，使得

$$\hat{\mathsf{P}}(C,\Delta) \notin p(C) \pm \frac{1}{|\Delta|}, \tag{2.7}$$

其中 $p(C) \triangleq \Pr_{x\in\{0,1\}^n}[C(x)=1]$ 是 C的接受概率。注意， C 和 Δ 由有限字符串编码（在 PV 的标准模型 $\mathbb{M}$ 中），且 $n \in \mathbb{N}$。

由于 $\hat{\mathsf{P}}$ 是可接受的，因此必须满足 Boundary Axiom。随后，当 $n=0$ 时，方程 (2.7) 不成立。只需考虑 $n>0$ 的情况。反设我们有

$$\left|\hat{\mathsf{P}}(C,\Delta) - p(C)\right| > \frac{1}{|\Delta|} + \varepsilon, \tag{2.8}$$

其中 $\varepsilon > 0$。令 $\Xi \triangleq 1^{10(n+1)/\varepsilon}$。由于 ˆP 满足 Precision Consistency Axiom，我们有

$$\left|\hat{\mathsf{P}}(C,\Xi) - p(C)\right| \geq \left|\hat{\mathsf{P}}(C,\Delta) - p(C)\right| - \left(\frac{1}{|\Delta|} + \frac{2}{|\Xi|}\right) > \varepsilon - \frac{2}{|\Xi|}. \tag{2.9}$$

令 C_0, C_1 为将 C 最右侧的输入位分别固定为 0 和 1 后得到的电路。由于 ˆP 必须满足 Local Consistency Axiom，我们有

$$\left|\hat{\mathsf{P}}(C,\Xi) - \frac{\hat{\mathsf{P}}(C_0,\Xi) + \hat{\mathsf{P}}(C_1,\Xi)}{2}\right| \leq \frac{3}{|\Xi|}, \tag{2.10}$$

此外， $p(C) = (p(C_0) + p(C_1))/2$ 由其定义。随后，存在 $\sigma \in \{0,1\}$ 使得 t

$$\left|\hat{\mathsf{P}}(C_\sigma,\Xi) - p(C_\sigma)\right| \geq \left|\hat{\mathsf{P}}(C,\Xi) - p(C)\right| - \frac{3}{|\Xi|}. \tag{2.11}$$

回顾一下， $n \in \mathbb{N}$ 是一个标准整数。设 $C^{(0)} \triangleq C$，以及 $C^{(1)} \triangleq C_\sigma$。根据上文定义的过程，对于每个 $1 \leq i \leq n$，我们可以将 $C^{(i)}$ 定义为由 $C^{(i-1)}$ 通过固定最右侧输入位而得到的电路，使得

$$\left|\hat{\mathsf{P}}(C^{(i)},\Xi) - p(C^{(i)})\right| \geq \left|\hat{\mathsf{P}}(C^{(i-1)},\Xi) - p(C^{(i-1)})\right| - \frac{3}{|\Xi|},$$

因此由方程（2.9），我们最终得到

$$\left|\hat{\mathsf{P}}(C^{(n)},\Xi) - p(C^{(n)})\right| \geq \varepsilon - \frac{6\cdot(n+1)}{|\Xi|} > 0.$$

注意，电路 $C^{(n)}$ 的输入长度为 0，因此计算的是一个常值函数。值$p(C^{(n)}) \in \{0,1\}$ 是其接受概率。由于 $\mathbb{M}$ (ˆP) 是可接受的，它满足 Boundary Axiom，因此 ˆP($C^{(n)}$, Ξ) $= p(C^{(n)})$。这与上述不等式矛盾。 □

定义 2.6。 在 APX 的标准模型中，将 P 解释为精确计数函数的模型称为 APX 的精确标准模型，记作 $\mathbb{M}^*$。

命题 2.7 (APX 的可靠性APX)。 APX 中的可证方程在任何 *APX* 的标准模型中都为真。

证明。 这可通过对证明进行归纳来验证。 □

2.4 一阶理论APX_1

类比一阶理论 PV_1,，我们将引入一阶理论 APX_1，它包含所有 APX 可证方程以及方便的推导规则。

APX 的语言$_1$。 一阶理论 APX_1 的语言包含所有 PV(P) 符号。

APX 的公理$_1$。 该理论由标准的带等词的一阶逻辑及以下非逻辑公理模式公理化：

- 对于 APX 中任意可证方程 $s(\vec{x}) = t(\vec{x})$，$\forall \vec{x}\ s(\vec{x}) = t(\vec{x})$ 是 APX_1 的一条公理。
- $\forall x\ \forall y\ (x = y \leftrightarrow s_i(x) = s_i(y))$，$i \in \{0,1\}$，是 APX_1 的一条公理。
- $\forall x\ \varepsilon \neq s_i(x)$ 是 APX_1 的一条公理。
- $\forall x\ s_0(x) \neq s_1(x)$ 是 APX_1 的一条公理。
- (n-归纳法)。设 φ 是一个无量词公式，且 $x_1, \ldots, x_n, \vec{y}$ 是变量。假设 φ 除 $x_1, \ldots, x_n$ 和 $\vec{y}$ 之外不含其他自由变量。那么

$$\forall \vec{y} \left(\bigwedge_{j \in [n]} \varphi(x_j/\varepsilon) \wedge \forall \vec{x} \left(\bigwedge_{\vec{\sigma} \in \{0,1\}^n} (\varphi \to \varphi_{\vec{\sigma}}) \right) \to \forall \vec{x}\ \varphi \right),$$

其中 $\varphi_{\vec{\sigma}}$ 表示公式 φ，该公式将 x_i 的所有自由出现都替换为 $s_{\sigma_i}(x_i)$（对每个 $i \in [n]$），这是 APX_1 的一条公理。

我们注意到，APX_1 满足以下性质。

命题 2.8. APX_1 可以进行全称公理化。

证明概要。 这本质上与证明 PV 可以进行全称公理化的证明相同（参见[Coo75、Kra95]）。请注意，APX_1 的所有公理都是全称句，除了 n-归纳公理模式，它是一个 $\forall\exists$-句。更具体地说，n-归纳公理模式在逻辑上等价于以下句子：对于每个 $\vec{y}$ 和 $\vec{x} = (x_1, \ldots, x_n)$，若满足

- $\varphi(x_j/\varepsilon)$ 对每个 $j \in [n]$ 都成立，并且
- $\neg\varphi$,

存在一个 $\vec{x}' = (x'_1, \ldots, x'_n)$ 和一个 $\vec{\sigma} = (\sigma_1, \ldots, \sigma_n) \in \{0,1\}^n$，使得 $\varphi(\vec{x}/\vec{x}')$ 为真，而 $\varphi(\vec{x}/\vec{x}'_\sigma)$ 为假，其中 $\vec{x}'_\sigma \triangleq (s_{\sigma_1}(x'_1) \ldots, s_{\sigma_n}(x'_n))$。然而，我们可以通过考察 x的前缀，设计一个直接的多项式时间算法，在给定 $\vec{x}$ 和 $\vec{y}$ 时输出这样的 $\vec{x}'$；并且该算法的正确性可以在 PV(P) 中得到证明。这可以用来证明 n-归纳公理模式可以从其他公理模式推导出来，并且 APX_1 可以进行全称公理化。 □

命题 2.9。 APX_1 是对APX的保守扩展。

证明概要。 证明与证明 PV_1 在 PV 上是保守的基本相同。我们建议感兴趣的读者参阅 [Coo75、Bus86、Kra95]，以了解更多详情。 □

与 PV_1 类似（参见 [KPT91]），我们可以证明，APX_1 中可证明一种针对无量词公式的归纳原理。为陈述这一结果，我们需要对记号作一些说明。

回顾一下，我们假设采用自然数的直接编码，例如[Coo75], 中的二进制编码，并使用 $[x]_{\mathbb{N}}$ 表示由 x编码的自然数。令 $\mathsf{Less}_{\mathbb{N}}(x,y)$ 为 PV 函数：如果（在标准模型中） $[x]_{\mathbb{N}} < [y]_{\mathbb{N}}$，则输出 1，否则输出 0。我们用 $[x < y]$ 作为 $\mathsf{Less}_{\mathbb{N}}(x,y)$ 的简写。我们用 $\forall x < y\ \varphi(x)$ 作为 $\forall x\ ([x < y] = 1 \to \varphi(x))$ 的简写，并用 $\exists x < y\ \varphi(x)$ 作为 $\exists x\ ([x < y] = 1 \wedge \varphi(x))$ 的简写。

定理 2.10。 令 $\varphi(x, \vec{y})$ 为一个无量词公式。则 APX_1 证明

$$\forall \vec{y}\ \forall b\ \left(\varphi(0,\vec{y}) \wedge \forall x < b\ (\varphi(x,\vec{y}) \to \varphi(x+1,\vec{y})) \to \varphi(b,\vec{y})\right),$$

其中，0 是编码 $0 \in \mathbb{N}$ 的 PV项，而 $+$ 是用于自然数加法的 PV函数。

证明概要。 该证明本质上与 PV_1,中这类归纳方案的可容许性证明相同，采用了二分搜索论证。有兴趣的读者可参阅 [Coo75、Bus86、KPT91、Kra95] 了解更多详情。 □

APX 的模型APX_1。 APX 的任意模型 $\mathcal{M}(\mathcal{P})$都会导出一个 APX_1 模型，且其论域以及对 PV(P)项的解释均相同。特别地，如果一个 APX_1 模型源自任意一个 APX 的标准模型，则称其为标准模型。APX_1 语言中的一阶句子 φ，若在任意标准模型中为真，则称为真句子。下面给出两个例子：

- 令 $C_{n,\ m} \equiv 0$ 为一个常值电路，它接受 $(x,\ y) \in \{0,1\}^n \times \{0,1\}^m$。该句子

  $$\forall n \in \mathsf{Log}\ \forall m \in \mathsf{Log}\ \forall x \in \{0,1\}^n\ \forall \delta^{-1} \in \mathsf{Log}\ \mathsf{P}_\delta(C(x,\cdot)) \le 2\delta$$

  在适当形式化后，是一个真句子，因为当 $\mathsf{P}_\delta(\cdot)$ 被解释为任意一个有效的、加性误差为 δ 的近似计数预言机时，该句子成立。
- 对于同一电路$C_{n,\ m}$，该句子

  $$\forall n \in \mathsf{Log}\ \forall m \in \mathsf{Log}\ \forall x \in \{0,1\}^n\ \forall \delta^{-1} \in \mathsf{Log}\ \mathsf{P}_\delta(C(x,\cdot)) = 0$$

  在精确标准模型中为真，但在如下标准模型中不为真：当 $D \neq C(x,\ \cdot)$时，$\mathsf{P}_\delta(C(x,\ \cdot)) \triangleq \delta$ 且$\mathsf{P}_\delta(D) \triangleq 0$。因此它不是真句子。

命题2.11 （APX_1的可靠性）。 在APX_1 中，任何可证的句子 φ 都是真句子。

证明。 这可以通过对证明进行归纳来验证。 □

3 APX_1中的概率推理

在本节中，我们证明若干元定理，用以展示APX_1 中近似计数函数的稳健性，并发展针对可行定义的随机变量的（近似）期望和方差等基本概念。

3.1 近似计数的一致性

现在我们陈述几个元定理，指出 APX 提供的近似计数功能在强意义下是一致的。

3.1.1 近似计数的全局一致性

单调性。 假设有两个电路 C_1，C_2：$\{0,1\}^n \to \{0,1\}$，满足对每个 $x \in \{0,1\}^n$，$C_1(x) \le C_2(x)$。那么，$C_1(x)$ 的接受概率至多为 $C_2(x)$ 的接受概率。因此，如果 P 是用于近似计数的函数，那么 P 报告的 C_1 的接受概率不应大于报告的 C_2 的接受概率加上两倍的计数精度。形式化地说：

引理 3.1. APX_1 证明

$$\forall n \in \mathsf{Log}\ \forall C_1, C_2 \in B_n\ \forall \delta^{-1} \in \mathsf{Log}\ \forall \beta^{-1} \in \mathsf{Log}$$
$$\big((\forall x \in \{0,1\}^n\ C_1(x) \le C_2(x) \to \mathsf{P}_\delta(C_1) \le \mathsf{P}_\delta(C_2) + 2 \cdot \delta + \beta\big).$$

证明。我们在 APX_1 中进行论证。Fix $\vec{y}$和 n，δ^{-1}，$\beta^{-1} \in \mathsf{Log}$ 以及电路 C_1，$C_2 \in B_n$。假设 $\forall x\ C_1(x) \le C_2(x)$。我们将证明

$$\mathsf{P}_\delta(C_1) \le \mathsf{P}_\delta(C_2) + 2 \cdot \delta + \beta.$$

令 $\eta^{-1} \in \mathsf{Log}$ 为一个稍后确定的参数，并令 $C^{k,\ x}_{\cdot\ 1}$，$C^{k,\ x}_{\cdot\ 2}$：$\{0,1\}^{n-k} \to \{0,1\}$ 分别为通过固定 C_1，C_2 中最右侧的 k 比特得到的电路，其中固定方式由 $x \in \{0,1\}^k$给出。

我们将证明 $\mathsf{P}_\eta(C_1) \le P_\eta(C_2) + 6 \cdot n \cdot \eta$。这就足够了，因为我们可以选择 $\eta = 1/(100 \cdot n \cdot \beta)$，并应用 Precision Consistency Axiom。

反设 $\mathsf{P}_\eta(C_1) > P_\eta(C_2) + 6 \cdot n \cdot \eta$。我们将设计一个 P-预言机算法，对于任意这样的 C_1，C_2 和 $k \le n$，输出一个长度为 k 的字符串 x，使其满足不变式

$$\mathsf{P}_\eta(C_1^{k,x}) > \mathsf{P}_\eta(C_2^{k,x}) + 6 \cdot (n-k) \cdot \eta.$$

此外，该算法的正确性可以在 APX_1 中证明。该算法是一个迭代算法，它依次考虑 $k = 0$，1、.....、n：

- 对于 $k = 0$，算法输出 ε。这是正确的，因为 $C^{0,\ \varepsilon}_{\cdot\ 1} = C_1, C_2 = C^{0,\ \varepsilon}_{\cdot\ 2}$，因此所需结论可由假设 $\mathsf{P}_\eta(C_1) > P_\eta(C_2) + 6 \cdot n \cdot \eta$ 推出。
- 现在假设该算法能够输出一个字符串 $x \in \{0,1\}^k$，使得

$$\mathsf{P}_\eta(C_1^{k,x}) > \mathsf{P}_\eta(C_2^{k,x}) + 6 \cdot (n-k) \cdot \eta.$$

我们的目标是输出一个字符串 $x' \in \{0,1\}^{k+1}$，使得

$$\mathsf{P}_\eta(C_1^{k+1,x'}) > \mathsf{P}_\eta(C_2^{k+1,x'}) + 6 \cdot (n-k-1) \cdot \eta.$$

注意，根据 Local Consistency Axiom[13]，我们知道

$$\mathsf{P}_\eta(C_1^{k,x}) \ge (1/2) \cdot (\mathsf{P}_\eta(\mathsf{Fix}(C_1^{k,x}, 0)) + \mathsf{P}_\eta(\mathsf{Fix}(C_1^{k,x}, 1))) - 3 \cdot \eta;$$
$$\mathsf{P}_\eta(C_2^{k,x}) \le (1/2) \cdot (\mathsf{P}_\eta(\mathsf{Fix}(C_2^{k,x}, 0)) + \mathsf{P}_\eta(\mathsf{Fix}(C_2^{k,x}, 1))) + 3 \cdot \eta.$$

随后，必定存在 $\sigma \in \{0,1\}$，使得 $\mathsf{P}_\eta(\mathsf{Fix}(C^{k,\ x}_{\cdot\ 1}, \sigma)) > \mathsf{P}_\eta(\mathsf{Fix}(C^{k,\ x}_{\cdot\ 2}, \sigma)) + 6 \cdot (n-k-1) \cdot \eta$。算法查询 P-预言机，找到这样的 $\sigma \in \{0,1\}$，并输出 $x' \triangleq \sigma \circ x$。这满足不变式，因为 $\mathsf{Fix}(C^{k,\ x}_{\cdot\ 1}, \sigma) = C^{k,\ \sigma \circ x}_{\cdot\ 1}$，且 $\mathsf{Fix}(C^{k,\ x}_{\cdot\ 2}, \sigma) = C^{k,\ \sigma \circ x}_{\cdot\ 2}$。

显然，该算法的正确性可以在 APX_1 中用针对开放公式的归纳法加以证明。[14]由此可知，当我们固定 $k = n$时，该算法可证地输出 $x^\star \in \{0,1\}^n$，使得在假设 $\mathsf{P}_\eta(C_1) > P_\eta(C_2) + 6 \cdot n \cdot \eta$下，$\mathsf{P}_\eta(C^{n,\ x^\star}_{\cdot,1}) > \mathsf{P}_\eta(C^{n,\ x^\star}_{\cdot,2})$。注意，$C^{n,\ x}_{\cdot,1}$ 与 $C^{n,\ x}_{\cdot,2}$ 是不读取其输入、并分别输出 $C_1(x^\star)$和 $C_2(x^\star)$的电路。这违反了 Boundary Axiom，因为对每个 $x \in \{0,1\}^n$都有$C_1(x) \le C_2(x)$。 □

[13]此处，局部一致性公理中的参数 β 设为 η。[14]形式上，我们对 $n = 1$使用 n-归纳法，并依赖这样一个事实：开放公式具有足够的表达能力，即 APX_1 的语言包含函数符号 P，以及可访问 P 的预言机多项式时间函数。

全局一致性。 单调性的一个推论是：若两个电路可证地相同，则由预言机 P 给出的它们的接受概率不应有显著差异。形式化地说：

引理 3.2。APX_1 证明

$$\forall n \in \mathsf{Log}\ \forall C_1, C_2 \in B_n\ \forall \delta^{-1}, \beta^{-1} \in \mathsf{Log}$$
$$\big((\forall x \in \{0,1\}^n\ C_1(x) = C_2(x)) \to |\mathsf{P}_\delta(C_1) - \mathsf{P}_\delta(C_2)| \le 2 \cdot \delta + \beta\big).$$

证明。根据引理 3.1，我们可以证明：对于任意 $x \in \{0,1\}^n$，如果 $C_1(x) = C_2(x)$，那么 $\mathsf{P}_\delta(C_1) - \mathsf{P}_\delta(C_2) \le 2 \cdot \delta + \beta$，且 $\mathsf{P}_\delta(C_2) - \mathsf{P}_\delta(C_1) \le 2 \cdot \delta + \beta$。随后，只要绝对值函数定义得当，我们就有 $|\mathsf{P}_\delta(C_1) - \mathsf{P}_\delta(C_2)| \le 2 \cdot \delta + \beta$。

□

Remark 3.3。 在 APX_1 中，对多项式时间可判定性质进行近似计数的标准方法是先将其转换为电路 C，然后查询 $\mathsf{P}_\delta(C)$。全局一致性性质表明，近似计数预言机 P 对于将 PV 函数转换为电路具有鲁棒性，前提是我们能在 APX_1 中证明该转换在函数意义上正确。后者已经可以在 PV_1 中完成（例如，参见 [Pic14，第2节。4]）。

3.1.2 近似计数的置换对称性

接下来，我们将证明近似计数预言机 P 具有置换对称性，也就是说，对输入变量进行置换，不会显著改变 P 给出的接受概率。

局部对称性。 首先，我们证明交换电路中两个相邻输入位不会显著改变接受概率。具体来说：

引理 3.4。 APX_1 证明

$$\forall n \in \mathsf{Log}\ \forall i \in [n-1]\ \forall C \in B_n\ \forall \delta^{-1}, \beta^{-1} \in \mathsf{Log}\ |\mathsf{P}_\delta(C) - \mathsf{P}_\delta(\mathsf{Swap}(C,i))| \le 2 \cdot \delta + \beta,$$

其中 $\mathsf{Swap}(C,i)$ 是一个 PV 函数，它输出电路 C'：该电路通过交换 C 从最右位起第 i 位和第 $(i+1)$ 位输入位得到。

证明。 我们在 APX_1 中进行论证。取 $n \in \mathsf{Log}$、$i \in [n-1]$、$C \in B_n$、$\delta^{-1} \in \mathsf{Log}$ 和 $\beta^{-1} \in \mathsf{Log}$。令 $\eta^{-1} \in \mathsf{Log}$ 为稍后确定的参数。

对于 $C \in B_n$ 和 $|x| < n$，我们将 $\mathsf{Fix}(C,x)$ 定义为 PV 函数，它输出一个电路，该电路是通过将 C 的最后 $|x|$ 个输入位固定为 x 而得到的；也就是说，它输出 $C_x \in B_{n-|x|}$，使得 $C_x(u) = C(u \circ x)$。注意，对于定义恰当的 PV 函数 Swap 和 Fix，我们可以在 PV 中证明：若 $|x| = i-1$，$\sigma = (\sigma_1, \sigma_2) \in \{0,1\}^2$，$C^{12}_{x,\sigma} \triangleq \mathsf{Fix}(C, \sigma_1 \circ \sigma_2 \circ x)$ 与 $C^{21}_{x,\sigma} \triangleq \mathsf{Fix}(\mathsf{Swap}(C,i)\ \sigma_2 \circ \sigma_1 \circ x)$ 函数等价。此外，我们可以假设，在 PV 中可证明：对于任意电路 $C \in B_n$，$x \in \{0,1\}^k$ 和 $z \in \{0,1\}^{n-k-1}$，$\mathsf{Eval}(\mathsf{Fix}(C,x)\ s_i(z)) = \mathsf{Eval}(\mathsf{Fix}(C, s_i(x))\ z)$，且 $\mathsf{Fix}(C,\varepsilon) = C$。

因此，根据近似计数的全局一致性，我们可得

$$\forall x \in \{0,1\}^{i-1}\ \forall \sigma \in \{0,1\}^2\ |\mathsf{P}_\eta(C^{12}_{x,\sigma}) - \mathsf{P}_\eta(C^{21}_{x,\sigma})| \le 3 \cdot \eta. \tag{3.1}$$

也就是说，对于 $x \in \{0,1\}^{i-1}$，如果我们任意固定 最右边的 两位 $\mathsf{Fix}(C,\ x)$ 和 $\mathsf{Fix}(\mathsf{Swap}(C,\ i)\ x)$，它们的接受概率彼此接近。通过两次应用 Local Consistency Axiom，随后利用近似计数的全局一致性，我们可以证明

$$\forall x \in \{0,1\}^{i-1}\ \left|\mathsf{P}_\eta(\mathsf{Fix}(C,x)) - (1/4) \sum_{\sigma \in \{0,1\}^2} \mathsf{P}_\eta(C^{12}_{x,\sigma})\right| \le 10 \cdot \eta;$$

$$\forall x \in \{0,1\}^{i-1}\ \left|\mathsf{P}_\eta(\mathsf{Fix}(\mathsf{Swap}(C,i),x)) - (1/4) \sum_{\sigma \in \{0,1\}^2} P_\eta(C^{21}_{x,\sigma})\right| \le 10 \cdot \hat{\eta}.$$

随后，由方程（3.1）可知

$$\forall x \in \{0,1\}^{i-1} \ |\mathsf{P}_\eta(\mathsf{Fix}(C,x)) - \mathsf{P}_\eta(\mathsf{Fix}(\mathsf{Swap}(C,i),x))| \le 20 \cdot \eta. \tag{3.2}$$

这表明，当 C 和 $\mathsf{Swap}(C, i)$ 的最右侧 $i-1$ 个比特均由 $x \in \{0,1\}^{i-1}$ 固定时，它们的接受概率相近。

现在我们将证明

$$|\mathsf{P}_\eta(C) - \mathsf{P}_\eta(\mathsf{Swap}(C,i))| \le 20 \cdot (n+1) \cdot \eta. \tag{3.3}$$

这就足够了 因为我们可以选取 $\eta \triangleq \beta/(100 \cdot (n+1))$ 并应用 Precision Consistency Axiom .

反设方程（3.3）不成立。我们设计一个迭代算法，该算法给定 C、i 和 $k \le i-1$，输出一个长度为 k 的字符串 x，使得

$$|\mathsf{P}_\eta(\mathsf{Fix}(C,x)) - \mathsf{P}_\eta(\mathsf{Fix}(\mathsf{Swap}(C,i),x))| > 20 \cdot (n+1-k) \cdot \eta.$$

该算法与引理 3.1 证明中的算法基本相同，即在每次迭代中通过查询近似计数预言机将字符串扩展一位。特别地，基础情形$k = 0$ 满足，因为方程（3.3）不成立。因此，对于 $k = i-1$，该算法输出一个字符串 $x \in \{0,1\}^{i-1}$，使得

$$|\mathsf{P}_\eta(\mathsf{Fix}(C,x)) - \mathsf{P}_\eta(\mathsf{Fix}(\mathsf{Swap}(C,i),x))| > 20 \cdot (n+1-i) \cdot \eta \ge 20 \cdot \eta.$$

这违反了方程（3.2），从而完成了证明。 □

置换对称性。 接下来，我们可以通过将一个置换分解为一系列变换 $C \mapsto \mathsf{Swap}(C, i)$，来陈述并证明近似计数的置换对称性。

我们假设采用一种简单直接的编码来表示 $[n]$ for $n \in \mathsf{Log}$ 的置换，并将 $\pi \in S_n$ 作为“π 是 $[n]$ 的一个置换”的简写，该简写由一个简单直接的 PV 函数编码。设 $C \in B_n$ 和$\pi \in S_n$ 是 $[n]$ 的一个置换。我们定义 $\mathsf{Permute}(C, \pi)$ 为输出电路 $C \circ \pi \in B_n$ 的 PV 函数，该电路定义为 $(C \circ \pi)(x) = C(x_{\pi_n} \circ \cdots \circ x_{\pi_1})$。于是有：

引理 3.5。 $\mathsf{APX}_1 \vdash \forall n \in \mathsf{Log} \ \forall \pi \in S_n \ \forall C \in B_n \ \forall \delta^{-1}, \ \beta^{-1} \in \mathsf{Log} \ |\mathsf{P}_\delta(C) - \mathsf{P}_\delta(C \circ \pi)| \le 2 \cdot \delta + \beta$。

证明概要。 通过对 $[n]$ 的置换进行直接编码，我们可以在 PV 中证明：对于某个 $k \in \mathsf{Log}$，存在一个列表 $\ell = (i_1, \ldots, i_k)$，使得 $C \circ \pi$ 与定义如下的 C_k 函数等价

$$C_0 \triangleq C, \quad C_j \triangleq \mathsf{Swap}(C_{j-1}, i_j) \quad (j \in [k]).$$

对 j 进行归纳法，我们可以通过应用引理 3.4 证明：对于任意 $\eta \in \mathsf{Log}$， $|\mathsf{P}\eta(C) - \mathsf{P}\eta(C_j)| \le 3 \cdot j \cdot \eta$。再结合近似计数的 全局一致性，可推出

$$|\mathsf{P}_\eta(C) - \mathsf{P}_\eta(C \circ \pi)| \le 3 \cdot (k+1) \cdot \eta.$$

然后，我们取 $\eta \triangleq \beta/(10 \cdot (k+1))$ 并应用 Precision ConsistencyAxiom 来证明该引理。

□

3.1.3 近似计数的存在性引理

一个重要的计数原理是：如果某个数学对象能够以非零概率被采样，那么它必然 存在。这一简单结果是组合数学中著名概率方法的基石（例如参见 [AS16]）。下面的引理在近似计数的背景下将这一原理形式化：

引理 3.6. $\mathsf{APX}_1 \vdash \forall n, \delta^{-1}, \beta^{-1} \in \mathsf{Log} \ \forall C \in B_n \, (\beta > 0 \wedge \mathsf{P}_\delta(C) > \delta + \beta \to \exists x \in \{0,1\}^n \ C(x) = 1$。

证明。 我们在 APX_1 中进行论证。任取 $n, \delta^{-1}, \beta^{-1} \in \mathsf{Log}$ 和 n-输入电路 $C \in B_n$。假设 $\beta > 0$ 且 $\mathsf{P}_\delta(C) > \delta + \beta$，并令 $\eta^{-1} \in \mathsf{Log}$ 稍后确定。

根据 Precision Consistency Axiom，我们可以看出$\mathsf{P}_\eta(C) \geq \beta - \eta$。反设，对每个 $x \in \{0,1\}^n$，$C(x) = 0$。在这种情况下，$C(\vec{x})$ 等价于始终输出 0 的电路Null_n。根据近似计数的全局一致性，我们有

$$\mathsf{P}_\eta(\mathsf{Null}_n) \geq \mathsf{P}_\eta(C) - 3\eta \geq \beta - 4\eta.$$

令 $\eta = \beta/10$。我们有 $\mathsf{P}_\eta(\mathsf{Null}_n) > 3\eta$，这与 Boundary Axiom 矛盾。 □

我们指出，该原理的一个更一般版本将在第3.2.3 节中证明，论证与此类似，但更复杂。稍后我们将用它来证明近似期望的线性。

3.1.4 具体电路的近似计数

在本小节中，我们考察近似计数预言机对具体电路的行为：解析输入为一个数值，并在其小于固定阈值时输出 1 的“less-than-t”电路，以及输入数量较少的电路。

“小于t”电路。 设 $t \in \{0,1,\ldots,2^n\}$、$C_{<t}: \{0,1\}^n \to \{0,1\}$ 为这样一个电路：它将其输入解析为数 $x \in \{0,1,\ldots,2^n-1\}$ 的二进制编码，并且当且仅当 $x < t$ 时接受。下面的引理表明，在 APX_1 中，$C_{<t}$ 的接受概率近似为 $t/2^n$，符合预期。

引理3.7 （小于t 电路）。 $\mathsf{APX}_1 \vdash \forall n,\ \delta^{-1},\ \beta^{-1} \in \mathsf{Log}\ \forall t \in \{0,1,\ldots,2^n\}\ |\mathsf{P}_\delta(C_{<t}) - t/2^n| \leq \delta + \beta$。

证明。 我们在 APX_1 中论证。Fix $n,\ \delta^{-1},\ \beta^{-1},\ t \in \{0,1,\ldots,2^n\}$。令 $\eta^{-1} \in \mathsf{Log}$ 为稍后确定的参数。注意，当 $t = 2^n$ 时，$C_{<t}$ 与 True_n 函数等价，因此该引理直接由 全局一致性 与 Boundary Axiom 得出。[15] 在证明的其余部分，我们假设 $t < 2^n$。

反设 $|\mathsf{P}_\delta(C_{\leq t}) - t/2^n| > \delta + \beta$。根据 Precision ConsistencyAxiom，我们有 $|\mathsf{P}_\eta(C_{<t}) - \mathsf{P}_\delta(C_{<t})| \leq \delta + 2\eta$，继而

$$|\mathsf{P}_\eta(C_{<t}) - t/2^n| > \beta - 2\eta.$$

我们可以假设 t 的最右位是最高有效位；根据置换对称性，这不失一般性。

我们将设计一个 P-预言机迭代算法，在第 i 次迭代中输出满足以下条件的 $t_i \in \{0,1,\ldots,2^{n-i}-1\}$:

- 令 $C_i: \{0,1\}^{n-i} \to \{0,1\}$ 为一个电路，它将输入解析为数字 $x \in \{0,1,\ldots,2^{n-i}-1\}$，并在 $x < t_i$ 时输出 1。于是 $\left|\mathsf{P}_\eta(C_i) - t_i/2^{n-i}\right| > \beta - 20\eta \cdot (i+1)$。

算法从 $t_0 \triangleq t$ （因此也从 $C_0 \triangleq C_{<t}$）开始。在第 i 次迭代中，算法考察 t_i 的最右位（即最高有效位）。回想一下，$\mathsf{Fix}(C,\ b)$ 输出通过将最右输入位固定为 b 而从 C 得到的电路。

如果 t_i 的最右位是 0，算法就输出 $t_{i+1} \triangleq t_i$。显然，$\mathsf{Fix}(C_i, 1)$ 与 Null_{n-i-1} 函数等价，因此根据全局一致性和 Boundary Axiom，$\mathsf{P}_\eta(\mathsf{Fix}(C_i, 1)) \leq 3\eta$。令 C_{i+1} 为一个电路，它将输入解析为数字 $x \in \{0,1,\ldots,2^n-1\}$，并在 $x < t_{i+1}$ 时输出 1。由此可得，$\mathsf{Fix}(C_i, 0)$ 与 C_{i+1} 函数等价，因此根据近似计数的全局一致性

[15] 要使这一步成立，我们需要能够证明 $C_{<t}$ 等价于 True_n。对于电路 $C_{<t}$ 的一种自然实现，这在 PV_1 中成立。

计数，$|\mathsf{P}_\eta(\mathsf{Fix}(C_i,\ 0))\ -\mathsf{P}_\eta(C_{i+1})| \le 3\eta$。随后：

$$
\begin{aligned}
&\left|\mathsf{P}_\eta(C_{i+1}) - t_{i+1}/2^{n-i-1}\right| \\
\ge\ &\left|\mathsf{P}_\eta(\mathsf{Fix}(C_i,0)) - t_{i+1}/2^{n-i-1}\right| - 3\eta \\
\ge\ &\left|\mathsf{P}_\eta(\mathsf{Fix}(C_i,0)) + \mathsf{P}_\eta(\mathsf{Fix}(C_i,1)) - t_{i+1}/2^{n-i-1}\right| - 6\eta \\
=\ &2\cdot\left|\frac{\mathsf{P}_\eta(\mathsf{Fix}(C_i,0)) + \mathsf{P}_\eta(\mathsf{Fix}(C_i,1))}{2} - \frac{t_{i+1}}{2^{n-i}}\right| - 6\eta \\
\ge\ &2\cdot\left|\mathsf{P}_\eta(C_i) - t_i/2^{n-i}\right| - 12\eta \qquad \text{(Local Consistency Axiom)} \\
>\ &\beta - 20\eta\cdot(i+1) - 12\eta \ge \beta - 20\eta\cdot(i+2).
\end{aligned}
$$

如果 t_i 的最右位为 1，算法就输出 $t_{i+1} = t_i - 2^{n-i-1}$。显然，$\mathsf{Fix}(C_i, 0)$ 与 True_{n-i+1} 函数等价，因此根据全局一致性和 Boundary Axiom，$|\mathsf{P}_\eta(\mathsf{Fix}(C_i, 0)) - 1| \le 3\eta$。令 C_{i+1} 为一个电路，它将输入解析为数字 $x \in \{0, 1, \ldots, 2^n - 1\}$，并在$x < t_{i+1}$时输出 1。由此可知，$\mathsf{Fix}(C_i, 1)$ 与 C_{i+1} 函数等价，因此根据近似计数的全局一致性，$|\mathsf{P}_\eta(\mathsf{Fix}(C_i, 1)) - \mathsf{P}_\eta(C_{i+1})| \le 3\eta$。随后：

$$
\begin{aligned}
&\left|\mathsf{P}_\eta(C_{i+1}) - t_{i+1}/2^{n-i-1}\right| \\
\ge\ &\left|\mathsf{P}_\eta(\mathsf{Fix}(C_i,1)) - t_{i+1}/2^{n-i-1}\right| - 3\eta \\
\ge\ &\left|\mathsf{P}_\eta(\mathsf{Fix}(C_i,0)) - 1 + \mathsf{P}_\eta(\mathsf{Fix}(C_i,1)) - t_{i+1}/2^{n-i-1}\right| - 6\eta \\
=\ &2\cdot\left|\frac{\mathsf{P}_\eta(\mathsf{Fix}(C_i,0)) + \mathsf{P}_\eta(\mathsf{Fix}(C_i,1))}{2} - \frac{t_{i+1} + 2^{n-i-1}}{2^{n-i}}\right| - 6\eta \\
=\ &2\cdot\left|\frac{\mathsf{P}_\eta(\mathsf{Fix}(C_i,0)) + \mathsf{P}_\eta(\mathsf{Fix}(C_i,1))}{2} - \frac{t_i}{2^{n-i}}\right| - 6\eta \\
\ge\ &2\cdot\left|\mathsf{P}_\eta(C_i) - t_i/2^{n-i}\right| - 12\eta \qquad \text{(Local Consistency Axiom)} \\
>\ &\beta - 20\eta\cdot(i+1) - 12\eta \ge \beta - 20\eta\cdot(i+2).
\end{aligned}
$$

显然，根据 APX_1 所允许的、针对可在多项式时间内验证的性质的归纳原理，算法的正确性便可得出。因此，经过 n 次迭代后，算法将输出 $t_n = 0$，使得电路 $C_n \equiv \mathsf{Null}_0$ 的接受概率至少为$\beta - 20\eta\cdot(n+1)$。令 $\eta \triangleq \beta/(40n+40)$，即可利用 BoundaryAxiom 得出矛盾。

□

短输入电路。对于电路 $C: \{0,1\}^n \to \{0,1\}$ 使得 $n \in \mathsf{LogLog}$ 可以枚举 C 的所有输入。下面的引理表明，$\mathsf{P}_\delta(C)$ 与通过暴力搜索算法计算出的接受概率一致。

引理 3.8（暴力计数引理）。APX_1 证明了以下陈述。对于任意 $n \in \mathsf{LogLog}$、电路 $C \in B_n$ 以及 $\delta^{-1},\ \beta^{-1} \in \mathsf{Log}$，令 t 表示 C 的接受输入数量。那么 $|\mathsf{P}_\delta(C) - t/2^n| \le \delta + \beta$。特别地，如果 $\delta \le 2^{-n-1}$，则 t 是 $\mathsf{P}_\delta(C)\cdot 2^n$ 的最近整数。

该引理的证明使用了 Local Consistency Axiom 和 Precision ConsistencyAxiom。我们将使用以下一般工具形式化这一论证：如果存在一系列电路，作为电路 C 的近似计数算法，并且满足边界条件且局部一致，那么该算法估计的接受概率必然接近 $\mathsf{P}_\delta(C)$。形式化地说：

引理 3.9（对决引理）。APX_1 证明了以下命题。设 $n \in \mathsf{Log}$，$C \in B_n$ 是一个电路，且$P_0, P_1, \ldots, P_n$ 是输出有理数的电路，使得 P_i 的输入长度为 i。设 $\delta^{-1}, \eta^{-1} \in \mathsf{Log}$。假设对于每个 $i < n$ 和每个 $x \in \{0,1\}^i$，

$$\left|P_i(x) - \frac{P_{i+1}(x\circ 0) + P_{i+1}(x\circ 1)}{2}\right| \le \eta;$$

并且对于每个 $x \in \{0,1\}^n$, $P_n(x) = C(x)$。那么 $|\mathsf{P}_\delta(C) - P_0| \le \delta + 4\eta \cdot (n+1)$。

证明。我们在 APX_1 中进行论证。固定 $n \in \mathsf{Log}$、$C \in B_n$、电路 P_0、P_1、……、P_n 以及 δ^{-1}、$\eta^{-1} \in \mathsf{Log}$。假设它满足引理中的两个条件。反设 $|\mathsf{P}_\delta(C) - P_0| > \delta + 3\eta \cdot (n+1)$。根据 Precision Consistency Axiom，我们有 $|\mathsf{P}_\eta(C) - P_0| > 4\eta \cdot n + 3\eta$。

令 C^x 为通过将 C 的最右侧 $|x|$ 个比特固定为 x 而得到的电路。考虑以下算法：在第 i 次迭代中，输出满足 $|\mathsf{P}_\eta(C^{x_i}) - P_i(x_i)| > 4\eta \cdot (n-i) + 3\eta$ 的 $x_i \in \{0,1\}^i$。算法从 $x_0 \triangleq \varepsilon$ 开始。在第 i 次迭代中，根据 Local Consistency Axiom，我们知道

$$\begin{aligned}
|\mathsf{P}_\eta(C^{x_i}) - P_i(x_i)| &\le \left| \frac{\mathsf{P}_\eta(C^{0\circ x_i}) + \mathsf{P}_\eta(C^{1\circ x_i})}{2} - P_i(x_i) \right| + 3\eta \\
&\le \left| \frac{\mathsf{P}_\eta(C^{0\circ x_i}) + \mathsf{P}_\eta(C^{1\circ x_i})}{2} - \frac{P_{i+1}(0\circ x_i) + P_{i+1}(1\circ x_i)}{2} \right| + 4\eta \\
&\le \frac{1}{2}\Big(|\mathsf{P}_\eta(C^{0\circ x_i}) - P_{i+1}(0\circ x_i)| + |\mathsf{P}_\eta(C^{1\circ x_i}) - P_{i+1}(1\circ x_i)| \Big) + 4\eta.
\end{aligned}$$

这意味着对于某个 $\sigma \in \{0,1\}$, $|\mathsf{P}_\eta(C^{\sigma\circ x_i}) - P_{i+1}(\sigma \circ x_i)| > 4\eta \cdot (n-i-1) + 3\eta$。随后，算法通过设置 $x_{i+1} = \sigma \circ x_i$ 继续执行。

显然，可以对无量词公式进行归纳法来证明该算法的正确性，而 APX_1 中具备这种归纳法。因此，在第 n 次迭代中，算法输出一个字符串 $x_n \in \{0,1\}^n$，使得 $|\mathsf{P}_\eta(C^{x_n}) - P_n(x_n)| > 3\eta$。然而，这违反了 Boundary Axiom，因为 $P_n(x_n) = C(x_n)$，且电路 C^{x_n} 是一个输出 $C(x_n)$ 的常值电路。 □

引理 3.8 的证明。我们在 APX_1 中进行论证。取 $n \in \mathsf{LogLog}$ 以及 $C \in B_n$, $\delta^{-1}, \beta^{-1} \in \mathsf{Log}$，并令 t 为 C 的接受输入数量。令 $P_0, \ldots, P_n$ 为满足以下条件的电路：$P_i(x)$ 接受一个 i 位输入 x，并输出 C^x 的接受概率：$\{0,1\}^{n-i} \to \{0,1\}$ 定义为 $C^x(z) = C(z \circ x)$。特别地，$P_0 = t/2^n$。令 $\eta^{-1} \in \mathsf{Log}$，稍后再确定其值。

由于 $n \in \mathsf{LogLog}$，因此可以在 PV_1 中证明 P_0、……、P_n 满足 对决引理 中的条件。于是，$|\mathsf{P}_\delta(C) - P_0| = |\mathsf{P}_\delta(C) - t/2^n| \le \delta + 4\eta \cdot (n+1)$。将 $\eta \triangleq \beta/(4n+4)$ 代入即可得到该引理。 □

3.2 近似期望及其基础理论

W现在我们来建立可行随机变量及其近似期望的理论 .

3.2.1 随机变量与近似期望的定义

我们首先定义取值于 $\mathbb{Q}$ 的离散随机变量的近似期望。回顾一下，显式集合是指由显式列表编码的集合；特别地，显式集合的大小总是可行的。为了使期望能够被可行地（近似）计算，我们将讨论范围限制在随机变量的支撑集为显式集合的情形。

设 $n \in \mathsf{Log}$，V 是一个由有理数组成的显式集合，C 是一个多输出电路，使得 APX_1 可以证明

$$\forall x \in \{0,1\}^n \; C(x) \in V.$$

我们称 (V, n, C) 定义了一个随机变量 $X \triangleq C(\mathcal{U}_n)$，并将 X 的期望定义为

$$\sum_{v \in V} v \cdot \Pr_x[C(x) = v],$$

其中，概率可以通过 APX 中的近似计数量词 P 来实现。由此得到随机变量和期望的如下形式化定义。

定义 3.10（随机变量）。设 V 是一个有理数显式集合，$n \in \mathsf{Log}$，且 C 是一个多输出电路。我们称 (V, n, C) 在 V 上定义了随机变量 X，如果 $\forall x \in \{0,1\}^n \; C(x) \in V$。集合 V 称为 X的支撑集，C 称为 X的采样器，而 n 称为 X 的种子长度。

定义 3.11（近似期望）。设 (V, n, C) 是定义随机变量 X 的元组，其取值范围为 V，且 $\delta^{-1} \in \mathsf{Log}$。我们将 X 的近似期望 定义为 $\mathbb{E}_\delta[X]$，记作

$$\sum_{v \in V} v \cdot \mathsf{P}_\delta(C_v),$$

其中，C_v 是一个 n输入电路，给定 $x \in \{0,1\}^n$后，若 $C(x) = v$（分别为 $C(x) \neq v$），则输出1（分别输出0）。"$\cdot$"表示有理数的乘法，而 $\sum$ 表示有理数的求和。

注意，存在一个 PV(P) 函数 $\mathsf{E}(V, n, C, \Delta)$，用于计算随机变量 X的 $\mathbb{E}_{|\Delta|^{-1}}[X]$；该随机变量由$(V, n, C)$定义。它遍历 $v \in V$，构造电路 C_v，调用预言机 $p_v \leftarrow \mathsf{P}(C_v, \Delta)$，并对所有 $v \in V$的 $v \cdot p_v$ 求和。为证明该算法是可行的，请注意，V是一个规模可行的显式集合；此外，在第 2.1 节规定的编码下，V中所有有理数的总长度在 PV 中可证明是可行的。

为简单起见，我们使用记号 $C: \{0,1\}^n \to \mathbb{Q}$ 表示 C 是一个多输出电路，其输出被解析为一个有理数。

此外，可以将电路 $C: \{0,1\}^n \to \{0,1\}$ 的接受概率视为指示随机变量 $I_C \triangleq (\{0,1\}, n, C)$的期望，并允许一个较小的加性误差，如下述命题所示。因此，我们接下来将证明的期望性质，也适用于近似计数。

命题 3.12. APX_1 证明以下陈述。设 $n, \delta^{-1} \in \mathsf{Log}$和 $C: \{0,1\}^n \to \{0,1\}$ 是一个布尔电路。设 $I_C \triangleq (\{0,1\}, n, C)$ 是 $C(x) = 1$的指示随机变量。那么，对于任意$\beta^{-1} \in \mathsf{Log}$，$|\mathsf{P}_\delta(C) - \mathbb{E}_\delta[I_C]| \leq 2\delta + \beta$。

证明。我们在 APX_1中进行论证。固定 n，δ^{-1}，$\beta^{-1} \in \mathsf{Log}$ 和一个电路 $C: \{0,1\}^n \to \{0,1\}$。根据近似期望的定义，我们知道 $\mathbb{E}_\delta[I_C] = 1 \cdot \mathsf{P}_\delta[C_1]$，其中 $C_1(x)$ $C(x)$是函数等价的电路。根据近似计数的 Global Consistency，我们有

$$|\mathsf{P}_\delta(C) - \mathbb{E}_\delta[I_C]| = |\mathsf{P}_\delta(C) - \mathsf{P}_\delta[C_1]| \leq 2\delta + \beta. \qquad \square$$

3.2.2 近似期望的基本性质

精度一致性。与近似计数的 Precision Consistency Axiom 类似，正如下述命题所示，近似期望的定义对于不同精度是一致的。

命题 3.13。APX_1 证明以下陈述。设 $n, \delta_1^{-1}, \delta_2^{-1} \in \mathsf{Log}$，$C: \{0,1\}^n \to \mathbb{Q}$, $V \subseteq \mathbb{Q}$为一个显式集合，使得 $\forall x \in \{0,1\}^n$ $C(x) \in V$。设 X 为由 (V, n, C) 定义的随机变量。那么对每个 $\beta^{-1} \in \mathsf{Log}$，

$$|\mathbb{E}_{\delta_1}[X] - \mathbb{E}_{\delta_2}[X]| \leq (\delta_1 + \delta_2 + \beta) \cdot \|V\|,$$

其中 $\|V\| \triangleq \sum_{v \in V} |v|$ 是 V 的 ℓ_1-范数，$|v|$ 表示有理数 v 的绝对值。

证明。我们在 APX_1 中进行论证。回忆一下，C_v 是一个电路：若 $C(x) = v$，则输出 1；否则输出 0。根据近似计数的定义，我们可以看出

$$\begin{aligned}
|\mathbb{E}_{\delta_1}[X] - \mathbb{E}_{\delta_2}[X]| &= \left| \sum_{v \in V} v \cdot \mathsf{P}_{\delta_1}(C_v) - \sum_{v \in V} v \cdot \mathsf{P}_{\delta_2}(C_v) \right| \\
&\leq \left| \sum_{v \in V} v \cdot (\mathsf{P}_{\delta_1}(C_v) - \mathsf{P}_{\delta_2}(C_v) \right| \\
&\leq \left| \sum_{v \in V} v \cdot (\delta_1 + \delta_2 + \beta) \right| \leq (\delta_1 + \delta_2 + \beta) \cdot \|V\|,
\end{aligned}$$

其中倒数第二个不等式由 Precision Consistency Axiom得出 . $\square$

局部一致性。 同样地，我们可以通过随机地将随机种子的最右位固定为 0 或 1，证明近似期望具有局部一致性。形式化地：

命题3.14。 APX_1 证明以下结论。设 $n, \delta^{-1} \in \mathsf{Log}$， $C\colon \{0,1\}^n \to \mathbb{Q}$, $V \subseteq \mathbb{Q}$ 为一个显式集合，满足 $\forall x \in \{0,1\}^n\ C(x) \in V$。设 X 为由(V, n, C)定义的随机变量。那么对于每个 $\beta^{-1} \in \mathsf{Log}$,

$$\left|\mathbb{E}_\delta[X] - \frac{\mathbb{E}_\delta[X|_0] + \mathbb{E}_\delta[X|_1]}{2}\right| \le (2\delta + \beta) \cdot \|V\|,$$

其中 $\|V\| \triangleq \sum_{v \in V} |v|$ 是 V的 ℓ_1 范数；对于 $b \in \{0,1\}$, $X|_b$ 表示由$(V, n-1, \mathsf{Fix}_b(C))$定义的随机变量。

证明。 我们在 APX_1中进行论证。设 $\eta^{-1} \in \mathsf{Log}$ 的取值稍后确定。回忆一下，$\mathsf{Fix}_b(C)$ 输出的是将 C 的最右侧输入位固定为 b后得到的电路，其中 $b \in \{0,1\}$。根据 Local ConsistencyAxiom，我们知道对于每个 $v \in V$,

$$\left|\mathsf{P}_\eta(C_v) - \frac{\mathsf{P}_\eta(\mathsf{Fix}(C_v, 0)) + \mathsf{P}_\eta(\mathsf{Fix}(C_v, 1))}{2}\right| \le 3\eta.$$

根据近似计数的定义，我们可以计算得出

$$\begin{aligned}
&\left|\mathbb{E}_\eta[X] - \frac{\mathbb{E}_\eta[X|_0] + \mathbb{E}_\eta[X|_1]}{2}\right| \\
&= \left|\sum_{v \in V} v \cdot \mathsf{P}_\eta(C_v) - \frac{1}{2}\left(\sum_{v \in V} v \cdot \mathsf{P}_\eta((\mathsf{Fix}_0(C))_v) + \sum_{v \in V} v \cdot \mathsf{P}_\eta((\mathsf{Fix}_1(C))_v)\right)\right| \\
&\le \left|\sum_{v \in V} v \cdot \mathsf{P}_\eta(C_v) - \frac{1}{2}\left(\sum_{v \in V} v \cdot \mathsf{P}_\eta(\mathsf{Fix}_0(C_v)) + \sum_{v \in V} v \cdot \mathsf{P}_\eta(\mathsf{Fix}_1(C_v))\right)\right| + 3\eta \cdot \|V\| \qquad \text{(全局一致性)} \\
&= \sum_{v \in V} |v| \cdot \left|\mathsf{P}_\eta(C_v) - \frac{\mathsf{P}_\eta(\mathsf{Fix}(C_v, 0)) + \mathsf{P}_\eta(\mathsf{Fix}(C_v, 1))}{2}\right| + 3\eta \cdot \|V\| \\
&\le 6\eta \cdot \|V\|.
\end{aligned}$$

该结果由期望的精度一致性 取 $\eta \triangleq \beta/10$即可得出。 □

支持扩展一致性。 设 X 是由元组(V, n, C)定义的随机变量。考虑满足 $V \subseteq V'$的显式集合 V'。通过考虑元组(V', n, C)，我们可以定义另一个随机变量 X'，它与 X 本质相同。下面的命题表明，X' 和 X 的期望几乎相同；也就是说，支撑扩张不会显著影响随机变量的期望。

命题3.15。 APX_1 证明了以下结论。设 n、 δ^{-1}、 $\beta^{-1} \in \mathsf{Log}$、 $C\colon \{0,1\}^n \to \mathbb{Q}$、 V、 $V' \subseteq \mathbb{Q}$是满足 $\forall x \in \{0,1\}^n\ C(x) \in V \subseteq V'$的显式集合。设 X 是由$(V$、 n、 $C)$定义的随机变量， X' 是由$(V'$、 n、 $C)$定义的随机变量。那么：

$$|\mathbb{E}_\delta[X] - \mathbb{E}_\delta[X']| \le (2\delta + \beta) \cdot \|V' \setminus V\| \le (2\delta + \beta) \cdot \|V'\|.$$

其中， $\|V' \setminus V\| = \sum_{v \in V' \setminus V} |v|$ 是 $V' \setminus V$的 ℓ_1-范数。

证明。 我们在 APX_1 中进行论证。根据近似期望的定义，我们知道 tha t

$$|\mathbb{E}_\delta[X] - \mathbb{E}_\delta[X']| = \left|\sum_{v \in V' \setminus V} v \cdot \mathsf{P}_\delta(C_v)\right| \le \sum_{v \in V' \setminus V} |v| \cdot \mathsf{P}_\delta(C_v), \tag{3.4}$$

其中，如果 $C(x) = v$，则 $C_v(x)$ 输出 1；否则输出 0。因此，只需证明对于 $v \in V' \setminus V$，$\mathsf{P}_\delta(C_v) \le 2\delta + \beta$。任取一个 $v \in V' \setminus V$。注意，由于对于 $x \in \{0,1\}^n$，$C(x) \in V$，我们知道 $C(x) \neq v$，因此 C_v（可证明地）与 Null_n 函数等价。利用近似计数的全局一致性，并根据 Boundary Axiom 得出 $\mathsf{P}_\delta(\mathsf{Null}_n) = 0$，即可得到所需的界。

□

置换对称性。 设 X，X' 是由元组 $(V,\ n,\ C)$ 和 $(V,\ n,\ C \circ \pi)$ 定义的随机变量，其中 $\pi \in S_n$ 表示输入位的一个置换。与近似计数的 置换对称性类似，我们将证明 $\mathbb{E}[X] \approx \mathbb{E}[X']$。

命题 3.16。 APX_1 证明以下陈述。设 $n, \delta^{-1}, \beta^{-1} \in \mathsf{Log}$、$C\colon \{0,1\}^n \to \mathbb{Q}$, $V \subseteq \mathbb{Q}$是一个显式集合，满足 $\forall x \in \{0,1\}^n\ C(x) \in V$。设 $\pi \in S_n$ 是输入位的一个置换。设 X, X'分别是由(V, n, C) 和$(V, n, C \circ \pi)$定义的随机变量。则：

$$|\mathbb{E}_\delta[X] - \mathbb{E}_\delta[X']| \le (2\delta + \beta) \cdot \|V\|,$$

其中 $\|V\|$ 是 V的 ℓ_1-范数。

证明。 我们在 APX_1 中进行论证。令 $\eta^{-1} \in \mathsf{Log}$，具体取值稍后确定。我们可以计算得

$$\begin{aligned}
|\mathbb{E}_\eta[X] - \mathbb{E}_\eta[X']| &\le \sum_{v \in V} |v| \cdot |\mathsf{P}_\eta(C_v) - \mathsf{P}_\eta((C \circ \pi)_v)| \\
&\le \sum_{v \in V} |v| \cdot |\mathsf{P}_\eta(C_v) - \mathsf{P}_\eta(C_v \circ \pi)| + 3\eta \cdot \|V\| \\
&\le 6\eta \cdot \|V\|.
\end{aligned}$$

这里，第二行由近似计数的全局一致性推出，第三行则由近似计数的置换对称性推出。随后，取期望的精度一致性即可得到该命题，令 $\eta \triangleq \beta/10$。

□

3.2.3 期望的平均论证

我们将证明一个更一般版本的平均论证，它允许我们搜索种子的一个后缀，使得在固定种子的某一部分之后，随机变量 $X_1, \ldots, X_m$ 的期望的给定线性组合近似保持不变。

假设 $X_1, \ldots, X_m$ 是由电路序列 $C_1, \ldots, C_m$ 定义、支撑集为 V 的随机变量，且每个电路的种子长度为 n，即对每个 $i \in [m]$ 和每个 $x \in \{0,1\}^n$，$C_i(x) \in V$。令 $\delta^{-1} \in \mathsf{Log}$。令$\lambda_1, \ldots, \lambda_m \in \mathbb{Q}$为系数，并考虑以下量

$$\mu_{n,m,\delta,\vec{\lambda}} \triangleq \lambda_1 \cdot \mathbb{E}_\delta[X_1] + \lambda_2 \cdot \mathbb{E}_\delta[X_2] + \cdots + \lambda_m \cdot \mathbb{E}_\delta[X_m]. \tag{3.5}$$

令 $z \in \{0,1\}^k$ 对于 $k \in [n]$。我们可以为每个来自 $(V,\ n-k,\ \mathsf{Fix}(C_i,\ z))$ 的 $i \in [m]$ 定义随机变量 $X_i|_z$，其中 $\mathsf{Fix}(C_i,\ z)$ 输出将 C_i 最右侧的 k 个比特固定为 z 后得到的电路。也就是说，$X_i|_z$ 是将 C_i 的最后 k 个输入位固定为 z 后得到的随机变量。[16] 令 $\mu_{n,\ m,\ \delta,\ \vec{\lambda}|z}$ 表示以下量

$$\mu_{n,m,\delta,\vec{\lambda}|z} \triangleq \lambda_1 \cdot \mathbb{E}_\delta[X_1|_z] + \lambda_2 \cdot \mathbb{E}_\delta[X_2|_z] + \cdots + \lambda_m \cdot \mathbb{E}_\delta[X_m|_z]. \tag{3.6}$$

定理 3.17 (期望的平均论证)。 APX_1 证明了以下陈述。令 n、m、$\delta^{-1} \in \mathsf{Log}$、$C_1$、……、$C_m$：$\{0,1\}^n \to \mathbb{Q}$ 为电路，$V \subseteq \mathbb{Q}$ 为一个显式集合，使得 $\forall x \in \{0,1\}^n\ \forall i \in [m]\ C_i(x) \in V$，并令 $\vec{\lambda} = (\lambda_1, \ldots\ldots, \lambda_m)$ 为一个长度为 m 的列表，使得 $\lambda_i \in \mathbb{Q}$ 对于 $i \in [m]$。

那么，对于每个 $k \in [n]$ 和 $\beta^{-1} \in \mathsf{Log}$，都存在一个 $z \in \{0,1\}^k$，使得

$$\mu_{n,m,\delta,\vec{\lambda}|z} \ge \mu_{n,m,\delta,\vec{\lambda}} - (2\delta + \beta) \cdot \|V\| \cdot \|\vec{\lambda}\|, \tag{3.7}$$

其中 $\|V\| \triangleq \sum_{v \in V} |v|$ 和 $\|\vec{\lambda}\| \triangleq \sum_{i \in [m]} |\lambda_i|$ 分别是 ℓ_1范数，适用于 V和 λ；而 $\mu_{n,\ m,\ \delta,\ \vec{\lambda}}$和$\mu_{n,\ m,\ \delta,\ \vec{\lambda}|z}$ 分别由方程 (3.5)和方程 (3.6)定义。

[16]根据 *Permutational Symmetry of Expectation*，不失一般性。

证明。 我们在 APX_1 中论证。设 $n, m, \delta^{-1} \in \mathsf{Log}$， $C_1, .., C_m$： $\{0,1\}^n \to \mathbb{Q}$，令 $V \subseteq \mathbb{Q}$ 为一个显式集合，$\vec{\lambda} = (\lambda_1, \ldots, \lambda_m) \in \mathbb{Q}$, $k \in [n]$, $\beta^{-1} \in \mathsf{Log}$。回想一下，根据定义，对于每个 $b \in \{0,1\}$，

$$\mu_{n,m,\eta,\vec{\lambda}}|_z = \lambda_1 \cdot \mathbb{E}_\delta[X_1|_z] + \cdots + \lambda_m \cdot \mathbb{E}_\delta[X_m|_z]; \tag{3.8}$$

$$\mu_{n,m,\eta,\vec{\lambda}}|_{z \circ b} = \lambda_1 \cdot \mathbb{E}_\delta[X_1|_{z \circ b}] + \cdots + \lambda_m \cdot \mathbb{E}_\delta[X_m|_{z \circ b}]. \tag{3.9}$$

我们将设计一个 P-预言机多项式时间算法 AvgSampler(π)，它接受

$$\pi \triangleq (1^n, 1^m, 1^{\delta^{-1}}, C_1, \ldots, C_m, V, \vec{\lambda}, 1^k, 1^{\beta^{-1}})$$

作为其输入并输出 $z \in \{0,1\}^k$ 使得方程（3.7）成立。定理 3.17 随之成立，如果AvgSampler(π)的正确性可在 APX_1中得到证明。

AvgSampler(π) 是关于 k （即 z 的长度）的迭代算法。我们将证明如下不变式：对任意 $k \in \{0, 1, \ldots, n\}$，算法 AvgSampler($\pi$) 输出一个字符串 $z \in \{0,1\}^k$，使得

$$\mu_{n,m,\eta,\vec{\lambda}}|_z \geq \mu_{n,m,\eta,\vec{\lambda}} - 3k \cdot \eta \cdot \|V\| \cdot \|\vec{\lambda}\| \tag{3.10}$$

其中 $\eta^{-1} \in \mathsf{Log}$。我们注意到，如果这是可能的，我们可以令 $\eta \triangleq \beta/(3n+3)$，使得方程（3.7）由期望的精度一致性推出。具体而言，我们可以看到

$$\begin{aligned}
&\left|\mu_{n,m,\eta,\vec{\lambda}}|_z - \mu_{n,m,\delta,\vec{\lambda}}|_z\right| \\
&= |\lambda_1 \cdot (\mathbb{E}_\eta[X_1|_z] - \mathbb{E}_\delta[X_1|_z]) + \cdots + \lambda_m \cdot (\mathbb{E}_\eta[X_m|_z] - \mathbb{E}_\delta[X_m|_z])| \\
&\leq |\lambda_1 \cdot (\delta + 2\eta) \cdot \|V\| + \cdots + \lambda_m \cdot (\delta + 2\eta) \cdot \|V\|| \leq (\delta + 2\eta) \cdot \|\vec{\lambda}\| \cdot \|V\|
\end{aligned}$$

并且类似地

$$\left|\mu_{n,m,\eta,\vec{\lambda}} - \mu_{n,m,\delta,\vec{\lambda}}\right| \leq (\delta + 2\eta) \cdot \|\vec{\lambda}\| \cdot \|V\|.$$

方程（3.7）随后由三角不等式得出。

对于 $k = 0$，AvgSampler(π) 输出 ε，并且方程（3.10）成立为 $\mu_{n,\ m,\ \vec{y},\ \eta,\ \vec{\lambda}}|_z = \mu_{n,\ m,\ \vec{y},\ \eta,\ \vec{\lambda}}$ （依定义）。假设它已经得到一个字符串 $z \in \{0,1\}^k$，使得方程（3.10）成立。我们的目标是选择一个比特 $b \in \{0,1\}$，使得

$$\mu_{n,m,\eta,\vec{\lambda}}|_{b \circ z} \geq \mu_{n,m,\eta,\vec{\lambda}} - 3(k+1) \cdot \eta \cdot \|V\| \cdot \|\vec{\lambda}\|.$$

对于每个 $i \in [m]$，根据期望的局部一致性可知

$$\left|\mathbb{E}_\eta[X_i|_z] - \frac{\mathbb{E}_\eta[X_i|_{0 \circ z}] + \mathbb{E}_\eta[X_i|_{1 \circ z}]}{2}\right| \leq 3\eta \cdot \|V\|$$

由此可得

$$\begin{aligned}
&\left|\mu_{n,m,\eta,\vec{\lambda}}|_z - \frac{\mu_{n,m,\eta,\vec{\lambda}}|_{0 \circ z} + \mu_{n,m,\eta,\vec{\lambda}}|_{1 \circ z}}{2}\right| \\
&= \left|\sum_{i \in [m]} \lambda_i \cdot \left(\mathbb{E}_\eta[X_i|_z] - \frac{\mathbb{E}_\eta[X_i|_{0 \circ z}] + \mathbb{E}_\eta[X_i|_{1 \circ z}]}{2}\right)\right| \leq 3\eta \cdot \|\vec{\lambda}\| \cdot \|V\|.
\end{aligned}$$

因此，对某个 $b \in \{0,1\}$，我们将有 $\mu_{n,\ m,\ \eta,\ \vec{\lambda}}|_{b \circ z} \geq \mu_{n,\ m,\ \eta,\ \vec{\lambda}}|_z - 3\eta \cdot \|\lambda\| \cdot \|V\|$，这进而意味着

$$\mu_{n,m,\eta,\vec{\lambda}}|_{b \circ z} \geq \mu_{n,m,\eta,\vec{\lambda}}|_z - 3\eta \cdot \|\vec{\lambda}\| \cdot \|V\| \geq \mu_{n,m,\eta,\vec{\lambda}} - 3(k+1) \cdot \eta \cdot \|\vec{\lambda}\| \cdot \|V\|.$$

算法 AvgSampler 可以使用 P-预言机来确定 b并输出 $b \circ z$。至此，证明完成。 □

3.2.4 补集

期望的 平均论证的一个简单推论是：互补计数。也就是说，如果 X是定义在 $\{0,1\}$ 上的随机变量，且 $X \triangleq 1-X$，那么 $\mathbb{E}[X] = 1 - \mathbb{E}[X]$。形式化地说：

推论 3.18 (互补计数)。 APX_1 证明了以下命题。设 $n, \delta^{-1}, \beta^{-1} \in \mathsf{Log}$,$C_1, C_2 \in B_n$，使得对于每个 $x \in \{0,1\}^n$, $C_1(x) \neq C_2(x)$。那么 $|\mathsf{P}_\delta(C_1) + \mathsf{P}_\delta(C_2) - 1| \leq 2\delta + \beta$。此外，设 X_1, X_2分别为 $\{0,1\}$ 上的 C_1, C_2 的指示随机变量。那么 $|\mathbb{E}_\delta[X_1] + \mathbb{E}_\delta[X_2] - 1| \leq 2\delta + \beta$。

证明。 我们在 APX_1 中进行论证。固定 $n, \delta^{-1}, \beta^{-1} \in \mathsf{Log}$, $C_1, C_2 \in B_n$。令 $\eta^{-1} \in \mathsf{Log}$ 稍后确定，并令X_1, X_2 为 C_1 和 C_2的指示随机变量。显然，对于种子的任意全赋值ρ， $\mathbb{E}_\eta[X_1|_\rho] + \mathbb{E}_\eta[X_2|_\rho] - 1 = 0$。因此，根据 期望的平均论证，取 $k = n$,$\mathbb{E}_\eta[X_1] + \mathbb{E}_\eta[X_2] - 1 \leq 6\eta$。类似地，我们可以证明 $-\mathbb{E}_\eta[X_1] - \mathbb{E}_\eta[X_2] + 1 \leq 6\eta$。这意味着

$$|\mathbb{E}_\eta[X_1] + \mathbb{E}_\eta[X_2] - 1| \leq 6\eta. \tag{3.11}$$

根据命题 3.12，我们有

$$|\mathsf{P}_\eta(C_1) + \mathsf{P}_\eta(C_2) - 1| \leq 12\eta.$$

随后，根据 Precision Consistency Axiom，我们有 $|\mathsf{P}_\delta(C_1) + \mathsf{P}_\delta(C_2) - 1| \leq 2\delta + 16\eta$。令 $\eta \triangleq \beta/30$, 即可得到所需的界。“此外”部分由方程（3.11）根据期望的精度一致性得出。

□

3.2.5 期望的线性性

现在我们可以证明期望的（近似）线性性，这是概率论中最有用的结果之一。设 $X_1, \ldots, X_m, Y$ 是显式集合 V 上的随机变量。对于这些随机变量的一个随机种子 z，我们用 $X_i|_z$ 和 $Y|_z$ 分别表示 X_i 和 Y 的求值结果。假设对于每个随机种子 z，都有

$$Y|_z = \gamma + \lambda_1 \cdot X_1|_z + \lambda_2 \cdot X_2|_z + \cdots + \lambda_m \cdot X_m|_z,$$

对于某些 $\lambda_1, \ldots, \lambda_m \in \mathbb{Q}$。那么我们应该能够得到， $\mathbb{E}[Y]$ 接近于

$$\gamma + \lambda_1 \cdot \mathbb{E}[X_1] + \lambda_2 \cdot \mathbb{E}[X_2] + \cdots + \lambda_m \cdot \mathbb{E}[X_m].$$

形式化地说：

定理 3.19 （期望的线性性）。 APX_1 证明如下：设 n、 m、 δ^{-1}、 $\beta^{-1} \in \mathsf{Log}$、 C_1、…、 C_m：$\{0,1\}^n \to \mathbb{Q}$ 为电路列表， $\lambda = (\lambda_1$、…、 $\lambda_m)$ 为长度为 m 的列表，使得对于 $i \in [m]$、 $\gamma \in \mathbb{Q}$， $\lambda_i \in \mathbb{Q}$，且设 $V \subseteq \mathbb{Q}$ 为一个显式集合，使得：

- *For any* $x \in \{0,1\}^n$ *and* $i \in [m]$, $C_i(x) \in V$.
- *For any* $x \in \{0,1\}^n$, $\gamma + \lambda_1 \cdot C_1(x) + \lambda_2 \cdot C_2(x) + \cdots + \lambda_m \cdot C_m(x) \in V$.

设 X_i 为由（V、 n、 C_i） 定义的随机变量，其中 $i \in [m]$; 设 Y为由（V、 n、 S）定义的随机变量，其中 S： $\{0,1\}^n \to \mathbb{Q}$ 是一个满足以下条件的电路

$$S(x) = \gamma + \lambda_1 \cdot C_1(x) + \lambda_2 \cdot C_2(x) + \cdots + \lambda_m \cdot C_m(x).$$

那么：

$$|\mathbb{E}_\delta[Y] - (\gamma + \lambda_1 \cdot \mathbb{E}_\delta[X_1] + \cdots + \lambda_m \cdot \mathbb{E}_\delta[X_m])| \leq (2\delta + \beta) \cdot \|V\| \cdot \|\vec{\lambda}\|, \tag{3.12}$$

其中， $\|V\|$ 和 $\|\lambda\|$ 分别是 V 和 λ的 ℓ_1-范数。

证明。我们在 $\mathbf{APX}_1$ 中进行论证。首先证明 $\mathbb{E}_\delta[Y]-(\gamma+\lambda_1\cdot\mathbb{E}_\delta[X_1]+\cdots+\lambda_m\cdot\mathbb{E}_\delta[X_m])\le(2\delta+\beta)\cdot\|V\|\cdot\|\lambda\|$。固定 $n,m,\delta^{-1},\beta^{-1}\in\mathsf{Log}$，$C_1,\ldots,C_m\colon\{0,1\}^n\to\mathbb{Q}$，$\vec{\lambda}$，$\gamma$ 和 V。令

$$\mu\triangleq 1\cdot\mathbb{E}_\delta[Y]+(-\lambda_1)\cdot\mathbb{E}_\delta[X_1]+\cdots+(-\lambda_m)\cdot\mathbb{E}_\delta[X_m],$$

对于每个 $z\in\{0,1\}^n$，我们将 $Y|_z$ 和 $X_i|_z$ 定义为种子长度为 0 的随机变量，如下所示

$$Y|_z\triangleq S(z),\quad X_i|_z\triangleq C_i(z),\quad (i\in[m]),\tag{3.13}$$

并将 $\mu|_z$ 定义为

$$\mu|_z\triangleq 1\cdot\mathbb{E}_\delta[Y|_z]+(-\lambda_1)\cdot\mathbb{E}_\delta[X_1|_z]+\cdots+(-\lambda_m)\cdot\mathbb{E}_\delta[X_m|_z].\tag{3.14}$$

根据期望的平均论证，存在一个字符串 $z\in\{0,1\}^n$ 使得 $\mu|_z\ge\mu-(2\delta+\beta)\cdot\|V\|\cdot\|\lambda\|$，这意味着 $\mu\le\mu|_z+(2\delta+\beta)\cdot\|V\|\cdot\|\lambda\|$。

注意，$\mathbb{E}_\delta[Y|_z]$ 定义为

$$\mathbb{E}_\delta[Y|_z]=\sum_{v\in V}v\cdot\mathsf{P}_\delta(S_v)=\sum_{v\in V}v\cdot\mathsf{Bool}(S_v)=S(z),$$

其中，S_v 是一个无输入电路，当且仅当 $S(z)=1$ 时输出 1。第二个等式由 Boundary Axiom 得出。类似地，我们可以证明，对于每个 $i\in[m]$，$\mathbb{E}_\delta[X_i|_z]=C_i(z)$。随后，$\mu|_z=S(z)-(\lambda_1\cdot C_1(z)+\cdots+\lambda_m\cdot C_m(z))=\gamma$，这进一步意味着 $\mu\le\gamma+(2\delta+\beta)\cdot\|V\|\cdot\|\vec{\lambda}\|$，即，

$$\mathbb{E}_\delta[Y]-(\gamma+\lambda_1\cdot\mathbb{E}_\delta[X_1]+\cdots+\lambda_m\cdot\mathbb{E}_\delta[X_m])\le(2\delta+\beta)\cdot\|V\|\cdot\|\vec{\lambda}\|.$$

最后，我们可以将相同的论证应用于由以下内容定义的 μ' 和 $\mu'|_z$

$$\mu'\triangleq(-1)\cdot\mathbb{E}_\delta[Y]+\lambda_1\cdot\mathbb{E}_\delta[X_1]+\cdots+\lambda_m\cdot\mathbb{E}_\delta[X_m]$$
$$\mu'|_z\triangleq(-1)\cdot\mathbb{E}[Y|_z]+\lambda_1\cdot\mathbb{E}[X_1|_z]+\cdots+\lambda_m\cdot\mathbb{E}[X_m|_z]$$

从而得出 $\mu=-\mu'\ge\gamma-(2\delta+\beta)\cdot\|V\|\cdot\|\vec{\lambda}\|$。证明完毕。 □

3.3 概率不等式

现在我们将介绍几个与（近似）概率和期望相关的标准不等式，包括并集界、马尔可夫不等式和切比雪夫不等式。

3.3.1 并集界

近似期望的平均论证（参见定理 3.17）的另一个应用是并集界。回顾一下，电路 C 的接受概率可以形式化为其指示随机变量 $I_C\in\{0,1\}$的期望。因此，并集界可以由以下原理推导出来：设 X_1、……、X_m、Y是布尔值随机变量，使得对于任意随机种子 z，$Y|_z=X_1|_z\vee X_2|_z\vee\cdots\vee X_m|_z$。那么，$\mathbb{E}[Y]$ 不应比 $\mathbb{E}[X_1]+\mathbb{E}[X_2]+\cdots+\mathbb{E}[X_m]$大很多。形式化地说：

定理 3.20（并集界）。$\mathbf{APX}_1$ 证明了以下陈述。设 $n,m,\delta^{-1},\beta^{-1}\in\mathsf{Log}$、$C_1$、…、$C_m\in B_n$ 是单输出电路，$V=\{0,1\}$。假设 $\forall x\in\{0,1\}^n$ 和 $i\in[m]$，$C_i(x)\in V$，并令$Y,X_1,\ldots,X_m$ 为如下定义的随机变量。

- 对每个 $i\in[m]$，X_i 定义为 (V,n,C_i)。
- Y定义为 (V,n,S)，其中 $S(x)\in\{0,1\}$ 是一个电路，满足 $S(x)\le C_1(x)\vee\cdots\vee C_m(x)$。

那么我们有 $\mathbb{E}_\delta[Y]\le\mathbb{E}_\delta[X_1]+\cdots+\mathbb{E}_\delta[X_m]+(2\delta+\beta)\cdot m$。

证明。 我们在 APX_1 中进行论证。固定 n，m，δ^{-1}，$\beta^{-1} \in \mathsf{Log}$、$C_1$、……、$C_m \in B_n$ 和 $V = \{0,1\}$。对于每个 $z \in \{0,1\}^n$，我们将 $Y|_z$ 定义为种子长度为 0 且输出 $S(z)$ 的随机变量，并将 X_i 定义为对于 $i \in [m]$，种子长度为 0 且输出 $C_i(z)$ 的随机变量。令 μ 和 $\mu|_z$ 定义为

$$\mu \triangleq 1 \cdot \mathbb{E}_\delta[Y] + (-1) \cdot \mathbb{E}_\delta[X_1] + \cdots + (-1) \cdot \mathbb{E}_\delta[X_m], \tag{3.15}$$

$$\mu|_z \triangleq 1 \cdot \mathbb{E}_\delta[Y|_z] + (-1) \cdot \mathbb{E}_\delta[X_1|_z] + \cdots + (-1) \cdot \mathbb{E}_\delta[X_m|_z]. \tag{3.16}$$

根据期望的平均论证，我们可以得出 $\mu \leq \mu|_z + (2\delta + \beta) \cdot m$ 对于某个字符串 z成立。接下来只需证明 $\mu|_z \leq 0$。类似于定理3.19的证明，我们可以通过Boundary Axiom 证明，对于 $\mathbb{E}_\delta[Y|_z] = S(z)$ 和 $\mathbb{E}_\delta[X_i|_z] = C_i(z)$，当 $i \in [m]$时成立。随后，根据 $\mu|_z$ 的定义以及关于 S 的假设，我们知道

$$\mu|_z = S(z) - (C_1(z) + \cdots + C_m(z)) \leq 0,$$

在 APX_1 中可证明。证明完毕。 □

3.3.2 马尔可夫不等式

接下来，我们讨论马尔可夫不等式。对于定义在显式集合 V 上的随机变量 X，我们应当能够证明：$X \geq k \cdot \mathbb{E}[X]$ 大于 $1/k$ 的程度不会太大。这可以自然地形式化如下：

定理3.21 (马尔可夫不等式)。 以下陈述在 APX_1 中可证明。设 X 是由 (V, n, C) 定义的随机变量，其中 V 是非负有理数的显式集合，$n \in \mathsf{Log}$，且C：$\{0,1\}^n \to \mathbb{Q}$ 是一个电路。设 $\delta^{-1}, \beta^{-1} \in \mathsf{Log}$，$\mu \in \mathbb{Q}$ 满足 $\mu \geq \mathbb{E}_\delta[X]$，且 $\mu > 0$，$k \in \mathbb{Q}$ 满足 $k > 0$，并且$T(x)$ 是一个电路：当 $C(x) \geq k \cdot \mu$ 时输出 1，否则输出 0。那么

$$\mathsf{P}_\delta(T) \leq \delta + k^{-1} \cdot (1 + \delta \cdot \mu^{-1} \cdot \|V\|) + \beta \cdot (\mu^{-1} \cdot \|V\| + 1),$$

其中 $\|V\|$ 是 V的 ℓ_1-范数。

证明。 我们在 APX_1中进行论证。固定 n，δ^{-1}，$\beta^{-1} \in \mathsf{Log}$，$C$：$\{0,1\}^n \to \mathbb{Q}$, μ，$k \in \mathbb{Q}$以及 V。令 $T(x)$ 为如上所定义的电路，并令 $m = |V|$。我们定义以下随机变量：

- Y是 $T(x)$的指示变量，即它定义为 $(\{0,1\}, n, T)$。
- 对于每个 $v \in V$，X_v 是 $\mathsf{EQ}(C(x), v)$的指示变量。形式上，令 $C_v(x)$ 为当且仅当 $C(x) = v$ 时输出 1、否则输出 0 的电路；X_v 是由 $(\{0,1\}, n, C_v)$ 定义的随机变量。

令 $\eta^{-1} \in \mathsf{Log}$ 为稍后确定的精度参数；对于 $b \in \{0,1\}$，令 $C_v^{(b)}(x) \in \{0,1\}$为当 $C(x) = b$ 时输出 1 的电路。根据近似期望的定义，我们有

$$\sum_{v \in V} v \cdot \mathbb{E}_\eta[X_v] = \sum_{v \in V} \sum_{b \in \{0,1\}} v \cdot b \cdot \mathsf{P}_\eta(C_v^{(b)}) = \sum_{v \in V} v \cdot \mathsf{P}_\eta(C_v^{(1)})$$

根据 $C_v(x)$和 $C_v^{(1)}(x)$的定义，我们知道 $C_v^{(1)}(x) = C_v(x)$，因此根据近似计数的 GlobalConsistency，我们有

$$|\mathsf{P}_\eta(C_v^{(1)}) - \mathsf{P}_\eta(C_v)| \leq 3 \cdot \eta.$$

接下来，我们可以从期望的精度一致性得知

$$\mu \geq \mathbb{E}_\delta[X] \geq \mathbb{E}_\eta[X] - (\delta + 2\eta) \cdot \|V\| \tag{3.17}$$
$$= \sum_{v \in V} v \cdot \mathsf{P}_\eta(C_v) - (\delta + 2\eta) \cdot \|V\| \tag{3.18}$$
$$\geq \sum_{v \in V} v \cdot \mathbb{E}_\eta[X_v] - (\delta + 5\eta) \cdot \|V\| \tag{3.19}$$
$$\geq k\mu \sum_{v \in V, v \geq k\mu} \mathbb{E}_\eta[X_v] - (\delta + 5\eta) \cdot \|V\|, \tag{3.20}$$

其中，最后一个不等式利用了 k、μ 和 V 均为非负数这一事实。这意味着

$$\sum_{v \in V, v \geq k \cdot \mu} \mathbb{E}_\eta[X_v] \leq k^{-1} \cdot (1 + (\delta + 5\eta) \cdot \mu^{-1} \cdot \|V\|). \tag{3.21}$$

下面我们还会用到以下不等式，它由命题 3.12 推得：

$$|\mathbb{E}_\eta[Y] - \mathsf{P}_\eta(T)| \leq 3 \cdot \eta. \tag{3.22}$$

从 $T(x)$ 和 $C_v(x)$ 的定义可以明显看出

$$T(x) = \bigvee_{v \in V, v \geq k \cdot \mu} C_v(x).$$

因此，根据 并集界，我们可以得出

$$\begin{aligned}
\mathsf{P}_\eta(T) &\leq \mathbb{E}_\eta[Y] + 3 \cdot \eta && \text{(Equation (3.22))} \\
&\leq \sum_{v \in V, v \geq k \cdot \mu} \mathbb{E}_\eta[X_v] + 3 \cdot \eta \cdot (m+1) && \text{(Union Bound)} \\
&\leq k^{-1} \cdot (1 + (\delta + 5\eta) \cdot \mu^{-1} \cdot \|V\|) + 3 \cdot \eta \cdot (|V| + 1), && \text{(Equation (3.21))}
\end{aligned}$$

最后，我们取 $\eta = \min\{\beta/(50(|V|+1)),\ \beta k/(50(|V|+1))\}$ 并应用 Precision Consistency Axiom，于是

$$\mathsf{P}_\delta(T) \leq \delta + \mathsf{P}_\eta(T) + 2\eta \leq \delta + k^{-1} \cdot (1 + \delta \cdot \mu^{-1} \cdot \|V\|) + \beta \cdot (\mu^{-1}\|V\| + 1).$$

证明至此完成。 □

3.3.3 方差与切比雪夫不等式

接下来，我们将建立（近似）方差的基本理论，并证明切比雪夫不等式的一种形式。

定义与基本性质。 设 X 是由元组 (V, n, C) 定义的随机变量，其中 $n \in$ 为 Log，V 是一个显式集合，且 $C: \{0,1\}^n \to \mathbb{Q}$。我们可以通过元组 (V^2, n, C^2) 定义随机变量 X^2，其中 $V^2 \triangleq \{v^2 \mid v \in V\}$ 且 $C^2(x) \triangleq (C(x))^2$。类似地，对于任意 $\mu \in \mathbb{Q}$，我们都可以通过元组 $(V - \mu, n, C_{-\mu})$ 定义随机变量 $X - \mu$，其中 $V - \mu \triangleq \{v - \mu \mid v \in V\}$ 且 $C_{-\mu}(x) \triangleq C(x) - \mu$。于是，我们可以定义：

定义 3.22（近似方差）。设 X 是由元组 (V, n, C) 定义的随机变量，其中 $\delta^{-1} \in \in$Log。X 在精度参数 δ 下的近似方差，记为 $\mathsf{Var}_\delta[X]$，定义为

$$\mathsf{Var}_\delta[X] \triangleq \mathbb{E}_\delta[(X - \mu)^2]$$

其中 $\mu \triangleq \mathbb{E}_\delta[X] \in \mathbb{Q}$。

举例来说，我们通过直接形式化 APX_1 中的标准证明，证明了近似方差的相等性 $\mathsf{Var}[X] = \mathbb{E}[X^2] - \mathbb{E}[X]^2$。

命题 3.23. APX_1 证明如下陈述。设 X 是由元组 (V, n, C) 定义的随机变量，其中 $V \subseteq \mathbb{Q}$ 是一个显式集合，$n \in \mathsf{Log}$，且 $C\colon \{0,1\}^n \to \mathbb{Q}$ 满足 $\forall x \in \{0,1\}^n\ C(x) \in V$。设 $\mu \triangleq \mathbb{E}_\delta[X] \in \mathbb{Q}$。则对任意 $\delta^{-1}, \beta^{-1} \in \mathsf{Log}$，

$$|\mathsf{Var}_\delta[X] - (\mathbb{E}_\delta[X^2] - \mu^2)| \le (2\delta + \beta) \cdot (1 + |\mu|) \cdot \|\hat{V}\|,$$

其中 $\hat{} V = V \cup (V - \mu)^2 \cup V^2 \cup \{1\}$。

证明. 我们在 APX_1 中论证。Fix $V \subseteq \mathbb{Q}, n, \delta^{-1}, \beta^{-1} \in \mathsf{Log}$，以及 $C\colon \{0,1\}^n \to \mathbb{Q}$。设 $\hat{} V = V \cup (V-\mu)^2 \cup V^2 \cup \{1\}$ 为一个显式集合，且 $\mu \triangleq \mathbb{E}_\delta[X]$。我们如下定义 $\hat{} V$ 上的随机变量 $\hat{} Y$、$\hat{} X$、$\hat{} X^2$：

- $\hat{} Y$ 是输出 $(X - \mu)^2$ 的随机变量。形式化地，设 $Y(x) \triangleq (C(x) - \mu)^2$ 是一个电路。我们可以证明，基于假设 $C(x) \in V$ 对任意 $x \in \{0,1\}^n$ 均成立，可得 $Y(x) \in V$。然后，我们通过元组 $Y(V, n, Y)$ 来定义。
- $\hat{} X$ 是输出 X 的随机变量。形式化地，它由元组 (V, n, C) 定义。
- $\hat{} X^2$ 是输出 X^2 的随机变量。形式化地，设 $C^2(x) \triangleq (C(x))^2$ 是一个电路。我们可以证明，基于假设 $C(x) \in V$ 对任意 $x \in \{0,1\}^n$ 均成立，可得 $C^2(x) \in \hat{} V$。然后，我们通过元组 $(\hat{} V, n, C^2)$ 来定义 $\hat{} X^2$。

令 $\eta^{-1} \in \mathsf{Log}$ 将在后文确定。根据电路 Y、C、C^2 的定义，显然 th at

$$Y(x) = \mu^2 + 1 \cdot C^2(x) + (-2\mu) \cdot C(x).$$

根据期望的线性性，我们可以看到

$$\left|\mathbb{E}_\eta[\hat{Y}] - (\mu^2 + \mathbb{E}_\eta[\hat{X}^2] - 2\mu \cdot \mathbb{E}_\eta[\hat{X}])\right| \le 6\eta \cdot \|\hat{V}\| \cdot (|\mu| + 1). \tag{3.23}$$

根据支持扩展一致性，我们还可以得出

$$\left|\mathbb{E}_\eta[\hat{Y}] - \mathbb{E}_\eta[(X-\mu)^2]\right|, \left|\mathbb{E}_\eta[\hat{X}^2] - \mathbb{E}_\eta[X^2]\right|, \left|\mathbb{E}_\eta[\hat{X}] - \mathbb{E}_\eta[X]\right| \le 3\eta \cdot \|\hat{V}\|. \tag{3.24}$$

根据三角不等式和期望的精度一致性，我们有

$$\begin{aligned}
&|\mathsf{Var}_\delta[X] - (\mathbb{E}_\delta[X^2] - \mu^2)| \\
&= |\mathbb{E}_\delta[(X-\mu)^2] - (\mathbb{E}_\delta[X^2] - \mu^2)| \\
&\le |\mathbb{E}_\eta[(X-\mu)^2] - (\mathbb{E}_\eta[X^2] - \mu^2)| + 2 \cdot (\delta + 2\eta) \cdot \|\hat{V}\| && \text{(Proposition 3.13)} \\
&\le |\mathbb{E}_\eta[\hat{Y}] - \mathbb{E}_\eta[\hat{X}^2] + \mu^2| + (2\delta + 10\eta) \cdot \|\hat{V}\| && \text{(Equation (3.24))} \\
&\le |\mu^2 - (2\mu \cdot \mathbb{E}_\eta[\hat{X}] - \mu^2)| + (2\delta + 10\eta) \cdot \|\hat{V}\| + 6\eta \cdot \|\hat{V}\| \cdot (|\mu| + 1) && \text{(Equation (3.23))} \\
&\le |\mu^2 - (2\mu \cdot \mathbb{E}_\eta[X] - \mu^2)| + (2\delta + 10\eta) \cdot \|\hat{V}\| + 6\eta \cdot \|\hat{V}\| \cdot (|\mu| + 1) + 6\eta \cdot |\mu| \cdot \|\hat{V}\| && \text{(Equation (3.24))} \\
&\le |\mu^2 - (2\mu \cdot \mathbb{E}_\delta[X] - \mu^2)| + (2\delta + 10\eta) \cdot \|\hat{V}\| + 6\eta \cdot \|\hat{V}\| \cdot (|\mu| + 1) \\
&\qquad + 6\eta \cdot |\mu| \cdot \|\hat{V}\| + 2|\mu| \cdot (\delta + 2\eta) \cdot \|\hat{V}\| && \text{(Proposition 3.13)} \\
&\le (2\delta + 10\eta) \cdot \|\hat{V}\| + 6\eta \cdot \|\hat{V}\| \cdot (|\mu| + 1) + 6\eta \cdot |\mu| \cdot \|\hat{V}\| + 2|\mu| \cdot (\delta + 2\eta) \cdot \|\hat{V}\|. && (\mu \triangleq \mathbb{E}_\delta[X])
\end{aligned}$$

取 $\eta = \beta/40$ 即可得出该定理。 □

切比雪夫不等式。现在我们证明切比雪夫不等式的一种形式，它为已知（近似）方差的随机变量提供尾界。形式化地说：

定理*3.24*（切比雪夫不等式）。*APX*$_1$ 证明以下命题。设 X 是由元组 (V, n, C) 、 $\delta^{-1} \in$*Log*定义的随机变量，其中 $V \subseteq \mathbb{Q}$ 是显式集合， $n \in$*Log*，且 C： $\{0,1\}^n \to \mathbb{Q}$ 是一个电路，满足 $\forall x \in \{0,1\}^n$ *C(x)* $\in V$。设 $\mu \triangleq \mathbb{E}_\delta[X] \in \mathbb{Q}$, $\sigma^2 \triangleq$ *Var*$_\delta[X]$，并设 *T(x)*是这样一个电路：当 $(C(x) - \mu)^2 \geq k \cdot \sigma^2$时输出*1*，否则输出*0*。

那么对于任意的 $\beta^{-1} \in \mathsf{Log}$ 和 $k \in \mathbb{Q}$，其中 $k > 0$，我们有

$$\mathsf{P}_\delta(T) \leq \delta + k^{-1} \cdot (1 + \delta \cdot \sigma^{-2} \cdot \|\hat{V}\|) + \beta \cdot (\sigma^{-2} \cdot \|\hat{V}\| + 1),$$

其中 $\hat{}V = (V - \mu)^2 = \{(v - \mu)^2 \mid v \in V\}$。

证明。 我们在 APX_1 中进行论证。固定 V， n， δ^{-1}， β^{-1}， C： $\{0,1\}^n \to \mathbb{Q}$， $\mu \triangleq \mathbb{E}_\delta[X]$， $\sigma^2 \triangleq \mathsf{Var}_\delta[X]$， β^{-1}， k。令 Y为由元组 $(\hat{}V$， n， $S)$ 定义的随机变量，其中 $S(x) \triangleq (C(x) - \mu)^2$。根据近似方差的定义，我们知道

$$\sigma^2 = \mathsf{Var}_\delta[X] = \mathbb{E}_\delta[(X - \mu)^2] = \mathbb{E}_\delta[Y].$$

通过应用 马尔可夫不等式 于随机变量 Y，我们可以看出

$$\mathsf{P}_\delta(T) \leq \delta + k^{-1} \cdot (1 + \delta \cdot \sigma^{-2} \cdot \|\hat{V}\|) + \beta \cdot (\sigma^{-2} \cdot \|\hat{V}\| + 1).$$

证明至此完成。 □

3.3.4 两两独立性和方差

现在我们建立（几乎）两两独立性的概念，并证明相等性 $\mathsf{Var}[X_1 + \cdots + X_m] = \mathsf{Var}[X_1] + \cdots + \mathsf{Var}[X_m]$ 对于两两独立的随机变量 X_1，……， X_m。这与切比雪夫不等式相结合，构成降低随机化算法错误概率的一种标准技术。

（几乎）独立性的定义。 我们从随机变量的（几乎）独立性定义开始。设 X_1， X_2 分别为取值于 V_1， V_2 的随机变量。回顾 X 与 Y 的协方差，记为 $\mathsf{Cov}(X, Y)$，定义为量 $\mathbb{E}[X \cdot Y] - \mathbb{E}[X] \cdot \mathbb{E}[Y]$，其中 $X \cdot Y$ 是取值于 $V_1 V_2 \triangleq \{v_1 \cdot v_2 \mid v_1 \in V_1, v_2 \in V_2\}$ 的随机变量。形式地说：

定义 3.25（协方差）。设 X_1 与 X_2 分别为由元组 (V_1, n, C_1) 和 (V_2, n, C_2) 定义的随机变量，其中 V_1、$V_2 \subseteq \mathbb{Q}$ 为显式集合， $n \in \mathsf{Log}$，并且 C_1、 C_2： $\{0,1\}^n \to \mathbb{Q}$ 为电路。设 $\delta^{-1} \in \mathsf{Log}$, $V_1 V_2 \triangleq \{v_1 \cdot v_2 \mid v_1 \in V_1, v_2 \in V_2\}$、 $Y(x)$ 为计算 $C_1(x) \cdot C_2(x)$ 的电路，且 Y 为由元组 $(V_1 V_2, n, Y)$ 定义的随机变量。 X_1 与 X_2 的 δ-近似协方差，记为 $\mathsf{Cov}_\delta(X_1, X_2)$，定义为

$$\mathsf{Cov}_\delta(X_1, X_2) \triangleq |\mathbb{E}_\delta[Y] - \mathbb{E}_\delta[X_1] \cdot \mathbb{E}_\delta[X_2]|.$$

定义 3.26 （几乎独立性）。 令 $\delta^{-1} \in \mathsf{Log}$、 $\varepsilon \in \mathbb{Q}$。若随机变量 X_1 和 X_2 满足 $\mathsf{Cov}_\delta(X_1, X_2) \leq \varepsilon$，则称它们是 ε-几乎 δ-近似独立的。

接下来，我们可以定义随机变量序列的两两独立性。

定义 3.27（两两独立性）。令 n、 $m \in \mathsf{Log}$、 C_1、…、 C_m： $\{0,1\}^n \to \mathbb{Q}$ 为电路， $V \subseteq \mathbb{Q}$为一个显式集合，使得 $\forall i \in [m]\, \forall x \in \{0,1\}^n\ C_i(x) \in V$。令 X_1、…、 X_m 为随机变量，其中对于每个 $i \in [m]$， X_i 由元组（V、 n、 C_i）定义，并令 $\delta^{-1} \in \mathsf{Log}$ 且 $\varepsilon \in \mathbb{Q}$。若对于每一对（$i$， j），其中i、 $j \in [m]$ 且 $i \neq j$、 X_i， X_j 和 ε是 ε-几乎 δ-近似独立的，则称随机变量序列 X_1、…、 X_m是 ε-几乎 δ-近似两两独立的。

我们可以省略参数 ε，直接称其为 δ近似独立（如果 $\varepsilon = 0$）。请注意，由于随机变量的近似期望可能会产生错误，即使 $\varepsilon = 0$，随机变量 X_1 和 X_2 也可能并非完全独立。

两两独立变量之和。 现在我们准备证明以下结果：假设 X_1、……、 X_m 几乎两两独立，且 $Y = X_1 + \cdots + X_m$。 那么， Y的方差接近 X_1、 X_2、……、 X_m的方差之和。形式化地说：

定理 3.28. 以下陈述可在APX_1中证明。设 n、 $m \in \mathsf{Log}$、 C_1、……、 C_m： $\{0,1\}^n \to \mathbb{Q}$为电路，且 $V \subseteq \mathbb{Q}$ 为显式集合，使得以下成立：

- $\forall i \in [m]\ \forall x \in \{0,1\}^n\ C_i(x) \in V$;
- $\forall x \in \{0,1\}^n\ C_1(x) + C_2(x) + \cdots + C_m(x) \in V$。

设 X_1，……， X_m 为随机变量，其中对每个 $i \in [m]$， X_i 由元组(V, n, C_i)定义。设 Y为由元组(V, n, S)定义的随机变量，其中 $S(x)$ 是计算 $C_1(x) + C_2(x) +$的电路 $\cdots + C_m(x)$。设 δ^{-1}、 $\beta^{-1} \in \mathsf{Log}$与 $\varepsilon \in \mathbb{Q}$。假设 X_1，……， X_m 是 ε-几乎 δ-近似两两独立的。则

$$|\mathsf{Var}_\delta[Y] - (\mathsf{Var}_\delta[X_1] + \cdots + \mathsf{Var}_\delta[X_m])| \leq (\varepsilon + 3\delta \cdot \|V\|^2) \cdot m^2 + \beta \cdot (\|V\| + 1)^3,$$

其中， $\|V\| = \sum_{v \in V} |v|$ 是 V的 ℓ_1-范数。

证明。 我们论证 $\mathbf{APX}_1$。固定 n， m、电路 C_1、. . 、 $C_m \in \{0,1\}^n \to \mathbb{Q}$、 V、 δ^{-1}、 ε^{-1}、 β^{-1}。令 $\eta^{-1} \in \mathsf{Log}$ 为稍后确定的精度参数， $\mu \triangleq \mathbb{E}_\eta[Y]$，并且对于 $i \in [m]$， $\mu_i \triangleq \mathbb{E}_\eta[X_i]$ 。

证明概述。 回顾命题3.23，我们有

$$\left|\mathsf{Var}_\eta[Y] - (\mathbb{E}_\eta[Y^2] - \mu^2)\right| \leq 3\eta \cdot (1 + |\mu|) \cdot \|\hat{V}_Y\|, \tag{3.25}$$

其中 ˆ $V_Y = V \cup (V - \mu)^2 \cup V^2 \cup \{1\}$。类似地，对于每个 $i \in [m]$，我们有

$$\left|\mathsf{Var}_\eta[X_i] - (\mathbb{E}_\eta[X_i^2] - \mu_i^2)\right| \leq 3\eta \cdot (1 + |\mu_i|) \cdot \|\hat{V}_i\|, \tag{3.26}$$

其中 ˆ $V_i = V \cup (V - \mu_i)^2 \cup V^2 \cup \{1\}$。因此，只需对以下量进行界定

$$\Delta \triangleq |\mathbb{E}_\eta[Y^2] - (\mathbb{E}_\eta[X_1^2] + \cdots + \mathbb{E}_\eta[X_m^2]) - \mu^2 + (\mu_1^2 + \ldots \mu_m^2)| \tag{3.27}$$

并将其与方程（3.25）和（3.26）结合起来。从整体上看，我们的计划是应用期望的线性性来证明 $\mathbb{E}_\eta[Y^2]$ 接近于

$$\sum_{i=1}^m \mathbb{E}_\eta[X_i^2] + \sum_{i,j \in [m], i \neq j} \mathbb{E}_\eta[X_i X_j], \tag{3.28}$$

而后者又接近于

$$\sum_{i=1}^m \mathbb{E}_\eta[X_i^2] + \sum_{i,j \in [m], i \neq j} \mu_i \mu_j$$

根据 X_1、……、 X_m的近似两两独立性。最后，我们可以应用期望的线性性来证明

$$\mu_1^2 + \cdots + \mu_m^2 + \sum_{i,j \in [m], i \neq j} \mu_i \mu_j = \left(\sum_{i=1}^m \mu_i\right)^2 \approx \mu^2.$$

将这些估计结合起来，即可得到 Δ 的上界。

步骤 1：近似 $\mathbb{E}_\eta[Y^2]$。我们首先证明 $\mathbb{E}_\eta[Y^2]$ 接近方程（3.28）。回忆一下Y^2，X^2，以及 X_iX_j 是定义在 V^2 上的随机变量，其定义如下：

- Y^2 由元组 (V^2, n, S^2) 定义，其中 $S^2(x) \triangleq (S(x))^2$。
- 对于 $i \in [m]$，X_i^2由元组 (V^2, n, C_i^2) 定义，其中 $C_i^2(x) \triangleq (C_i(x))^2$。
- 对于 $i, j \in [m]$ 满足 $i \neq j$ 的情形，X_iX_j 由元组 (V^2, n, C_{ij}) 定义，其中 $C_{ij}(x) \triangleq C_i(x) \cdot C_j(x)$。

根据各项的定义显然，对于任意 $z \in \{0,1\}^n$，都有

$$S^2(z) = \sum_{i=1}^{m} C_i^2(z) + \sum_{i,j\in[m],i\neq j} C_{ij}(z).$$

因此，根据期望的线性性，我们有

$$\left| \mathbb{E}_\eta[Y^2] - \left(\sum_{i=1}^{m} \mathbb{E}_\eta[X_i^2] + \sum_{i,j\in[m],i\neq j} \mathbb{E}_\eta[X_iX_j] \right) \right| \leq 3\eta \cdot \|V^2\| \cdot (m^2+m+1) \leq 9\eta \cdot m^2 \cdot \|V^2\|. \tag{3.29}$$

步骤 2：应用两两独立性。在此步骤中，我们证明 $\mathbb{E}_\eta[X_iX_j]$ 接近于 $\mu_i\mu_j$ 对于任意$i, j \in [m]$。回顾一下，$\mu_i \triangleq \mathbb{E}_\eta[X_i]$。根据期望的精度一致性，我们有

$$|\mathbb{E}_\eta[X_iX_j] - \mathbb{E}_\delta[X_iX_j]| \leq (\delta + 2\eta) \cdot \|V^2\|$$

对于任意 i，$j \in [m]$、$i \neq j$。此外，由于 X_1、.....、X_m 是 ε-几乎 δ-近似两两独立的，我们知道

$$|\mathbb{E}_\delta[X_iX_j] - \mathbb{E}_\delta[X_i] \cdot \mathbb{E}_\delta[X_j]| \leq \varepsilon.$$

对于每个 $i \in [m]$，我们都有 $|\mathbb{E}_\delta[X_i] - \mathbb{E}_\eta[X_i]| \leq (\delta + 2\eta) \cdot \|V\|$，这意味着 t

$$\begin{aligned}
&|\mathbb{E}_\delta[X_i] \cdot \mathbb{E}_\delta[X_j] - \mathbb{E}_\eta[X_i] \cdot \mathbb{E}_\eta[X_j]| \\
\leq &|\mathbb{E}_\delta[X_i] \cdot \mathbb{E}_\delta[X_j] - \mathbb{E}_\eta[X_i] \cdot \mathbb{E}_\delta[X_j]| + |\mathbb{E}_\eta[X_i] \cdot \mathbb{E}_\delta[X_j] - \mathbb{E}_\eta[X_i] \cdot \mathbb{E}_\eta[X_j]| \\
\leq &(\delta + 2\eta) \cdot \|V\| \cdot (|\mathbb{E}_\eta[X_i]| + |\mathbb{E}_\delta[X_j]|) \leq 2(\delta + 2\eta) \cdot \|V\|^2.
\end{aligned}$$

结合上述方程，我们得到

$$|\mathbb{E}_\eta[X_iX_j] - \mu_i\mu_j| \leq \varepsilon + (\delta + 2\eta) \cdot \|V^2\| + 2(\delta + 2\eta) \cdot \|V\|^2 \leq \varepsilon + 3(\delta + 2\eta)\|V\|^2. \tag{3.30}$$

步骤 3：应用期望的线性性。最后一步是证明 $\mu \approx \mu_1 + \cdots + \mu_m$。回顾 $\mu \triangleq \mathbb{E}_\eta[Y]$ 和 $\mu_i \triangleq \mathbb{E}_\eta[X_i]$，其中 Y由元组 $(V,\ n,\ S)$ 定义，而 X_i 由元组 $(V,\ n,\ C_i)$ 定义。根据 S和 C_i 的定义，很明显，对于任意 $z \in \{0,1\}^n$，

$$S(z) = C_1(z) + C_2(z) + \cdots + C_m(z).$$

因此，根据期望的线性性，我们有

$$|\mu - (\mu_1 + \cdots + \mu_m)| = |\mathbb{E}_\eta[Y] - (\mathbb{E}_\eta[X_1] + \cdots + \mathbb{E}_\eta[X_m])| \leq 3\eta \cdot \|V\| \cdot (m+1). \tag{3.31}$$

接下来，我们可以看到

$$\begin{aligned}
\left|\mu^2 - (\mu_1 + \cdots + \mu_m)^2\right| &= |\mu + (\mu_1 + \cdots + \mu_m)| \cdot |\mu - (\mu_1 + \cdots + \mu_m)| \\
&\leq (2|\mu| + 3\eta \cdot \|V\| \cdot (m+1)) \cdot 3\eta \cdot \|V\| \cdot (m+1) \\
&\leq 6|\mu| \cdot \eta \cdot 2m \cdot \|V\| + 9\eta^2 \cdot (2m)^2 \cdot \|V\|^2 \\
&\leq 4 \cdot (9\eta^2 + 6\eta) \cdot m^2 \cdot \|V\|^2 \qquad \text{(since } |u| \leq \|V\|\text{)} \\
&\leq 60 \cdot \eta \cdot (m\|V\|)^2, \qquad (3.32)
\end{aligned}$$

其中，最后一个不等式成立，是因为我们将取 $\eta \leq 1$。

总结一下。结合方程（3.29）、（3.30）和（3.32），我们可以看出 t hat

$$
\begin{aligned}
\Delta &= |\mathbb{E}_\eta[Y^2] - (\mathbb{E}_\eta[X_1^2] + \cdots + \mathbb{E}_\eta[X_m^2]) - \mu^2 + (\mu_1^2 + \ldots \mu_m^2)| \\
&\le \left| \sum_{i,j\in[m], i\neq j} \mathbb{E}_\eta[X_i X_j] - \mu^2 + \sum_{i=1}^m \mu_i^2 \right| + 9\eta \cdot m^2 \cdot \|V\|^2 && \text{(Equation (3.29))} \\
&\le \left| \sum_{i,j\in[m], i\neq j} \mu_i \mu_j - \mu^2 + \sum_{i=1}^m \mu_i^2 \right| + 9\eta \cdot m^2 \cdot \|V\|^2 + m^2(\varepsilon + 3(\delta + 2\eta) \cdot \|V\|^2) && \text{(Equation (3.30))} \\
&\le \left| -\mu^2 + \left(\sum_{i=1}^m \mu_i \right)^2 \right| + (\varepsilon + 3\delta \cdot \|V\|^2) \cdot m^2 + 20 \cdot \eta \cdot (m\|V\|)^2 \\
&\le 60 \cdot \eta \cdot (m\|V\|)^2 + (\varepsilon + 3\delta \cdot \|V\|^2) \cdot m^2 + 20 \cdot \eta \cdot (m\|V\|)^2 && \text{(Equation (3.32))} \\
&\le (\varepsilon + 3\delta \cdot \|V\|^2) \cdot m^2 + 80 \cdot \eta \cdot (m\|V\|)^2.
\end{aligned}
$$

最后，我们将此与方程（3.25）和（3.26）相结合，从而得到

$$
|\mathsf{Var}_\delta[Y] - (\mathsf{Var}_\delta[X_1] + \cdots + \mathsf{Var}_\delta[X_m])| \le \Delta + 3\eta \cdot (1 + |\mu|) \cdot \|\hat{V}_Y\| + 3\eta \cdot \sum_{i=1}^m (1 + |\mu_i|) \cdot \|\hat{V}_i\|. \tag{3.33}
$$

注意

$$
\begin{aligned}
|\mu| \le \|\hat{V}_Y\| &\le \|V\| + \|(V - \mu)^2\| + \|V^2\| + 1 \\
&\le \|V\| + \|V\|^2 + 1 + \sum_{v\in V} (v - \mu)^2 \\
&\le \|V\| + \|V\|^2 + 1 + \|V\|^2 + |V| \cdot \mu^2 + 2\mu \cdot \|V\|^2 \\
&\le 2 \cdot \|V\|^3 + (|V| + 2) \cdot \|V\|^2 + \|V\| + 1 = 8 \cdot |V| \cdot (\|V\| + 1)^3.
\end{aligned}
$$

类似地，我们有 $|\mu_i| \le \|\hat{V}_i\| \le 8 \cdot |V| \cdot (\|V\| + 1)^3$。

令 $\eta \triangleq \min\{\beta/(2000 \cdot m^2 \cdot |V|)\ 1/10\} \le 1$。将方程（3.33）与上述上界相结合，我们有

$$
\begin{aligned}
&|\mathsf{Var}_\delta[Y] - (\mathsf{Var}_\delta[X_1] + \cdots + \mathsf{Var}_\delta[X_m])| \\
&\le (\varepsilon + 3\delta \cdot \|V\|^2) \cdot m^2 + 80 \cdot \eta \cdot (m\|V\|)^2 + 1000 \cdot m \cdot \eta \cdot |V| \cdot (\|V\| + 1)^3 \\
&\le (\varepsilon + 3\delta \cdot \|V\|^2) \cdot m^2 + \beta \cdot (\|V\| + 1)^3.
\end{aligned}
$$

这就完成了证明。 □

3.4 独立性、错误归约与集中性界 s

我们现在考虑独立同分布随机变量的集中界在 $\mathbf{APX}_1$ 中的可证明性，这些集中界是组合学、概率以及随机化算法分析中的重要工具。

3.4.1 显式独立性

在陈述并证明集中界之前，我们先正式定义独立同分布随机变量的表述方式，并证明近似计数的乘法原理的一种形式。

独立同分布随机变量的形式化。 我们只考虑“显式”独立同分布的随机变量，即由相同的采样算法使用随机种子中互不重叠的部分来定义的随机变量。这足以满足我们的应用需求，并大大简化近似计数中参数的计算。我们首先将随机变量的显式独立性正式定义如下：

定义 3.29 (显式独立性)。 设 X 和 X' 分别是由 (V, n, C) 和 (V, n, C') 定义的随机变量。若 C 和 C' 读取 n 比特种子中互不相交的比特，则称 X 和 X' 是显式独立的；也就是说，存在 $[n]$ 的一个划分 $\pi_1 \cup \pi_2$，使得对于任意种子 $x \in \{0,1\}^n$， C 只读取 x_{π_1}，而 C' 只读取 x_{π_2}，其中 x_π 表示 x 中索引属于 π 的比特。

类似地，我们定义显式独立同分布随机变量如下：

定义 3.30 (显式独立同分布随机变量)。 设 $n, m \in \mathsf{Log}$，$C\colon \{0,1\}^n \to \mathbb{Q}$ 是一个电路， $V \subseteq \mathbb{Q}$ 是一个显式集合，且 $\forall x \in \{0,1\}^n\ C(x) \in V$。由元组 (V, n, C) 定义的显式独立同分布随机变量 $X_1, \ldots, X_m$ 如下获得。

令 $C_i(\cdot)\colon \{0,1\}^{nm} \to V$ 为满足以下条件的电路：对于任意 $\overline{x} = x_1 \circ x_2 \circ \cdots \circ x_m \in \{0,1\}^n$，其中 $x_i \in \{0,1\}^n$ 对每个 $i \in [m]$， $C_i(x) \triangleq C(x_i)$。对于每个 $i \in [m]$，随机变量 X_i 由元组 $(V,\ nm,\ C_i)$ 定义。

3.4.2 乘法原理

我们需要乘法原理的一种形式：对于任意显式独立随机变量 X 和Y，有 $\mathbb{E}[XY] \approx \mathbb{E}[X] \cdot \mathbb{E}[Y]$，或者等价地，$\mathsf{Cov}(X,\ Y)$ 很小。换句话说，显式独立随机变量近似独立。形式化地说：

定理 3.31 （乘法原理）。 APX_1 证明了以下命题。设 n、$\delta^{-1} \in \mathsf{Log}$、 V_1、V_2为显式集合， C_1、$C_2 \in \{0,1\}^n \to \mathbb{Q}$ 为电路。假设由元组 $(V_1,\ n,\ C_1)$ 和 $(V_2,\ n,\ C_2)$ 分别定义的随机变量 X_1 和 X_2是显式独立的。那么对于任意 $\beta^{-1} \in \mathsf{Log}$,

$$\mathsf{Cov}_\delta(X, Y) = |\mathbb{E}_\delta[X_1 X_2] - \mathbb{E}_\delta[X_1] \cdot \mathbb{E}_\delta[X_2]| \le (2\delta + \beta) \cdot \|\hat{V}\| + (4\delta + \beta) \cdot \|\hat{V}\|^2,$$

其中 $\hat{V} \triangleq V_1 \cup V_2 \cup V_1 V_2$，且 $V_1 V_2 \triangleq \{v_1 v_2 \mid v_1 \in V_1, v_2 \in V_2\}$。

证明。 我们在 APX_1 中进行论证。固定 $n,\ \delta^{-1} \in \mathsf{Log}$、 $V_1,\ V_2,\ C_1,\ C_2$，以及 $\beta^{-1} \in \mathsf{Log}$。令 $\eta^{-1} \in \mathsf{Log}$ 在稍后确定，并令 $\hat{V} \triangleq V_1 \cup V_2 \cup V_1 V_2$ 为一个显式集合。

证明概述。 证明的大致思路如下。令 $\pi_1 \cup \pi_2$ 为 $[n]$ 的一个划分，使得对于任意种子 $x \in \{0,1\}^n$， X_1 只读取 x_{π_1}，而 X_2 只读取 x_{π_2}。反设$|\mathbb{E}[X_1 X_2] - \mathbb{E}[X_1] \cdot \mathbb{E}[X_2]|$ 很大。根据 期望的平均论证，我们可以找到一个赋值ρ_1，赋给种子的部分 x_{π_1}，使得

$$|\mathbb{E}[X_1 X_2|_{\rho_1}] - \mathbb{E}[X_1|_{\rho_1}] \cdot \mathbb{E}[X_2]|$$

很大。更正式地说，我们通过将 期望的平均论证 应用于：把 $X_1 X_2$ 和 X_1 分别视为系数为 1 和 $-\mathbb{E}[X_2]$ 的随机变量。注意，由于 X_2 没有读取种子的这部分x_{π_1}，我们知道 $\mathbb{E}[X_2]$接近 $\mathbb{E}[X_2|_{\rho_1}]$，因此

$$|\mathbb{E}[X_1 X_2|_{\rho_1}] - \mathbb{E}[X_1|_{\rho_1}] \cdot \mathbb{E}[X_2|_{\rho_1}]|$$

也很大。

接下来，我们再次应用期望的平均论证，将 $X_1 X_2|_{\rho_1}$ 和 $X_2|_{\rho_1}$ 分别视为系数为 1 和 $-\mathbb{E}[X_1|_{\rho_1}]$的随机变量，并使用种子 x_{π_2}。由此可得一个赋值 ρ_2，使得x_{π_2} 满足

$$|\mathbb{E}[X_1 X_2|_{\rho_1}|_{\rho_2}] - \mathbb{E}[X_1|_{\rho_1}] \cdot \mathbb{E}[X_2|_{\rho_1}|_{\rho_2}]|\,.$$

很大。注意，再次由于 X_1 不读取种子中的部分 x_{π_2}，我们知道 $\mathbb{E}[X_1|_{\rho_1}]$ 接近$\mathbb{E}[X_1|_{\rho_1}|_{\rho_2}]$，进而

$$|\mathbb{E}[X_1X_2|_{\rho_1}|_{\rho_2}] - \mathbb{E}[X_1|_{\rho_1}|_{\rho_2}] \cdot \mathbb{E}[X_2|_{\rho_1}|_{\rho_2}]| .$$

也很大。然而，这是不可能的，因为 $X_1X_2|_{\rho_1}|_{\rho_2}$、$X_1|_{\rho_1}|_{\rho_2}$ 和 $X_2|_{\rho_1}|_{\rho_2}$ 是种子长度为 0 的随机变量，按定义应满足 $X_1X_2|_{\rho_1}|_{\rho_2} = X_1|_{\rho_1}|_{\rho_2} \cdot X_2|_{\rho_1}|_{\rho_2}$。

现在我们详细证明该定理。注意，为了简化计算，我们将沿着上述证明思路的逆向进行证明。

步骤 1：固定 ρ_1 后应用平均论证。设 $\hat{Y}$、$\hat{X}_1$ 和 $\hat{X}_2$ 是通过支撑扩张从 X_1X_2、X_1、X_2 得到的、定义在 $\hat{V} \triangleq V_1 \cup V_2 \cup V_1V_2$ 上的随机变量。设 $\pi_1 \cup \pi_2$ 是 $[n]$ 的一个划分，使得对于任意种子 $x \in \{0,1\}^n$，C_1 只读取 x_{π_1}，而 C_2 只读取 x_{π_2}。令 $\eta^{-1} \in \mathsf{Log}$ 为稍后确定的参数。显然，对于任意固定的赋值 ρ_1、ρ_2，分别赋给 x_{π_1} 和 x_{π_2}，

$$\mathbb{E}_\eta[\hat{Y}|_{\rho_1}|_{\rho_2}] = \mathbb{E}_\eta[\hat{X}_1|_{\rho_1}|_{\rho_2}] \cdot \mathbb{E}_\eta[\hat{X}_2|_{\rho_1}|_{\rho_2}] \tag{3.34}$$

根据随机变量的定义。

注意，$\hat{X}_1|_{\rho_1}$ 是一个不会读取其种子的随机变量x_{ρ_2}。因此，对于任意固定的 ρ_2，ρ_2'，$|\mathbb{E}_\eta[\hat{X}_1|_{\rho_1}|_{\rho_2'}] - \mathbb{E}_\eta[\hat{X}_1|_{\rho_1}|_{\rho_2}]| = 0$。根据期望的平均论证，对于任意 ρ_2，我们有

$$|\mathbb{E}_\eta[\hat{X}_1|_{\rho_1}] - \mathbb{E}_\eta[\hat{X}_1|_{\rho_1}|_{\rho_2}]| \le 3\eta \cdot \|\hat{V}\|, \tag{3.35}$$

随后根据方程（3.34），

$$|\mathbb{E}_\eta[\hat{Y}|_{\rho_1}|_{\rho_2}] - \mathbb{E}_\eta[\hat{X}_1|_{\rho_1}] \cdot \mathbb{E}_\eta[\hat{X}_2|_{\rho_1}|_{\rho_2}]| \le 3\eta \cdot \|\hat{V}\| \cdot \mathbb{E}_\eta[\hat{X}_2|_{\rho_1}|_{\rho_2}] \le 3\eta \cdot \|\hat{V}\|^2. \tag{3.36}$$

因此，根据期望的平均论证，对于任意固定的赋值 ρ_1 到x_{π_1}，我们有

$$|\mathbb{E}_\eta[\hat{Y}|_{\rho_1}] - \mathbb{E}_\eta[\hat{X}_1|_{\rho_1}] \cdot \mathbb{E}_\eta[\hat{X}_2|_{\rho_1}]| \le 3\eta \cdot \|\hat{V}\| \cdot (1 + |\mathbb{E}_\eta[\hat{X}_1|_{\rho_1}]|) \le 3\eta \cdot \|\hat{V}\| \cdot (1 + \|\hat{V}\|). \tag{3.37}$$

注意，这里我们将$\hat{Y}|_{\rho_1}$、$\hat{X}_2|_{\rho_1}$ 视为随机变量，并将 $\mathbb{E}_\eta[\hat{X}_1|_{\rho_1}]$ 视为系数。

步骤 2：再次使用平均论证。与方程（3.35）类似，我们先证明，对于任意 $\mathbb{E}_\eta[\hat{X}_2|_{\rho_1}]$，它都接近 $\mathbb{E}_\eta[\hat{X}_2]$。我们可以看到，对于任意赋值 ρ_1，ρ_1 到 ρ_1' 和 x_{π_1} 到 ρ_2，x_{π_2}，$\mathbb{E}_\eta[\hat{X}_2|_{\rho_1}|_{\rho_2}] = \mathbb{E}_\eta[X_2|_{\rho_1'}|_{\rho_2}]$，因为 X_2 不读取 x_{π_1}。因此，根据期望的平均论证，对于每个ρ_1，ρ_1'，

$$|\mathbb{E}_\eta[\hat{X}_2|_{\rho_1}] - \mathbb{E}_\eta[\hat{X}_2|_{\rho_1'}]| \le 6\eta \cdot \|\hat{V}\|.$$

再次根据应用于 $\hat{X}_2$的期望的平均论证，我们得到 ρ_1'，使得

$$|\mathbb{E}_\eta[\hat{X}_2|_{\rho_1}] - \mathbb{E}_\eta[\hat{X}_2]| \le 3\eta \cdot \|\hat{V}\| + |\mathbb{E}_\eta[\hat{X}_2|_{\rho_1}] - \mathbb{E}_\eta[\hat{X}_2|_{\rho_1'}]| \le 9\eta \cdot \|V\|.$$

将此与方程（3.37）结合起来，我们得到

$$\begin{aligned} |\mathbb{E}_\eta[\hat{Y}|_{\rho_1}] - \mathbb{E}_\eta[\hat{X}_1|_{\rho_1}] \cdot \mathbb{E}_\eta[\hat{X}_2]| &\le |\mathbb{E}_\eta[\hat{Y}|_{\rho_1}] - \mathbb{E}_\eta[\hat{X}_1|_{\rho_1}] \cdot \mathbb{E}_\eta[\hat{X}_2|_{\rho_1}]| + 9\eta \cdot \|\hat{V}\|^2 \\ &\le 12\eta \cdot \|\hat{V}\|^2 + 3\eta \cdot \|\hat{V}\|. \end{aligned} \tag{3.38}$$

应用期望的平均论证于方程（3.38），对于随机变量 $\hat{Y}$ 和 $\hat{X}_1$，我们有

$$\begin{aligned} |\mathbb{E}_\eta[\hat{Y}] - \mathbb{E}_\eta[\hat{X}_1] \cdot \mathbb{E}_\eta[\hat{X}_2]| &\le |\mathbb{E}_\eta[\hat{Y}|_{\rho_1}] - \mathbb{E}_\eta[\hat{X}_1|_{\rho_1}] \cdot \mathbb{E}_\eta[\hat{X}_2]| + 3\eta \cdot \|V\| \cdot (1 + \|V\|) \\ &\le 15\eta \cdot \|\hat{V}\|^2 + 6\eta \cdot \|\hat{V}\|. \end{aligned} \tag{3.39}$$

Wr总结一下。请注意，根据支持扩展一致性，我们有 t hat

$$|\mathbb{E}_\eta[\hat{Y}] - \mathbb{E}_\eta[X_1X_2]|, |\mathbb{E}_\eta[\hat{X}_1] - \mathbb{E}_\eta[X_1]|, |\mathbb{E}_\eta[\hat{X}_2] - \mathbb{E}_\eta[X_2]| \leq 3\eta \cdot \|\hat{V}\|.$$

根据期望的精度一致性，我们有

$$|\mathbb{E}_\delta[X_1X_2] - \mathbb{E}_\eta[X_1X_2]|, |\mathbb{E}_\delta[X_1] - \mathbb{E}_\eta[X_1]|, |\mathbb{E}_\delta[X_2] - \mathbb{E}_\eta[X_2]| \leq (2\delta + \eta) \cdot \|\hat{V}\|.$$

因此，我们可以从方程（3.39）推导出

$$\begin{aligned}
&|\mathbb{E}_\delta[X_1X_2] - \mathbb{E}_\delta[X_1] \cdot \mathbb{E}_\delta[X_2]| \\
\leq\ &|\mathbb{E}_\eta[X_1X_2] - \mathbb{E}_\eta[X_1] \cdot \mathbb{E}_\eta[X_2]| + (2\delta + \eta) \cdot \|\hat{V}\| + (4\delta + 2\eta) \cdot \|V\|^2 \\
\leq\ &|\mathbb{E}_\eta[\hat{Y}] - \mathbb{E}_\eta[\hat{X}_1] \cdot \mathbb{E}_\eta[\hat{X}_2]| + (2\delta + \eta) \cdot \|\hat{V}\| + (4\delta + 2\eta) \cdot \|V\|^2 + 3\eta \cdot \|\hat{V}\| + 6\eta \cdot \|\hat{V}\|^2 \\
\leq\ &|\mathbb{E}_\eta[\hat{Y}] - \mathbb{E}_\eta[\hat{X}_1] \cdot \mathbb{E}_\eta[\hat{X}_2]| + (2\delta + 4\eta) \cdot \|\hat{V}\| + (4\delta + 8\eta) \cdot \|\hat{V}^2\| \\
\leq\ &(2\delta + 10\eta) \cdot \|\hat{V}\| + (4\delta + 23\eta) \cdot \|\hat{V}\|^2.
\end{aligned}$$

令 $\eta = \beta/100$，由此完成证明。 □

随后，我们可以得到显式独立伯努利随机变量的乘法原理的以下更方便形式：

推论 3.32（伯努利随机变量乘法原理）。 APX_1 证明了以下陈述。设n、 m、 $\delta^{-1} \in \mathsf{Log}$和 X_1、...、 X_m 是定义在 $\{0,1\}$上的显式独立随机变量，种子长度为 n。那么

$$\left|\mathbb{E}_\delta[X_1X_2 \dots X_m] - \prod_{j\in[i]} \mathbb{E}_\delta[X_i]\right| \leq 8\delta \cdot m,$$

其中，随机变量 $X_1X_2 \dots X_m$ 以自然方式定义。

证明。 我们在 APX_1 中进行论证。固定 $n, m, \delta^{-1} \in \mathsf{Log}$。我们对 i 进行归纳，使得对每个 $i \in [m]$，都有

$$\left|\mathbb{E}_\delta[X_1X_2 \dots X_i] - \prod_{j\in[i]} \mathbb{E}_\delta[X_i]\right| \leq 8\delta \cdot i. \tag{3.40}$$

请注意，这里对无量词公式进行归纳，而这在 APX_1 中是可行的。基础情形$i = 1$ 显然成立。假设方程（3.40）成立。根据乘法原理，

$$\begin{aligned}
&|\mathbb{E}_\delta[X_1X_2 \dots X_iX_{i+1}] - \mathbb{E}_\delta[X_1X_2 \dots X_i] \cdot \mathbb{E}_\delta[X_{i+1}]| \\
&\quad \leq 3\delta \cdot \|V\| + 5\delta \cdot \|V\|^2 \leq 8\delta,
\end{aligned} \tag{3.41}$$

随后

$$\begin{aligned}
&\left|\mathbb{E}_\delta[X_1X_2 \dots X_iX_{i+1}] - \prod_{j\in[i+1]} \mathbb{E}_\delta[X_i]\right| \\
\leq\ &\left|\mathbb{E}_\delta[X_1X_2 \dots X_i] \cdot \mathbb{E}_\delta[X_{i+1}] - \prod_{j\in[i+1]} \mathbb{E}_\delta[X_i]\right| + 8\delta && \text{(Equation (3.41))} \\
\leq\ &\left|\mathbb{E}_\delta[X_1X_2 \dots X_i] - \prod_{j\in[i]} \mathbb{E}_\delta[X_i]\right| \cdot |\mathbb{E}_\delta[X_{i+1}]| + 8\delta \\
\leq\ &8\delta \cdot i \cdot \|V\| + 8\delta \leq 8\delta \cdot (i+1). && \text{（归纳假设）}
\end{aligned}$$

证明至此完成。 □

3.4.3 单边错误陈述的误差缩减

乘法原理使我们能够证明，通过重复对单侧错误算法进行误差缩减是正确的。具体而言，对于接受其输入中占 $1-\varepsilon$ 比例的电路 C，电路 $C^{\vee k}(x_1, \ldots, x_k) = \bigvee_{i\in[k]} C(x_i)$ 接受其输入中除占 ε^k 比例以外的所有输入。

这可以形式化为以下定理：

定理 *3.33*（单边误差归约引理）。设 $C^{\vee k}\colon \{0,1\}^{nk} \to \{0,1\}$ 是由任意电路 $C\colon \{0,1\}^n \to \{0,1\}$ 定义的电路 $C^{\vee k}(x_1, \ldots, x_k) \triangleq \bigvee_{i\in[k]} C(x_i)$。以下陈述可在 APX_1 中证明。对于任意 $n, k, \delta^{-1}, \gamma^{-1}, \beta^{-1} \in \mathit{Log}$ 和电路 $C\colon \{0,1\}^n \to \{0,1\}$，若 $\mathsf{P}_\delta(\neg C) \le \varepsilon$ 且 $\gamma \ge (\delta+\beta+\varepsilon)^k + \delta + \beta$，则 $\mathsf{P}_\delta(\neg C^{\vee k}) \le \gamma$。

证明。我们在 APX_1 中进行论证。Fix $n, \delta^{-1}, \gamma^{-1}, \beta^{-1} \in \mathsf{Log}$ 和电路 $C\colon \{0,1\}^n \to \{0,1\}$。令 $V \triangleq \{0,1\}$，并令 $\eta^{-1} \in \mathsf{Log}$ 为稍后确定的参数。令 X_i 为一个随机变量，它取一个 nk 位的种子 $(x_1, \ldots, x_k) \in (\{0,1\}^n)^k$，并对 $i \in [k]$ 输出 $\neg C(x_i)$。显然，$X_1, \ldots, X_m$ 是显式独立随机变量。令 Y 为一个随机变量，它取一个 nk 位的种子 $(x_1, \ldots, x_k) \in (\{0,1\}^n)^k$，并输出 $\neg C^{\vee k}(x_1, \ldots, x_k)$。

随机变量与近似计数。显然，Y 是电路 $\neg C^{\vee k}$ 对应的指示随机变量，因此根据命题3.12，$|\mathbb{E}_\eta[Y] - \mathsf{P}_\eta(\neg C^{\vee k})| \le 3\eta$。

我们将证明，对每个 $i \in [k]$，$|\mathbb{E}_\eta[X_i] - \mathsf{P}_\eta(\neg C)| \le 6\eta$。任取 $i \in [k]$，并令 $\pi_i \cup \pi_{\bar{i}} = [nk]$，其中 π_i 表示与 i 第 n 位比特块相对应的索引集合，该块会读取 X_i；而 $\pi_{\bar{i}}$ 表示其余的 $(k-1)n$ 个索引。对每个赋值 ρ，对于 π_i，我们可以看到 $X_i|_\rho$ 是 C 的指示随机变量，因此根据命题3.12，

$$|\mathbb{E}_\eta[X_i|_\rho] - \mathsf{P}_\eta(\neg C)| \le 3\eta.$$

随后，我们可以应用期望的平均论证来证明

$$|\mathbb{E}_\eta[X_i] - \mathsf{P}_\eta(\neg C)| \le 6\eta. \tag{3.42}$$

注意，根据假设，我们有 $\mathsf{P}_\delta(\neg C) \le \varepsilon$。根据用于近似计数的 Precision Consistency Axiom，我们有 $\mathsf{P}_\eta(C) \le \delta + 2\eta + \varepsilon$，因此

$$\mathbb{E}_\eta[X_i] \le \mathsf{P}_\eta(C) + 6\eta \le \delta + 8\eta + \varepsilon \tag{3.43}$$

对每个 $i \in [k]$。

总结一下。我们首先证明 $|\mathbb{E}_\eta[Y] - \mathbb{E}_\eta[X_1 X_2 \ldots X_k]| \le 6\eta$。注意，$Y$ 和 $X_1 X_2 \ldots X_k$ 都是取值为 nk 位种子的随机变量，并且对种子的每个赋值 ρ，都有 $\mathbb{E}_\eta[Y|_\rho] = \mathbb{E}_\eta[X_1 X_2 \ldots X_k|_\rho]$。根据期望的平均论证，我们得到

$$|\mathbb{E}_\eta[Y] - \mathbb{E}_\eta[X_1 X_2 \ldots X_k]| \le 3\eta \cdot \|V\| \cdot 2 \le 6\eta. \tag{3.44}$$

此外，根据近似计数的 Precision Consistency Axiom，我们得到

$$\mathsf{P}_\delta(\neg C^{\vee k}) \le \mathsf{P}_\eta(\neg C^{\vee k}) + \delta + 2\eta.$$

令 $\eta \triangleq \beta/(20k)$。回想一下，只需证明 $\mathbb{E}_\eta[Y] \le \gamma$。由此可得

$$\begin{aligned}
\mathsf{P}_\delta(\neg C^{\vee k}) &\le \mathsf{P}_\eta(\neg C^{\vee k}) + \delta + 2\eta && \text{(Precision Consistency Axiom)}\\
&\le \mathbb{E}_\eta[Y] + \delta + 5\eta\\
&\le \mathbb{E}_\eta[X_1 X_2 \ldots X_k] + \delta + 12\eta && \text{(Equation (3.44))}\\
&\le \prod_{i\in[k]} \mathbb{E}_\eta[X_i] + \delta + 8\eta k + 12\eta && \text{(伯努利随机变量乘法原理)}\\
&\le \prod_{i\in[k]} (\delta + 8\eta + \varepsilon) + \delta + 8\eta k + 12\eta && \text{(Equation (3.43))}\\
&\le (\delta+\beta+\varepsilon)^k + \delta + \beta \le \gamma,
\end{aligned}$$

由此完成证明。 □

3.4.4 O(logn) 个随机变量的 Chernoff 界

我们考虑一种切尔诺夫界，其中随机变量的数量为 $m \in \mathsf{LogLog}$。简而言之，我们将 Chv´atal 提出的、使用二项式系数的组合证明形式化（例如参见 [Mul18，第 3 节。2]）。

定义 3.34 （二项式系数，在 PV_1 中）。 设 n， $m \in \mathsf{Log}$ 和 $m \le n$。二项式系数 $\binom{n}{m}$ 递归定义如下：

$$\binom{n}{0} \triangleq 1, \quad \binom{n}{m} \triangleq \binom{n-1}{m-1} + \binom{n-1}{m}. \tag{3.45}$$

对于 $m > n$，令 $\binom{n}{m} \triangleq 0$。注意，计算 $(1^n, 1^m) \mapsto \binom{n}{m}$ 的函数可以由一个在 PV中运行、用时为 $\mathsf{poly}(n)$ 的函数定义，使得方程 (3.45) 可在PV_1中证明。

引理 3.35 （二项式定理）。 以下陈述可在 PV_1 中证明。对于每个 $n \in \mathsf{Log}$ 以及$x, y \in \mathbb{Q} \setminus \{0\}$,

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}.$$

证明概要。 Fix $n \in \mathsf{Log}$ 以及 x， $y \in \mathbb{Q}$。我们对 $n \in \mathsf{Log}$ 使用归纳法证明。基础情形中，该方程对 $n = 0$ 显然成立，因为等式两边均为 1。归纳步骤由方程 (3.45) 得出。 □

现在我们已经准备好证明 $n \in \mathsf{LogLog}$ 时的切尔诺夫界。

定理 *3.36*（切尔诺夫界 *I*，*LogLog* 形式）。以下命题在 APX_1 中可证。设 $V = \{0,1\}$, $n, \delta^{-1}, \beta^{-1} \in Log$, 且 $m \in LogLog$。设 $X_1, \ldots, X_m$ 是由元组 (V, n, C) 定义、取值于 V 上的一列显式独立同分布随机变量，并使用一个 nm 位种子 $(z_1, \ldots, z_m) \in (\{0,1\}^n)^m$。设对任意 $i \in [m]$， $p \triangleq \mathbb{E}_\delta[X_i] \in \mathbb{Q}$，且 $Y_{\ge k}$ 是 $X_1 + \cdots + X_m \ge k$ 的指示变量，它使用一个 nm 位种子。则对于$t \in \mathbb{Q}$, $0 \le t \le 1$，以及 $k \ge (1+t)pm$,

$$\mathbb{E}_\delta[Y_{\ge k}] \le \left(e^{-t^2 p/4} + (4\delta + \beta) \cdot 2^{-pt(1+t)}\right)^m + \delta + \beta.$$

证明。 我们在 APX_1中论证。Fix $V = \{0,1\}$、 n、 δ^{-1}、 $\beta^{-1} \in \mathsf{Log}$、 $m \in \mathsf{LogLog}$以及 X_1、……、 X_m。令 $p \triangleq \mathbb{E}_\delta[X_i]$、 t、 k 以及 $Y_{\ge k}$ 如上定义。令 $\eta^{-1} \in \mathsf{Log}$ 为稍后确定的参数。根据期望的精度一致性，

$$|\mathbb{E}_\eta[X_i] - p| = |\mathbb{E}_\delta[X_i] - \mathbb{E}_\eta[X_i]| \le \delta + 2\eta. \tag{3.46}$$

每个子集的概率。 令 $\alpha \subseteq [m]$ 编码一个变量子集。我们如下定义 $\{0,1\}$ 上的随机变量Y_α： 给定任意种子 $(z_1, \ldots\ldots, z_m) \in (\{0,1\}^n)^m$， $Y_\alpha = 1$ 当且仅当对每个 $i \in \alpha$， $X_i = 1$。在第一步中，我们证明

$$\mathbb{E}_\eta[Y_\alpha] \le (p + \delta + O(\eta m))^{|\alpha|} \tag{3.47}$$

对每个 $\alpha \subseteq [m]$。注意，由于 $m \in \mathsf{LogLog}$，我们可以通过一个显式的电路列表，为 $\alpha \subseteq [m]$ 定义所有随机变量 Y_α。这将在后续证明中有用。

任取 $\alpha = \{i_1, \ldots, i_t\} \subseteq [m]$。由于 X_1，…， X_m是显式独立随机变量，根据伯努利随机变量乘法原理，我们有

$$\left| \mathbb{E}_\eta \left[\prod_{j \in [t]} X_{i_j} \right] - \prod_{j \in [t]} \mathbb{E}_\eta[X_{i_j}] \right| \le 8\eta m.$$

随后，我们有

$$\mathbb{E}_\eta\left[\prod_{j\in[t]} X_{i_j}\right] \le 8\eta m + (p+\delta+2\eta)^{|\alpha|}.$$

注意，对于每一个赋值 ρ 到随机种子，$\mathbb{E}_\eta[Y_\alpha|_\rho] = \mathbb{E}_\eta[\prod_{j\in[t]} X_{i_j}|_\rho]$。根据期望的平均论证，我们有

$$\mathbb{E}_\eta[Y_\alpha] \le \mathbb{E}_\eta\left[\prod_{j\in[t]} X_{i_j}\right] + 6\eta \le 14\eta m + (p+\delta+2\eta)^{|\alpha|}. \tag{3.48}$$

设 $\overline{Y}_\alpha$ 为定义在 $\{0,1\}$ 上的随机变量，定义如下：给定任意种子（z_1，……，z_m）$\in$（$\{0,1\}^n$）^{m}，$Y_\alpha = 1$ 当且仅当对于每一个 $i \in [m]\setminus\alpha$，$X_i = 0$。与上述证明类似，我们有

$$\mathbb{E}_\eta\left[\overline{Y}_\alpha\right] \le (1-p+\delta+10\eta m)^{m-|\alpha|} + 20\eta m. \tag{3.49}$$

合并所有子集。设ˆ $Y_{\ge k}$ 为 $\{0,1\}$上的如下随机变量：

$$\hat{Y}_{\ge k} \triangleq \sum_{\alpha\subseteq[m],|\alpha|\ge k} Y_\alpha \overline{Y}_\alpha.$$

通过应用乘法原理和期望的线性性，我们有

$$\begin{aligned}
&\mathbb{E}_\eta[\hat{Y}_{\ge k}] \\
&\le 3\eta\cdot 2^m + \sum_{\alpha\subseteq[m],|\alpha|\ge k} \mathbb{E}_\eta[Y_\alpha\overline{Y}_\alpha] && (\textit{Union Bound}) \\
&\le 3\eta\cdot 2^m + 8\eta\cdot 2^m + \sum_{\alpha\subseteq[m],|\alpha|\ge k} \mathbb{E}_\eta[Y_\alpha]\cdot\mathbb{E}[\overline{Y}_\alpha] && (\textit{Multiplication Principle}) \\
&\le 11\eta\cdot 2^m + \sum_{\alpha\subseteq[m],|\alpha|\ge k} \Big((p+\delta+2\eta m)^{|\alpha|} + 14\eta m\Big)\Big((1-p+\delta+10\eta m)^{m-|\alpha|} + 20\eta m\Big) \\
& && (\text{Equations (3.48) and (3.49)}) \\
&\le 90\eta m\cdot 2^m + \sum_{j\ge k}\binom{m}{j}(p+\delta+2\eta m)^j(1-p+\delta+10\eta m)^{m-j}.
\end{aligned}$$

注意，最后一行中的二项式系数可以高效计算（即使使用暴力计数算法），因为 m，$j \in$ 为LogLog。

回顾，$Y_{\ge k}$ 是如下随机变量，它表明 $X_1+\cdots+X_m \ge k$。注意，对于每一个赋值ˆρ 到随机种子，我们有 $\mathbb{E}_\eta[Y_{\ge k}|_\rho] \le \mathbb{E}_\eta[Y_{\ge k}|_\rho]$。因此，根据期望的平均论证，我们有

$$\mathbb{E}_\eta[Y_{\ge k}] \le \mathbb{E}_\eta[\hat{Y}_{\ge k}] + 6\eta \le \sum_{j\ge k}\binom{m}{j}(p+\delta+2\eta m)^j(1-p+\delta+10\eta m)^{m-j} + 100\eta m\cdot 2^m. \tag{3.50}$$

二项式系数不等式。剩下的工作是证明方程（3.50）的一个上界。注意，由于 $m \in$LogLog，我们可以轻松地形式化 [Mul18 第 3 节中的标准证明。2], 其中关于二项式系数的所有等式都可以在 PV中证明。

令 $\tau = e^{\lambda} \geq 1$ 为一个稍后确定的参数。更具体地说，对于任意 $\varepsilon^{-1} \in \mathsf{Log}$，我们可以进行如下计算：

$$\begin{aligned}
&\sum_{j\geq k} \binom{m}{j} (p+\varepsilon)^j (1-p+\varepsilon)^{m-j} \\
\leq &\sum_{j\geq k} \binom{m}{j} (p+\varepsilon)^j (1-p+\varepsilon)^{m-j} \tau^{j-k} + \sum_{0\leq j<k} (p+\varepsilon)^j (1-p+\varepsilon)^{m-j} \tau^{j-k} \\
= &\tau^{-k} \sum_{j=0}^{m} \binom{m}{j} \left((p+\varepsilon)\tau\right)^j (1-p+\varepsilon)^{m-j} \\
= &\tau^{-k} \big(1 + p(\tau-1) + \varepsilon(\tau+1)\big)^m && (\textit{Binomial Theorem}) \\
\leq &\left(\frac{1 + p(e^{\lambda}-1) + \varepsilon(e^{\lambda}+1)}{e^{\lambda p(1+t)}}\right)^m .
\end{aligned}$$

注意，对于 $\lambda \in (0,1)$，我们有 $1+\lambda \leq e^{\lambda} \leq 1+\lambda+3\lambda^2/4$，且这可在 PV 中证明。接着

$$\ln\big(1 + p(e^{\lambda}-1)\big) \leq p(e^{\lambda}-1) \leq p\lambda + 3p\lambda^2/4.$$

这意味着 $1 + p(e^{\lambda}-1) \leq \exp(p\lambda + 3p\lambda^2/4)$。令 $\varepsilon \triangleq \delta + 30\eta m$, $\eta \leq \beta/(120m)$，则 $\varepsilon \leq \delta + \beta/4$，并且 $\lambda \triangleq t$。于是我们有

$$\left(\frac{1 + p(e^{\lambda}-1) + \varepsilon(e^{\lambda}+1)}{e^{\lambda p(1+t)}}\right)^m \leq \left(e^{-t^2 p/4} + 4(\delta+\beta/4)\cdot e^{-pt(1+t)}\right)^m .$$

最后，我们可以得到

$$\begin{aligned}
\mathbb{E}_{\delta}[Y_{\geq k}] &\leq \mathbb{E}_{\eta}[Y_{\geq k}] + \delta + 2\eta && (\textit{Precision Consistency of Expectation}) \\
&\leq \left(e^{-t^2 p/4} + 4(\delta+\beta/4)\cdot e^{-pt(1+t)}\right)^m + 200\eta m \cdot 2^m + \delta + 2\eta \\
&\leq \left(e^{-t^2 p/4} + (4\delta+\beta)\cdot e^{-pt(1+t)}\right)^m + \delta + \beta,
\end{aligned}$$

其中，最后一个不等式在令 $\eta \triangleq \beta/(1000m\cdot 2^m)$ 时成立。 □

基本上使用相同的证明方法，并取 $\tau = e^{-\lambda} < 1$，我们可以得到尾部概率另一侧的 Chernoff 界：

定理 3.37 (切尔诺夫界 II，LogLog 形式)。 以下句子可在 APX_1 中证明。设 $V = \{0,1\}$, $n, \delta^{-1}, \beta^{-1} \in \mathsf{Log}$，且 $m \in \mathsf{LogLog}$。设 $X_1, \ldots, X_m$ 是一列定义在 V 上的显式独立同分布随机变量，其使用 nm 位种子 $(z_1, \ldots, z_m) \in (\{0,1\}^n)^m$。设 $p \triangleq \mathbb{E}_{\delta}[X_i] \in \mathbb{Q}$，且 $Y_{\leq k}$ 是 $X_1 + \cdots + X_m \leq k$ 的指示变量，它使用 nm 位种子。那么对于 $t \in \mathbb{Q}$, $0 \leq t \leq 1$，以及 $k \leq (1-t)pm$,

$$\mathbb{E}_{\delta}[Y_{\leq k}] \leq \left(e^{-t^2 p/4} + (4\delta+\beta)\cdot 2^{-pt(1-t)}\right)^m + \delta + \beta.$$

4 APX中的理论计算机科学$_1$

在本节中，我们在 APX_1 中形式化来自算法、复杂性理论及相关领域的若干基本结果。

4.1 姚期智的区分器到预测器变换

定理 4.1（姚氏转换）. APX_1 证明如下陈述。设 n、m、δ^{-1}、$\beta^{-1} \in \mathsf{Log}$、$G\colon \{0,1\}^m \to \{0,1\}^n$ 为一个多输出电路，且 $C \in B_n$ 为一个电路，使得

$$|\mathsf{P}_\delta(C \circ G) - \mathsf{P}_\delta(C)| \geq 2\delta + \varepsilon \tag{4.1}$$

对于某些 $\varepsilon \in (0,\ 1) \cap \mathbb{Q}$，其中 $C \circ G$ 是由以下方式定义的 m 输入电路：$(C \circ G)(u) \triangleq C(G(u))$.

那么存在一个索引 $i \in [n]$ 和一个电路 $P\colon \{0,1\}^{i-1} \to \{0,1\}$，使得以下结论成立：令$T(u) \in B_m$ 为满足以下条件的电路：若 $T(u) = 1$，则 $P(G(u)_{<i}) = G(u)_i$（即， P成功预测了 $G(u)$ 的第 i 位），那么

$$\left|\mathsf{P}_\delta(T) - \frac{1}{2}\right| \geq \frac{\varepsilon}{4n} - (\delta + \beta).$$

证明。我们将 APX_1 中姚引理的标准证明形式化（例如参见 [AB09，第 9]章）。取n、m、δ^{-1}、$\beta^{-1} \in \mathsf{Log}$、$G\colon \{0,1\}^m \to \{0,1\}^n$以及电路 $C \in B_n$。对于每个索引 $i \in \{0,1,\ldots,n\}$，我们定义电路 $C_i\colon \{0,1\}^m \times \{0,1\}^n \to \{0,1\}$ 如下：

- C_i 将其输入解析为 $(u,\ x) \in \{0,1\}^m \times \{0,1\}^n$。
- 令 $z \triangleq G(u)_{\leq i} \circ x_{>i}$，即一个字符串，其前 i 比特与 $G(u)$ 的前 i 比特一致，其余比特与 x 的最后 $n-i$ 比特一致。于是，电路 $C_i(u,\ x)$ 输出 $C(z)$。

令 X_0、X_1、...、X_n 为定义在 $\{0,1\}$ 上、种子长度为 $m+n$ 的随机变量，其中 X_i 是 $C_i(j、\ x) = 1$ 的指示变量。也就是说， X_i 由元组 $(\{0,1\}、\ m+n、\ C_i)$ 定义。

步骤 1： $\mathbb{E}_\eta[X_0]$ **与** $\mathbb{E}_\eta[X_n]$**之间的差距。** 我们首先论证 $|\mathbb{E}_\eta[X_0] - \mathbb{E}_\eta[X_n]|$ 很大。注意，由方程（4.1）和 Precision Consistency Axiom，可得

$$|\mathsf{P}_\eta(C \circ G) - \mathsf{P}_\eta(C)| \geq \varepsilon - 4\eta. \tag{4.2}$$

注意， X_0 是定义在 $\{0,1\}$ 上、种子长度为 $m+n$ 的随机变量；对于种子（u、x） $\in \{0,1\}^m \times \{0,1\}^n$，它忽略种子的第一部分并输出 C（x）。对于种子的第一部分的任意赋值 $u \in \{0,1\}^m$，可以验证 $|\mathbb{E}_\eta[X_0|_u] - \mathsf{P}^\eta(C)| \leq 3\eta$，因此根据期望的平均论证，可知

$$|\mathbb{E}_\eta[X_0] - \mathsf{P}_\eta(C)| \leq 6\eta.$$

同样，我们可以证明

$$|\mathbb{E}_\eta[X_n] - \mathsf{P}_\eta(C \circ G)| \leq 6\eta. \tag{4.3}$$

这是因为 X_n 是一个随机变量，它在种子 $(u,\ x) \in \{0,1\}^m \times \{0,1\}^n$ 上忽略种子的第二部分，并输出 $C \circ G(u)$。

结合方程 (4.2) 和方程 (4.3)，我们得到

$$|\mathbb{E}_\eta[X_0] - \mathbb{E}_\eta[X_n]| \geq \varepsilon - 16\eta \tag{4.4}$$

步骤 2： **与** $\mathbb{E}_\eta[X_{i+1}]$**之间的差距。** 由于$\overline{|\mathbb{E}_\eta}[X_0] - \mathbb{E}_\eta[X_n]| \geq \beta - 16\eta + \varepsilon$，我们知道对于某个$1 \leq i \leq n$，

$$|\mathbb{E}_\eta[X_{i-1}] - \mathbb{E}_\eta[X_i]| \geq \frac{\varepsilon}{n} - \frac{16\eta}{n}. \tag{4.5}$$

更具体地说，假设为了导出矛盾，这并不成立。我们可以对 j 使用归纳法证明：如果 $j \leq n$，那么 $|\mathbb{E}_\eta[X_0] - \mathbb{E}_\eta[X_j]| < (j/n) \cdot (\varepsilon - 16\eta)$。

我们将为这个索引 i构造一个预测器 P。回想一下， X_{i-1} 和 X_i 都是随机变量，它们将种子解析为 $(u,\ x) \in \{0,1\}^m \times \{0,1\}^n$，并且

- X_{i-1} outputs $C(G(u)_{<i} \circ x_i \circ x_{>i})$;

- X_i 输出 $C(G(u)_{<i} \circ G(u)_i \circ x_{>i})$。

令 $\overline{X_i}$ 为这样一个随机变量：它将输入解析为 $(u,\ x) \in \{0,1\}^m \times \{0,1\}^n$，并输出 $C(G(u)_{<i} \circ \overline{G(u)_i} \circ x_{>i})$。我们将证明

$$\left|\mathbb{E}_\eta[X_i] - \mathbb{E}_\eta[\overline{X_i}]\right| > \frac{\varepsilon}{2n} - 100\eta \tag{4.6}$$

通过重写方程 $\mathbb{E}_\eta[X_{i-1}]$ 和 $\mathbb{E}_\eta[X_i]$（4.5）来证明。

令 X^0_{i-1}，X^1_{i-1} 为定义在 $\{0,1\}$ 上的随机变量，它们将种子解析为 $(u,\ x) \in \{0,1\}^m \times \{0,1\}^n$，满足：

- X^0_{i-1} 当且仅当 $C(G(u)_{<i} \circ x_i \circ x_{>i}) = 1$ 且 $G(u)_i = x_i$ 时输出 $\mathbf{1}$。
- X^1_{i-1} 当且仅当 $C(G(u)_{<i} \circ G(u)_i \circ x_{>i}) = \overline{1 \text{ 且 } G(u)_i \neq x_i}$ 时输出 $\mathbf{1}$。

可以观察到，对于任意 ρ 种子的赋值，$X_{i-1}|_\rho = X^0_{i-1}|_\rho + X^1_{i-1}|_\rho$，因此根据期望的线性性，

$$\left|\mathbb{E}_\eta[X_{i-1}] - \left(\mathbb{E}_\eta[X^0_{i-1}] + \mathbb{E}_\eta[X^1_{i-1}]\right)\right| \le 6\eta. \tag{4.7}$$

类似地，令 X^0_i，X^1_i 为定义在 $\{0,1\}$ 上的随机变量，它们将种子解析为 $(u,\ x) \in \{0,1\}^m \times \{0,1\}^n$，并满足：

- X^0_i 当且仅当 $C(G(u)_{<i} \circ x_i \circ x_{>i}) = 1$ 且 $G(u)_i = x_i$ 时输出 $\mathbf{1}$。
- X^1_i 当且仅当 $C(G(u)_{<i} \circ G(u)_i \circ x_{>i}) = 1$ 且 $G(u)_i \neq x_i$ 时输出 $\mathbf{1}$。

对于任意 ρ 种子的赋值，$X_i|_\rho = X^0_i|_\rho + X^1_i|_\rho$，因此根据期望的平均论证，

$$\left|\mathbb{E}_\eta[X_i] - \left(\mathbb{E}_\eta[X^0_i] + \mathbb{E}_\eta[X^1_i]\right)\right| \le 6\eta. \tag{4.8}$$

可以观察到，X^0_i 和 X^0_{i-1} 是完全相同的随机变量。此外，我们论证

$$\left|\mathbb{E}_\eta[X_i] - 2 \cdot \mathbb{E}_\eta[X^1_i]\right| \le 20\eta. \tag{4.9}$$

（作为合理性检查，$\mathbb{E}[X_i] = 2 \cdot \mathbb{E}[X^1_i]$ 在精确期望下成立。）反设此结论不成立。根据期望的平均论证，存在一个赋值 ρ，为除 x_i 以外的所有变量赋值，使得

$$\left|\mathbb{E}_\eta[X_i|_\rho] - 2 \cdot \mathbb{E}_\eta[X^1_i|_\rho]\right| > 10\eta.$$

注意，$X_i|_\rho$ 和 $X^1_i|_\rho$ 的种子长度都为 $\mathbf{1}$，并且我们知道 $\mathbb{E}[X_i|_\rho] = 2 \cdot \mathbb{E}[X^1_i|_\rho]$。由暴力计数引理可知，这会导致矛盾。类似地，我们可以证明

$$\left|\mathbb{E}_\eta[X_{i-1}] - 2 \cdot \mathbb{E}_\eta[X^1_{i-1}]\right| \le 10\eta. \tag{4.10}$$

根据方程（4.5）和（4.7）至（4.10），我们有

$$\begin{aligned}
\left|\mathbb{E}_\eta[X_i] - \mathbb{E}_\eta[\overline{X_i}]\right| &\ge \left|\left(\mathbb{E}_\eta[X^0_{i-1}] + \mathbb{E}_\eta[X^1_{i-1}]\right) - \left(\mathbb{E}_\eta[X^0_i] + \mathbb{E}_\eta[X^1_i]\right)\right| - 12\eta && \text{(Equations (4.7) and (4.8))} \\
&\ge \left|\mathbb{E}_\eta[X^1_{i-1}] - \mathbb{E}_\eta[X^1_i]\right| - 12\eta \\
&\ge \frac{\left|\mathbb{E}_\eta[X_{i-1}] - \mathbb{E}_\eta[X_i]\right|}{2} - 60\eta && \text{(Equations (4.9) and (4.10))} \\
&> \frac{\varepsilon}{2n} - 100\eta. && \text{(Equation (4.5))}
\end{aligned}$$

步骤 3：构造预测器。现在我们证明，公式（4.6）足以构造预测器。令 $P\colon \{0,1\}^{i-1} \times \{0,1\}^n \to \{0,1\}$ 和 $T\colon \{0,1\}^m \times \{0,1\}^n \to \{0,1\}$ 为以下电路：$P(v,x) \triangleq C(v \circ x_i \circ x_{>i}) \oplus x_i$，且 $T(u,x)$ 的输出为 $\mathbf{1}$，当且仅当 $P(G(u)_{<i}, x) = G(u)_i$。

我们还定义两个电路 T_0，$T_1\colon \{0,1\}^m \times \{0,1\}^n \to \{0,1\}$，使得

- $T_0(u,\ x)$ 在 $C(G(u)_{<i} \circ G(u)_i \circ x_{>i}) = 0$ 且 $x_i = G(u)_i$ 时输出 $\mathbf{1}$。
- $T_1(u,\ x)$ 若 $C(G(u)_{<i} \circ G(u)_i \circ x_{>i}) = \overline{1}$ 且 $x_i \neq G(u)_i$，则输出 $\mathbf{1}$。

可以证明（在 $\mathbf{PV}_1$ 中），$T_0(u,x) = 1$ 当且仅当 $T(u,x) = 1$ 且 $x_i = G(u)_i$；而 $T_1(u,x) = 1$ 当且仅当 $T(u,x) = 1$ 且 $x_i \neq G(u)_i$。因此，对于每个 $(u,x) \in \{0,1\}^m \times \{0,1\}^n$，$T(u,x) = T_0(u,x) + T_1(u,x)$。通过考察它们的指示变量并应用期望的线性性，可以证明

$$|\mathsf{P}_\eta(T) - (\mathsf{P}_\eta(T_0) + \mathsf{P}_\eta(T_1))| \leq 50\eta. \tag{4.11}$$

接下来，我们论证

$$|\mathbb{E}_\eta[X_i] - (1 - 2 \cdot \mathsf{P}_\eta(T_0))| \leq 20\eta. \tag{4.12}$$

反设方程（4.12）不成立。令 I_{T_0} 为 T_0的指示随机变量，并且有 $|\mathbb{E}_\eta[I_{T_0}] - \mathsf{P}\eta(T_0)| \leq 3\eta$（见命题3.12）。和 I_{T_0} 的种子为（u，x）。根据期望的平均论证，存在一个对除 x_i 之外所有变量的 ρ 赋值（即 i 的第 x位比特为 i）使得

$$|\mathbb{E}_\eta[X_i|_\rho] - (1 - 2 \cdot \mathbb{E}_\eta[I_{T_0}|_\rho])| > 10\eta.$$

注意，$X_i|_\rho$ 和 $I_{T_0}|_\rho$ 的种子长度均为 $\mathbf{1}$，根据定义可知[17]

$$|\mathbb{E}[X_i|_\rho] - (1 - 2 \cdot \mathbb{E}[I_{T_0}|_\rho])| = 0.$$

根据暴力计数引理，我们得到矛盾，从而证明了方程（4.12）。类似地，我们可以证明

$$\left|\mathbb{E}_\eta[\overline{X_i}] - 2 \cdot \mathsf{P}_\eta(T_1)\right| \leq 20\eta. \tag{4.13}$$

结合方程（4.6）以及（4.11）至（4.13），可得

$$\begin{aligned}
\left|\mathsf{P}_\eta(T) - \frac{1}{2}\right| &\geq \left|\mathsf{P}_\eta(T_0) + \mathsf{P}_\eta(T_1) - \frac{1}{2}\right| - 50\eta && \text{(Equation (4.11))} \\
&\geq \left|\frac{1 - \mathbb{E}_\eta[X_i]}{2} + \frac{\mathbb{E}_\eta[\overline{X_i}]}{2} - \frac{1}{2}\right| - 80\eta && \text{(Equations (4.12) and (4.13))} \\
&\geq \frac{1}{2} \cdot \left|\mathbb{E}_\eta[X_i] - \mathbb{E}_\eta[\overline{X_i}]\right| - 80\eta \\
&\geq \frac{\varepsilon}{4n} - 180\eta. && \text{(Equation (4.6))}
\end{aligned}$$

回顾一下，T接受输入（u，x）$\in \{0,1\}^m \times \{0,1\}^n$。令 T_x 为将其输入的第二部分固定为 $x \in \{0,1\}^n$后得到的电路。考虑其指示变量（见命题3.12），并应用期望的平均论证，存在一个字符串 $x \in \{0,1\}^n$ 使得

$$\left|\mathsf{P}_\eta[T_x] - \frac{1}{2}\right| \geq \frac{\varepsilon}{4n} - 200\eta.$$

根据定义，可以看出，T_x 求值为 $\mathbf{1}$ 意味着预测器 $P_x(v) \triangleq C(v \circ x \circ x_{>i}) \oplus x_i$ 正确预测了 i的第 $G(u)$ 位。应用近似计数的全局一致性、Precision Consistency Axiom，并令 $\eta \triangleq \beta/400$，即可完成证明。□

4.2 Schwartz-Zippel引理

在陈述 Schwartz-Zippel 引理之前，我们需要明确有限域和多项式的形式化定义。若有限域 $\mathbb{F}$ 满足 $|\mathbb{F}| \in \mathsf{Log}$，则称其为可行域，例如，$\mathbb{F} = \mathbb{F}_p$ 对于某个素数 $p \in \mathsf{Log}$。文献 [Je˘r05第 4.3 节中证明了3]，对于任意可行域，都可以对域元素进行编码，使得（1）

[17]事实上，由于固定 ρ 后，唯一的随机性是 x_i，且 $X_i\restriction_\rho$ 与 x_i相互独立，因此我们有 $I_{T_0}\restriction_\rho = \mathbf{1}\{x_i = G(u)_i\}\,\mathbf{1}\{X_i\restriction_\rho = 0\} = \mathbf{1}\{x_i = G(u)_i\}\,(1 - X_i\restriction_\rho)$。由此可得 $\mathbb{E}[I_{T_0}\restriction_\rho] = \frac{1}{2} \cdot (1 - X_i\restriction_\rho) = \frac{1}{2} \cdot \left(1 - \mathbb{E}[X_i\restriction_\rho]\right)$，这意味着 $\mathbb{E}[X_i\restriction_\rho] = 1 - 2 \cdot \mathbb{E}[I_{T_0}\restriction_\rho]$.

域运算可以由 PV 函数符号实现，并且（2）域公理可以在 PV 中证明。为简单起见，我们将 $\mathbb{F}$ 中的一个元素与其作为字符串的编码视为相同。

固定一个可行域 $\mathbb{F}$。次数为 d 的一元多项式 $p \in \mathbb{F}[x]$ 可以由系数列表 $c_0, c_1, \ldots\ldots, c_d \in \mathbb{F}$ 定义，使得 $p(x) \triangleq c_0 + c_1 x + \cdots + c_d x^d$。如果 $c_0, c_1, \ldots\ldots, c_d$ 中至少有一个非零，则称多项式非零。

命题 4.2（隐含于 [Je˘r05，引理 4.3。6]）。在 PV 中可以证明，任何非零的次数为 d 多项式 $p \in \mathbb{F}[x]$ 至多有 d 个根。

命题 4.3（隐含于 [Je˘r05]）。在 PV 中可以证明，对于任意 $d < |\mathbb{F}|$、任意互不相同的 $x_1, \ldots\ldots, x_d \in \mathbb{F}$以及 $y_1, \ldots\ldots, y_d \in \mathbb{F}$，存在一个次数为 d 的多项式 $p \in \mathbb{F}[x]$，使得 $p(x_i) = y_i$ 对每个 $i \in [d]$都成立。

令 $m, d \in \mathsf{Log}$。我们称电路 C 计算一个 m元 $\mathbb{F}$上的函数，记作 $C : \mathbb{F}^m \to \mathbb{F}$，如果对每个 $x_1, \ldots, x_m \in \mathbb{F}$，都有 $C(x_1, \ldots, x_m) \in \mathbb{F}$。根据域元素的编码方式，某些电路可能无法计算 $\mathbb{F}$ 上的 m元函数，因为它输出的字符串并未编码任何域元素。我们称 $C : \mathbb{F}^m \to \mathbb{F}$ 的个体次数至多为 d，如果对每个 $i \in [m]$ 以及对除第 i 个变量外所有变量的任意赋值 ρ，都存在一个次数至多为 d 的多项式 $p_{i,\rho} \in \mathbb{F}[x]$，使得对于 $x \in \mathbb{F}$，$p_{i,\rho}(x) = C|_\rho(x)$。

定理 4.4 (Schwartz-Zippel引理)。APX_1 证明了以下陈述。设 $\mathbb{F}$ 是一个可行域，其中每个域元素都由长度为 $b \in \mathsf{LogLog}$ 的字符串编码。设 $m, d \in \mathsf{Log}$、$d < |\mathbb{F}|$ 和$C : \mathbb{F}^m \to \mathbb{F}$ 是个体次数至多为 d 的电路。设 $T_C : (\{0,1\}^b)^m \to \{0,1\}$ 是一个电路，给定$(x_1, \ldots, x_m) \in \{0,1\}^b$时，如果对每个 $i \in [m]$ 都有 $x_i \in \mathbb{F}$，且 $C(x_1, \ldots, x_m) = 0$，则该电路接受。

假设 f 对于某些 $\vec{z} \in \mathbb{F}^m$、$C(\vec{z}) \neq 0$。那么对于每个 δ^{-1}、$\beta^{-1} \in \mathsf{Log}$，$\mathsf{P}_\delta(T_C) \leq md/|\mathbb{F}| + \delta + \beta$。

证明。关键思路是将 Atserias 和 Tzameret 的证明形式化 [AT25] 于 APX_1。我们在 APX_1中进行论证。任取一个可行域 $\mathbb{F}$，$b \in \mathsf{LogLog}$，m，$d \in \mathsf{Log}$，C：$\mathbb{F}^m \to \mathbb{F}$，$\vec{z} = (z_1, \ldots, z_m) \in \mathbb{F}_m$，以及 δ^{-1}，$\beta^{-1} \in \mathsf{Log}$，如陈述所示。

令 $\eta^{-1} \in \mathsf{Log}$ 为稍后确定的参数。对于每个 $i \in \{0, 1, \ldots, m\}$，我们定义 $T_C^i : (\{0,1\}^b)^m \to \{0,1\}$ 如下：给定 $(x_1, \ldots, x_m) \in \{0,1\}^b$，若对于每个 $i \in [m]$ 和 $C(x_1, \ldots, x_i, z_{i+1}, \ldots, z_m) = 0$，则接受 $x_i \in \mathbb{F}$。显然，$T_C^0 \equiv \mathsf{Null}$，且 $T_C^m \equiv T_C$。

令 X_0、X_1、……、X_m为 T_C^0、T_C^1、……、T_C^m的指示随机变量。我们将证明，对于每个$i \geq 1$，

$$\mathbb{E}_\eta[X_i] - \mathbb{E}_\eta[X_{i-1}] \leq d/|\mathbb{F}| + 10\eta. \tag{4.14}$$

反设结论不成立。根据 期望的平均论证，存在一个赋值 ρ，赋给种子的除第 i 部分 x_i 以外的所有部分，使得

$$\mathbb{E}_\eta[X_i|_\rho] - \mathbb{E}_\eta[X_{i-1}|_\rho] > d/|\mathbb{F}| + 10\eta - 6\eta > 0. \tag{4.15}$$

注意，$X_{i-1}|_\rho$是 $T_C^{i-1}|_\rho$的指示随机变量；根据定义，$T_C^{i-1}|_\rho$是一个不读取种子的常值电路。因此，它属于以下两种情况之一：

- 假设 $T_C^{i-1}|_\rho \equiv$为 True。我们还知道，电路 $\mathsf{EQ}(T_C^{i-1}|_\rho, 1)$ 接收 $x \in \{0,1\}^b$时，当且仅当 $T_C^{i-1}(x) = 1$时输出 1，也与 True 函数等价。根据定义可以证明

$$\mathbb{E}_\eta[X_{i-1}|_\rho] = \mathsf{P}_\eta(\mathsf{EQ}(T_C^{i-1}|_\rho, 1)) = 1,$$

  其中第二个不等式由 Boundary Axiom得出。这与方程（4.15）矛盾。

- 否则，$T_C^{i-1}|_\rho \equiv \mathsf{Null}$。令 $\rho = (y_1, \ldots\ldots, y_{i-1}, *, y_{i+1}, \ldots\ldots, y_m)$。回想一下，由于 C的个体次数至多为 d，存在一个多项式 $p \in \mathbb{F}[x]$ 使得 $p \equiv C(y_1, \ldots\ldots, y_{i-1}, \cdot, z_{i+1}, \ldots\ldots, z_m)$。由 $T_C^{i-1}|_\rho \equiv \mathsf{Null}$ 和方程（4.15）可得

$$p(z_i) = C(y_1, \ldots, y_{i-1}, z_i, z_{i+1}, \ldots, z_m) \neq 0,$$

因此 p是一个非零多项式。根据命题4.2，它至多有 d个根。此外，由于$T_C^{i-1}|_\rho$ 的输入长度为 $b \in \mathsf{LogLog}$，我们可以根据命题3.12 和暴力计数引理证明

$$\mathbb{E}_\eta[X_i|_\rho] \le \mathsf{P}_\eta(T_C^i) + 2\eta \le d/|\mathbb{F}| + 4\eta.$$

这与方程（4.15）矛盾。

最后，由于 $T_C^0 \equiv \mathsf{Null}$，我们知道 $\mathbb{E}_\eta[X_0] \le 10\eta$。通过对 i 进行归纳（使用 n-Induction Axiom）和方程（4.14），我们可以证明

$$\mathbb{E}_\eta[X_m] \le md/|\mathbb{F}| + 10\eta \cdot (m+1). \tag{4.16}$$

随后，我们有

$$\begin{aligned}
\mathsf{P}_\delta(T_C) &\le \mathsf{P}_\eta(T_C) + \delta + 2\eta && \text{(Precision Consistency Axiom)}\\
&\le \mathsf{P}_\eta(T_C^m) + \delta + 5\eta && \text{(全局一致性)}\\
&\le \mathbb{E}_\eta(X_m) + \delta + 8\eta && \text{(Proposition 3.12)}\\
&\le md/|\mathbb{F}| + \delta + 10\eta \cdot (m+1) + 8\eta\\
&\le md/|\mathbb{F}| + \delta + \beta,
\end{aligned}$$

其中，最后一个不等式是通过取 $\eta \triangleq \beta/(10m+20)$ 得出的。 □

4.3 线性哈希

线性哈希函数 $x \mapsto Ax \bmod 2$ 是最简单的哈希函数构造之一。以下定理将线性哈希形式化为一种（近似）通用哈希函数。

定理 4.5 (线性哈希的通用性)。 APX_1 证明以下命题。设 $n, m, \delta^{-1}, \beta^{-1} \in \mathsf{Log}$。对于每个 $x, y \in \{0,1\}^n$，令 $T_{x,y}\colon \{0,1\}^{nm} \to \{0,1\}$ 为如下电路：将输入解析为布尔矩阵 $A \in \{0,1\}^{m\times n}$，当且仅当 $Ax \equiv Ay \pmod 2$时输出 1 。那么，对于所有互不相同的 $x, y \in \{0,1\}^n$，$\mathsf{P}_\delta(T_{x,y}) \le \delta + \beta + (1/2+\beta)^m$。

证明。 我们在 APX_1 中进行论证。固定 $n, m, \delta^{-1}, \beta^{-1} \in \mathsf{Log}$、 $x, y \in \{0,1\}^n$，并令 $T_{x,y}$为上文定义的电路。假设 $x \neq y$。我们将证明 $\mathsf{P}_\delta(T_{x,y}) \le \delta + \beta + (1/2+\beta)^m$。

我们首先给出 $m = 1$ 时概率的上界。令 $\eta^{-1} \in \mathsf{Log}$ 为一个待定参数，并令 $C\colon \{0,1\}^n \to \{0,1\}$ 是这样一个电路：给定 $c \in \{0,1\}^n$，它输出 $\langle c,\ x - y\rangle$ 模 2。我们将证明 $\mathsf{P}_\eta(\neg C) \le 1/2 + 6\eta$。

反设$\mathsf{P}_\eta(\neg C) > 1/2 + 6\eta$。由于 $x \neq y$，存在一个索引 $i \in [n]$ 使得 $x_i \neq y_i$。固定该索引 i。令 X 为 $\neg C$的指示随机变量；根据命题3.12，我们知道 $\mathbb{E}_\eta[X] > 1/2 + 6\eta - 3\eta = 1/2 + 3\eta$。接下来，根据期望的平均论证，存在一个赋值 ρ，赋给随机种子的第 i位以外的所有比特，使得 $\mathbb{E}_\eta[X|_\rho] > 1/2$。然而，由于 $X|_\rho$ 的种子长度为 **1**，且概率为 $1/2$，这与暴力计数引理矛盾。

令 $C^{\vee m}\colon \{0,1\}^{nm} \to \{0,1\}$ 表示电路 $C^{\vee m}(x_1, \ldots, x_m) \triangleq \bigvee_{i\in[m]} C(x_i)$。根据 单边误差归约引理，我们有

$$\mathsf{P}_\eta(\neg C^{\vee m}) \le (1/2 + 8\eta)^m + 2\eta.$$

可以观察到， $\neg C^{\vee m}$ 与 $T_{x\text{函数等价}y}$，因此根据近似计数的全局一致性，

$$\mathsf{P}_\eta(T_{x,y}) \le \mathsf{P}_\eta(\neg C^{\vee m}) + 3\eta \le (1/2 + 8\eta)^m + 5\eta.$$

根据 Precision Consistency Axiom，我们有

$$\mathsf{P}_\delta(T_{x,y}) \le \mathsf{P}_\eta(T_{x,y}) + \delta + 2\eta \le (1/2 + 8\eta)^m + \delta + 7\eta.$$

取 $\eta \triangleq \beta/20$ 时，证明即告完成。 □

4.4 针对 AC^0 电路的奇偶性下界

本节的第一个结果，是在 APX_1 中对奇偶函数 $\oplus_n$ 相对于 AC^0 的一个平均情形下界进行形式化。我们的证明基于 Furst、Saxe 和 Sipser [FSS84] 提出的一种技巧。此前，由 M¨uller 和 Pich [MP20]（沿用 [FSS84] 的方法）以及 Kraj´ıˇcek[Kra95 定理 15.2.3]（沿用 Razborov 对切换引理 [Raz95] 的证明）给出的该下界形式化，都需要 $\mathsf{APC}_1 = \mathsf{PV}_1$ +dWPHP(PV)[19] 理论。

定理 1.6（平均情况 AC^0 下界 $\oplus_n$ 在 APX_1中）。对于所有常元 k、$d \geq 1$，存在一个常元 $n_0 \geq 1$，使得 APX_1 证明以下陈述。设 n、δ^{-1}、$\beta^{-1} \in \mathsf{Log}$、$n > n_0$和$C$：$\{0,1\}^n \to \{0,1\}$是一个规模至多为 n^k 的 AC^0_d电路。设 T_C：$\{0,1\}^n \to \{0,1\}$ 是这样一个电路：给定 $x \in \{0,1\}^n$，当且仅当 $C\ (x) = \oplus_n\ (x)$ 时输出 1。那么

$$\mathsf{P}_\delta(T_C) \leq \frac{1}{2} + \frac{1}{n^k} + \delta + \beta. \tag{1.1}$$

主要的技术挑战在于避免依赖 dWPHP（PV）的“基于编码的计数论证”，因为 APX_1中无法使用它。基于编码的计数论证同时用于 [MP20]以及 Razborov 的 [Raz95] 切换引理证明。Agrawal 等人对此作了部分处理 [AAI+01]（另见 [Agr01]）[20]，，他们提出了一种确定性多项式时间算法，该算法根据切换引理输出一个合适的限制。作为我们的贡献之一，我们证明 Agrawal 等人 [AAI+01] 中的算法的正确性可以在 PV_1 中得到证明。结合第 3 节中开发的工具，我们得以在 $\boldsymbol{APX}_1$中形式化平均情况下界。

有趣的是，利用相同的技术，我们进一步证明 最坏情况下界 $\oplus_n \notin \mathsf{AC}^0$ 可以在 PV_1中形式化。这解决了 [MP20]中的一个开放问题。

定理 1.7（最坏情况 AC^0 针对 $\oplus_n$ 在 PV_1中的下界）。对于所有常元 k、$d \geq 1$，存在一个常元 $n_0 \geq 1$，使得 PV_1 证明以下陈述。对于每个 $n \in \mathsf{Log}$、$n > n_0$和 AC^0_d 电路C：$\{0,1\}^n \to \{0,1\}$ 其大小至多为 n^k，都存在一个字符串 $x \in \{0,1\}^n$，使得 $C\ (x) \neq \oplus_n\ (x)$。

记号。我们令 n 表示输入变量的数量。k-合取范式是形式为$C_1 \wedge C_2 \wedge \cdots \wedge C_m$的命题公式，其中每个子句 C_i都是至多含有 k个文字的析取，也就是说，由变量或其否定构成。类似地，k-析取范式是若干项的析取，其中每一项都是至多含有 k 个文字的合取。如果一个公式是 k-合取范式或 k-析取范式，我们就称它为 k-范式。k-范式中的子句[21] C 可由其类型（即 $\wedge$或 $\vee$）及两个大小为 $|S^+_C| + |S^-_C| \leq k$的子集 S^+_C，$S^-_C \subseteq [n]$ 来描述，其中 S^+_C 表示子句中变量的标识符，S^-_C 表示子句中变量否定的标识符。令 $S_C \triangleq S^+_C \cup S^-_C$。

注意，我们不妨假设 $S^+_C \cap S^-_C = \varnothing$，否则该子句要么恒为 0，要么恒为 1。

为简单起见，我们不妨假设 AC^0 电路满足以下性质：

- 该电路是分层的，也就是说，每一层中的门仅由前一层中的门馈入。
- 所有否定门都被移到输入变量的正上方。等价地，电路内部没有否定门，也就是说，第一层中的门可以由文字馈入，即输入变量或其否定。

满足这些性质的 AC^0 电路称为良构电路。请注意，任意 AC^0 电路都可以转换为良构电路，且只需付出多项式规模开销；该转换的正确性可在 PV_1 中证明。为简化计算，我们直接从良构电路开始。

---

[18]这两个结果都只考虑最坏情形下界，但可以验证，经过适当形式化后，类似的论证也能推出平均情形下界（采用 Je˘r´abek [Je˘r05, Je˘r07a] 的方法）。[19]注意，这两个结果都自动给出了 PV_1 +rWPHP(PV) 中最坏情形下界的形式化，因为 APC_1 is$\forall\Sigma^b_1$ 相对于 PV_1 +rWPHP(PV) 是保守的 [Je˘r04, Je˘r07a]，而最坏情形下界可以形式化为一个 $\forall\Sigma^b_1$-句子（例如，参见 [MP20, Theorem 1.1]）。[20]如 [AAI+01] 中所述，Ajtai 和 Wigderson 已知晓这一结果（尚未发表）。[21]在 k-NF 的语境中，我们用“子句”指代子公式，而不论其联结词为何。

4.4.1 针对限制的子集确定性选择

我们先陈述两个引理，它们形式化了 Furst、Saxe 和 Sipser 证明中用到的核心组合性质 [FSS84]。类似的函数也被隐式地用于 [AAI+01]。这里，我们使用势函数，通过条件期望法实现去随机化。这种方法同时提供了一个可行算法和一个可行证明。

引理 4.6（小集合的势函数）。 以下命题可在PV_1 中对每个常元$c \geq 1$证明。令 $n, t \in \mathsf{Log}$ 满足 $t \leq n$, $s, m \in \mathsf{LogLog}$, $s \leq m$, $p \triangleq t/n \in \mathbb{Q}$，且 $S_1, \ldots, S_m \subseteq [n]$ 为大小至多为 c 的两两不相交集合，并满足 $pc < 1$。存在一个电路 Φ_{s}：$\{*, \circ\}^{\leq n} \to \mathbb{Q} \cap [0,1]$，使得以下结论成立。

- （初始条件）。 $\Phi_{\mathsf{s}}(\varepsilon) \leq m^s (pc)^{m-s}$。
- （递归条件）。对于每个 $x \in \{*, \circ\}^i$, $i < n$，都有

$$\Phi_{\mathsf{s}}(x) = p \cdot \Phi_{\mathsf{s}}(x*) + (1-p) \cdot \Phi_{\mathsf{s}}(x\circ).$$

- （终止条件）。对于每个 $x \in \{*, \circ\}^n$, $\Phi_{\mathsf{s}}(x) \in \{0, 1\}$。此外，设 $T_x \triangleq \{i \in [n] \mid x_i = \circ\}$。那么 $\Phi_{\mathsf{s}}(x) = 0$ 当且仅当存在至少 s 个子集 $S \in \{S_1, \ldots, S_m\}$ 满足 $S \subseteq T_x$。

证明概要。 我们在 PV_1 中进行论证。令 $n, t, s \in \mathsf{Log}$、$m \in \mathsf{LogLog}$、$p \triangleq t/n$ 和 $S_1, \ldots, S_m \subseteq [n]$。电路$\Phi_{\mathsf{s}}$ 定义如下：给定某个 $0 \leq i \leq n$ 的 $x \in \{*, \circ\}^i$，令 $T_x \triangleq \{j \leq i \mid x_j = \circ\}$。它输出

$$\Phi_{\mathsf{s}}(x) \triangleq \sum_{\alpha \subseteq [m], |\alpha| < s} \phi(x, \alpha),$$

其中

$$\phi(x,\alpha) \triangleq \begin{cases} 0 & \exists j \in \alpha \; \exists k \in [i] \; (k \in S_j \wedge x_k = *) \\ \displaystyle\prod_{j \in [\alpha]} (1-p)^{|S_j \setminus T_x|} \prod_{j' \in [m] \setminus \alpha} \psi(x, j') & \text{otherwise} \end{cases},$$

$$\psi(x,j') \triangleq \begin{cases} 1 & \exists k \in [i] \; (k \in S_{j'} \wedge x_k = *) \\ 1 - (1-p)^{|S_{j'} \setminus T_x|} & \text{otherwise} \end{cases}.$$

为便于理解，我们提及这些函数的组合解释（这并非 PV_1 证明的一部分）：给定任意 $x \in \{*, \circ\}^i$，我们以概率 p 独立地将 $x_{i+1}, \ldots, x_n$ 随机赋给 $*$，并以概率 $1-p$赋给 $\circ$。令 $T'_x \triangleq \{i \in [n] \mid x_i = \circ\}$。那么

- $\psi(x, j')$ 是 $S_{j'} \not\subseteq T'_x$ 的概率。
- $\phi(x, \alpha)$是 $S_j \subseteq T'_x$ 当且仅当 $j \in \alpha$的概率。
- $\Phi_{\mathsf{s}}(x)$是至多 $s-1$ 个子集 $S \in \{S_1, \ldots, S_m\}$ 满足 $S \subseteq T_x$的概率。

我们回到PV_1 证明。递归条件和终止条件可以通过繁琐但直接的计算加以验证，此处我们将其省略。为证明初始条件，注意到

$$\begin{aligned} \psi(\varepsilon, j') &= 1 - (1-p)^{|S'_j|} \leq 1 - (1-p)^c \leq pc \\ \phi(\varepsilon, \alpha) &\leq \prod_{j' \in [m] \setminus \alpha} \psi(\varepsilon, j') \leq (pc)^{m - |\alpha|} \\ \Phi_{\mathsf{s}}(\varepsilon) &\leq \sum_{0 \leq j < s} \binom{m}{j} (pc)^{m-j} \leq m^s (pc)^{m-s} \end{aligned}$$

该论证可以在 PV_1 中实现，这是因为 $s, m \in \mathsf{LogLog}$ 且 c 为常元。至此证明完成。

□

引理 4.7（一般集合系统的势函数）. 对常元 k、$c \geq 1$ 的每一种选取，都存在常元b、$n_0 \geq 1$，使得下述语句在 PV_1 中可证。设 n、t、$m \in \mathsf{Log}$、$n > n_0$、$p \triangleq t/n \in \mathbb{Q}$ 以及S_1、S_2、……、$S_m \subseteq [n]$ 为大小至多为 c 的非空子集。则存在电路 $\Phi\colon \{*,\circ\}^{\leq n} \to \mathbb{Q} \cap [0,1]$，使得下述结论成立。

- (初始条件)。如果 $t \leq \sqrt{n}$，那么 $\Phi(\varepsilon) \leq n^{-k}$。
- (递归条件)。对于每个 $x \in \{*,\circ\}^i$、$i < n$，都有

$$\Phi(x) = p \cdot \Phi(x*) + (1-p) \cdot \Phi(x\circ).$$

- (终止条件)。对于每个 $x \in \{*,\circ\}^n$、$\Phi(x) \in \{0,1\}$。此外，对于 $T_x \triangleq \{i \in [n] \mid x_i = \circ\}$，如果 $\Phi(x) = 0$，则以下条件之一成立：

  1. $|S_1 \cup S_2 \cup \cdots \cup S_m \setminus T_x| \leq b$。*2.* 存在互不相交的非空集合 V_1、…、$V_\ell \subseteq [n]$，它们是 ℓ 的子集，且属于 S_1、…、S_m 中不同的集合，并且对于每个 $i \in [\ell]$，都有 $V_i \subseteq T_x$，其中 $\ell \geq k \ln n$。

此外，给定 S_1、…, S_m 和 $x \in \{*,\circ\}^n$，可以通过一个 PV 函数得到这些互不相交的集合 V_1、…, V_ℓ。

证明。固定任意常元 k，$c \geq 1$ 并令 b，$n_0 \geq 1$ 为稍后确定的常元。我们在 PV_1 中进行论证。固定 n，t，$m \in \mathsf{Log}$、$p \triangleq t/n$ 和 S_1，…，$S_m \subseteq [n]$。

不相交集分解。考虑以下迭代算法：令 $\mathcal{U}_0 \leftarrow \{S_1, \ldots, S_m\}$。在第 i 步中，其中 $i \geq 1$，我们选择一个极大集合 $\mathcal{V}_i \subseteq \mathcal{U}_{i-1}$，使得 $\mathcal{V}_i$ 中的集合两两不相交，并按如下方式计算 $\mathcal{U}_i$：

- 令 $\mathcal{U}_i \leftarrow \varnothing$。对于每个 $S \in \mathcal{U}_{i-1}$，若该集合非空，我们就将 $S \setminus (\bigcup_{S \in \mathcal{V}_i} S)$ 纳入 $\mathcal{U}_i$。

注意，$\mathcal{U}_i$ 中剩余的每个集合都必须是某个 S_1，…，S_m 的子集。此外，其大小至多为 $c - i$，因为极大集合 $\mathcal{V}_i$ 与 $\mathcal{U}_{i-1}$ 中的每个集合都有交集（否则它就不是极大的）。如果一次迭代中没有集合被加入 $\mathcal{U}_i$，算法就会终止。

设 $d \leq c$ 与 $\mathcal{V}_1, \ldots, \mathcal{V}_d$ 为由该算法得到的集合。可以证明，$\mathcal{V}_1, \ldots, \mathcal{V}_d$ 中各集合的并覆盖 $S_1 \cup \cdots \cup S_m$。此外，可以验证，对每个 $i \in [d]$ 与 $V_1, \ldots, V_\ell \in \mathcal{V}_i$，存在互不相同的 $i_1, \ldots, i_\ell \in [m]$，使得 $V_1 \subseteq S_{i_1}, \ldots, V_\ell \subseteq S_{i_\ell}$。

宽情形。我们首先考虑如下情形：对某个 $i \in [d]$，$\mathcal{V}_i$ 至少包含 $\ell \triangleq 2k \ln n$ 个集合。Fix i 为满足该条件的最小数。设 $V_1, \ldots, V_\ell$ 为 $\mathcal{V}_i$ 中的前 ℓ 个集合。设 $\Phi_s(x)$ 为引理 4.6 中关于 $V_1, \ldots, V_\ell$ 与 $s \triangleq \ell/2$ 的势函数（注意 $\ell \in \mathsf{LogLog}$）。我们定义 $\Phi(x) \triangleq \Phi_s(x)$。

接下来只需验证所要求的三个性质成立。

- (初始条件)。根据引理 4.6，我们知道

$$\Phi(\varepsilon) \leq \ell^{\ell/2} \cdot (pc)^{\ell/2} \leq \left(\frac{bkc \ln n}{\sqrt{n}}\right)^{\ell/2} \leq n^{-k},$$

其中我们假设选取了 $b \geq 2$，且 n 足够大；将 n_0 设为一个较大的常元即可确保这一点。

- (递归条件)。这可由引理 4.6中的递归条件推出。
- （终止条件）。对于 $x \in \{*,\circ\}^n$，根据引理 4.6，$\Phi(x) \in \{0,1\}$。令 $T_x \triangleq \{i \in [n] \mid x_i = \circ\}$。假设 $\Phi(x) = 0$。我们知道，在 V_1、……、V_ℓ 中，至少有 $\ell/2 \geq k \ln n$ 个集合 V 满足 $V \subseteq T_x$。这满足第二个终止条件。此外，给定 S_1、……、S_m 和 $x \in \{*,\circ\}^n$，可以使用构造 $\mathcal{V}_1$、……、$\mathcal{V}_d$ 的算法，通过一个 PV 函数得到这 $k \ln n$ 个集合。

窄情形。现在我们考虑这样的情形：对于每个 $i \in [d]$，都有 $\mathcal{V}_i \le 2k \ln n$ 个集合。注意， $\mathcal{V}_1$、……、 $\mathcal{V}_d$ 中各集合的并覆盖了 $S_1 \cup \cdots \cup S_m$。我们知道

$$|S_1 \cup \cdots \cup S_m| = \left| \bigcup_{i \in [d]} \bigcup_{V \in \mathcal{V}_i} V \right| \le d \cdot (2k \ln n) \cdot c \le 2kc^2 \ln n.$$

回顾一下， $b \ge 1$ 是一个待确定的常元。令 $S \triangleq S_1 \cup \cdots \cup S_m$。我们将势函数$\Phi(x)$定义如下。给定 $x \in \{*, \circ\}^i$ 且满足 $i < n$，令 $q^* \triangleq |\{j \in [i] \cap S \mid x_j = *\}|$、 $q^\circ \triangleq |\{j \in [i] \cap S \mid x_j = \circ\}|$和 $q^\diamond \triangleq |S| - q^* - q^\circ$。那么

$$\Phi(x) \triangleq \sum_{j=\max\{b+1, q^*\}}^{|S|-q^\circ} \binom{q^\diamond}{j-q^*} p^{j-q^*} (1-p)^{q^\diamond - j + q^*}. \tag{4.17}$$

为便于理解，我们说明该函数的组合解释如下。我们独立地将 x_{i+1}、……、 x_n 以概率 p 赋值为 $*$，并以概率 $1-p$赋值为 $\circ$。那么，$\Phi(x)$表示满足 $x_j = *$ 的索引 $j \in [n] \cap S$ 的数量至少为 $b+1$的概率。组合解释并非PV_1 证明的一部分。

注意到 $\Phi(x) \ge 0$ 因为每一项均非负，且 $\Phi(x) \le 1$ 由二项式定理可得。只需验证所要求的三个性质。

- (初始条件). 注意到

$$\Phi(\varepsilon) \le \sum_{j=b+1}^{|S|} \binom{|S|}{j} p^j \le \sum_{j=b+1}^{|S|} |S|^j p^j \le \sum_{j=b+1}^{|S|} \left(\frac{2kc^2 \ln n}{\sqrt{n}} \right)^j \le n^{-k},$$

其中，当我们将 $b \ge 10k$ 和 n_0 设为足够大时，最后一个不等式成立。

- (递归条件)。任取满足 $i < n$ 的 $x \in \{*, \circ\}^i$，我们考虑 $i+1 \in S$ 是否成立。若不成立，则有 $\Phi(x) = \Phi(x*) = \Phi(x\circ)$，且方程成立。否则，令 $q^* \triangleq |\{j \in [i] \cap S \mid x_j = *\}$、$q^\circ \triangleq \{j \in [i] \cap S \mid x_j = \circ\}$ 和 $q^\diamond \triangleq |S| - q^* - q^\circ$。我们可以看到

$$\Phi(x*) \triangleq \sum_{j=\max\{b+1, q^*+1\}}^{|S|-q^\circ} \binom{q^\diamond - 1}{j-q^*-1} p^{j-q^*-1} (1-p)^{q^\diamond - j + q^*};$$

$$\Phi(x\circ) \triangleq \sum_{j=\max\{b+1, q^*\}}^{|S|-q^\circ-1} \binom{q^\diamond - 1}{j-q^*} p^{j-q^*} (1-p)^{q^\diamond - 1 - j + q^*}.$$

由方程（3.45）可得 $\Phi(x) = p \cdot \Phi(x*) + (1-p) \cdot \Phi(x\circ)$。

- （终止条件）。对于 $x \in \{*, \circ\}^n$，令 q^*，q°，$q^\diamond$ 如上定义。我们有 $q^\diamond = 0$ 和$q^* + q^\circ = |S|$。在这种情况下，可以观察到，如果 $q^* > b$，那么 $\Phi(x) = 1$；否则， $\Phi(x) = 0$。此外，根据 q^* 的定义，我们知道，如果 $\Phi(x) = 0$，对于 $T_x \triangleq \{i \in [n] \mid x_i = \circ\}$，则有$|S \setminus T_x| = q^* \le b$。这满足第一个终止条件。

证明至此完成。 □

现在我们可以陈述子集选择引理了。

引理 4.8（子集选择引理）。对于每个 k、$c \ge 1$，都存在常元 b、$n_0 \ge 1$，使得以下命题可在PV_1中证明。令 n、 t、 $\ell \in \mathsf{Log}$、 $n > n_0$、 $\ell \le n^k$ 以及 F_1、 F_2、 …、 F_ℓ 为定义在 n 个输入变量上的 c-NF。若 $t \le \sqrt{n}$，则存在一个子集 $T \subseteq [n]$，其大小至多为 $n-t$，使得对于每个 $i \in [\ell]$，以下条件至少有一个成立。

- 如果我们为每个 $j \in T$ 固定第 j 个变量， F_i 至多由 b 个文字输入。

- 存在 $m' \geq k \ln n$ 个互不相交的非空子句 $C'_1, \ldots, C'_{m'}$，使得：*(1)* 每个 C'_j 都是 F_i 中不同子句的子子句；*(2)* $S_{C'_j} \subseteq T$。

此外，对于每个 i，子集 T 和子句 $C'_1, \ldots, C'_m$ 都由一个 PV 函数根据 $F_1, \ldots, F_\ell$ 以及 $1^n, 1^t, 1^\ell$ 计算得出。

证明。任取 $k, c \geq 1$，并令 $b, n_0 \geq 1$ 稍后确定。我们在 PV_1 中进行论证。固定 $n, t \in$ 个 Log、$\ell \leq n^k$、$p \triangleq t/n$ 和 c-NF $F_1, \ldots, F_\ell$，它们定义在 n 个变量上。

任取 $i \in [\ell]$。假设 F_i 有 m_i 个子句，并令 C_{ij} 为 j-个子句，属于 F_i。令 $S_{ij} \triangleq S_{C_{ij}}$ 为变量的子集，其中这些变量或其否定输入 C_{ij}。对于每个 $i \in [\ell]$，考虑集合 $S_{i1}, \ldots, S_{im_i}$；根据引理 4.7 (用 $3k$ 代替 k)，存在常元 b', n'_0 和势函数 $\Phi_i \colon \{*, \circ\}^{\leq n} \to \mathbb{Q} \cap [0, 1]$，使得以下条件成立。

- (初始条件）。 $\Phi_i(\varepsilon) \leq n^{-3k}$;
- (递归条件）。 $\Phi_i(x) = p \cdot \Phi_i(x*) + (1-p) \cdot \Phi_i(x\circ)$ 。
- (终止条件）。对于 $x \in \{*, \circ\}^n$， $\Phi_i(x) \in \{0, 1\}$。此外，设 $T_x \triangleq \{i \in [n] \mid x_i = \circ\}$。如果$\Phi_i(x) = 0$，则以下两个条件之一成立：

  1. $|S_{i1} \cup \cdots \cup S_{im_i} \setminus T_x| \leq b$。这实际上意味着，如果我们为每个 $j \in T_x$ 固定第 j 个变量，那么F_i 至多由 b 个文字构成。2. 存在互不相交的非空集合 V_1、……、$V_{\ell_i} \subseteq [n]$，它们是S_{i1}、……、S_{im_i} 中 ℓ_i 个不同集合的子集，并且对于每个 $i \in [\ell]$， $V_i \subseteq T_x$，其中 $\ell_i \geq 3k \ln n \geq k \ln n$。这意味着存在 $m' = \ell_i \geq k \ln n$ 个互不相交的子句 C'_1、……、$C'_{m'}$，每个子句都是 F_i中某个子句的子子句，并且 $S_{C'_j} \subseteq T$。

Th因此，如果 $\Phi_i(x) = 0$，那么只要选择 $T \triangleq T$，该子句就满足所需的性质 x.

考虑如下势函数 $\Phi(x)$。给定任意 $x \in \{*, \circ\}^i$、$i \leq n$，令 q° 为 x 中 $\circ$ 的数量。我们定义

$$\Phi(x) \triangleq q^\circ + (1-p)(n-i) + n \cdot \sum_{i \in [\ell]} \Phi_i(x).$$

我们可以证明 $\Phi(x)$满足以下条件：

- (初始条件). $\Phi(\varepsilon) \leq (1-p)n + n \cdot \ell \cdot n^{-3k} < (1-p)n + 1$.
- (递归条件)。 $\Phi(x) = p \cdot \Phi(x*) + (1-p) \cdot \Phi(x\circ)$。
- (终止条件)。对于 $x \in \{*, \circ\}^n$， $\Phi(x)$ 是一个整数。此外，如果我们选择 $T = T_x = \{i \in [n] \mid x_i = \circ\}$，那么 $\Phi(x)$ 至多为以下两项之和：(1) x 中 $*$的数量；(2) n 乘以违反所需性质的 c-NF F_i 的数量。特别地，若 $\Phi(x) \leq (1-p)n$，则 $T = T_x$ 是一个所需的子集。

剩下的任务是构造 $x \in \{*, \circ\}^n$，使得 $\Phi(x) \leq (1-p)n$。事实上，可以通过贪心算法得到它：从 $x \leftarrow \varepsilon$ 开始，将 $*$ 或 $\circ$ 追加到 x，以使 $\Phi(x)$ 最小。根据 i 进行归纳，可以证明，算法执行第 i 轮后得到的字符串 $x \in \{*, \circ\}^{\leq i}$ 满足 $\Phi(x) \leq \Phi(\varepsilon) < (1-p)n + 1$。由于该性质可以通过一个直接的多项式时间算法验证，因此这在 PV_1 中是可实现的。最后，经过 n 轮后得到的字符串 $x \in \{*, \circ\}^n$ 满足 $\Phi(x) \leq (1-p)n$，因为它必定是一个小于 $(1-p)n + 1$ 的整数。证明完毕。 □

4.4.2 APX 中的平均情况下界$_1$

我们称部分赋值 ρ 使……平凡化一个 NF F，如果应用 ρ后， F 是一个常值函数。注意，对于每个包含非恒定子句 C 的 NF F，都存在一个对 C 中的变量所作的赋值，可以使 F平凡化。

引理 4.9 (随机限制引理)。对于每个 k、c、$b \in \mathbb{N}$，都存在一个 $n_0 \geq 1$，使得以下命题可在 APX_1 中证明。设 n、t、$\ell \in$ Log、$n > n_0$。设 F_1、…、F_ℓ 是关于 n 个输入变量的 *c-NF*，且 $T \subseteq [n]$ 是一个大小为 $n - t$ 的子集，使得对于每个 $i \in [\ell]$，以下条件至少有一个成立。

- (窄)。如果我们同时固定所有索引属于 T 的变量，那么 c-*NF* F_i 至多由 b 个文字决定。

- (宽)。存在 $m_i' \geq k \ln n$ 个（显式给出的）非空且互不相交的子句 $C'_{i,1}, \ldots, C'_{i,m_i'}$，满足：*(1)* 每个 $C'_{i,j}$ 都是 F_i 中不同子句的子子句；*(2)* 对每个 $j \in [m_i']$，$S_{C'_{i,j}} \subseteq T$。

设 Y 为 $\{0,1\}$ 上的随机变量：它取长度为 n 的种子 x，将其解析为对 T 中变量的赋值 ρ（即，对每个 $i \in T$，它将第 i 个变量固定为 x_i），并且当且仅当在应用 ρ 后，$F_1, \ldots, F_\ell$ 中至少有一个既未被平凡化，也不至多依赖 b 个文字时，输出 1。那么对每个 δ^{-1}，$\beta^{-1} \in \mathsf{Log}$

$$\mathbb{E}_\delta[Y] \leq \ell \cdot (1 - 2^{-c} + \beta)^{k \ln n} + \delta + \beta.$$

证明。我们在 APX_1 中论证。固定 $k, c, b \in \mathbb{N}$，并令 $n_0 \geq 1$ 为待确定的常元。固定 $n, t, \ell \in \mathsf{Log}, F_1, \ldots, F_\ell$，以及 $T \subseteq [n]$。令 $\eta^{-1} \in \mathsf{Log}$ 为稍后确定的参数。

为简单起见，我们假设 $F_1, \ldots, F_{\ell'}$ 是满足第二个条件的门，并令 $m_i' \geq k \cdot \ln n$ 表示互不相交的子句 $C'_{i,1}, \ldots, C'_{i,m_i'}$ 的数量。我们将在 $\{0,1\}$ 上定义具有 n 比特种子的随机变量如下。

- 对于每个 $i \in [\ell']$ 和 $j \in [m_i']$，X_{ij} 定义如下随机变量：令 $x \in \{0,1\}^n$ 为种子。当且仅当对每个 $r \in T$ 将第 r 个变量固定为 x_r 不会使 $C'_{i,j}$ 平凡化时，$X_{ij} = 1$。
- 对于每个 $i \in [\ell']$，令 $X_i = \prod_{j=1}^{m_i'} X_{ij}$。
- 注意，$Y \leq \bigvee_{i \in [\ell']} X_i$。

注意，每个 X_{ij} 读取其种子中的至多 $c \in \mathbb{N}$ 个比特。因此，根据 暴力计数引理，我们知道 $\mathbb{E}_\eta[X_{ij}] \leq 1 - 2^{-c} + 2\eta$。根据 乘法原理，我们有

$$\mathbb{E}_\eta[X_{i1} X_{i2} \ldots X_{im_i'}] \leq (1 - 2^{-c} + 2\eta)^{m_i'} + 8\eta \cdot m_i' \leq (1 - 2^{-c} + 2\eta)^{k \cdot \ln n} + 8\eta \cdot |F_i| \leq (1 - 2^{-c} + \beta)^{k \ln n} + 8\eta \cdot |F_i|,$$

其中，当 $\eta \leq \beta/2$ 时，最后一个不等式成立。根据 并集界，

$$\mathbb{E}_\eta[Y] \leq \sum_{i=1}^{\ell'} \mathbb{E}_\eta[X_i] + 3\eta \cdot \ell' \leq \ell \cdot (1 - 2^{-c} + \beta)^{k \ln n} + 8\eta \cdot \ell \cdot (2^c n^c) + 3\eta \cdot \ell.$$

该引理随即得证　　这是由 期望的精度一致性 得到的，只需令 $\eta \triangleq \beta/(20 \cdot \ell \cdot 2^c n^c)$ 即可。 □

现在我们可以证明关于 $\oplus_n$ 相对于 AC^0 的平均情形下界。

定理 1.6（平均情况 AC^0 下界：$\oplus_n$ 在 APX_1 中）。对于所有常元 k、$d \geq 1$，存在常元 $n_0 \geq 1$，使得 APX_1 证明以下陈述。设 n、δ^{-1}、$\beta^{-1} \in \mathsf{Log}$、$n > n_0$ 和 C：$\{0,1\}^n \to \{0,1\}$ 是一个大小至多为 n^k 的 AC^0_d 电路。设 T_C：$\{0,1\}^n \to \{0,1\}$ 为如下电路：给定 $x \in \{0,1\}^n$ 后，当且仅当 $C(x) = \oplus_n(x)$ 时输出 1。那么

$$\mathsf{P}_\delta(T_C) \leq \frac{1}{2} + \frac{1}{n^k} + \delta + \beta. \tag{1.1}$$

证明。我们在元理论中对 d 进行归纳，证明该命题对每个 k 都成立。常元 $n^{k_0}{}^d \geq 1$ 将在证明后续部分确定。在基础情形和归纳情形中，我们都在 APX_1 中进行论证。固定 $n, \delta^{-1}, \beta^{-1} \in \mathsf{Log}$ 和电路 C：$\{0,1\}^n \to \{0,1\}$。令 $\eta^{-1} \in \mathsf{Log}$ 为一个待后续确定的参数。

基础情形。假设 $d = 1$。为导出矛盾，假设方程（1.1）不成立。于是根据 Precision Consistency Axiom，我们有

$$\mathsf{P}_\eta(T_C) > \frac{1}{2} + \frac{1}{n^k} + (\beta - 2\eta). \tag{4.18}$$

注意，$\mathsf{Fix}_b(T_C)$ 是电路 $T_{\mathsf{Fix}_b\ (C)\ \oplus b}$。

我们首先证明，对于 $D\colon\ \{0,1\}^n \to \{0,1\}$，若 D 至多依赖其 $n-1$ 个输入位，则$\mathsf{P}_\eta(T_D) \le 1/2 + O(\eta)$。假设 D 不依赖第 i 个输入位。令 X_D 为 T_D 的指示随机变量，并令 ρ 为除第 i 个输入位之外， D所有输入位的任意赋值。根据暴力计数引理，有 $\mathbb{E}_\eta[X_D|_\rho] \le 1/2 + 2\eta$。随后，根据期望的平均论证，我们可以得出

$$\mathbb{E}_\eta[X_D] \le \frac{1}{2} + 2\eta + 3\eta \le \frac{1}{2} + 5\eta. \tag{4.19}$$

这意味着 $\mathsf{P}_\eta(T_D) \le 1/2 + 8\eta$，由命题 3.12可知。

现在假设 C 依赖其所有输入位，且深度至多为 $d = 1$。考虑以下迭代式 P-预言机算法。令 $C_0 \triangleq C$ 和 $s_0 \triangleq 0$。该算法维持如下不变式：第 i 轮之后， C_i 依赖其所有输入位。已知该不变式在第（$i-1$）轮之后成立，则存在 $b_i \in \{0,1\}$ 使得

- $\mathsf{Fix}_{b_i}(C_{i-1})$ 是一个常值电路；
- $\mathsf{Fix}_{1-b_i}(C_{i-1})$ 依赖于它的所有输入位。

Fix that $b_i \in \{0,1\}$. 随后，算法在第i轮中定义 $C_i \triangleq \mathsf{Fix}_{1-b_i}(C_{i-1}) \oplus (1-b_i)$ 和 $s_i \triangleq s_{i-1} \oplus (1-b_i)$，并保持不变式。

我们将对 $i \le n$ 进行归纳证明：

$$\mathsf{P}_\eta(T_{C_i \oplus s_i}) > \frac{1}{2} + \frac{2^i}{n^k} + (\beta - 8(i+1)\cdot\eta).$$

（注意， $n \in$Log 和 $i \le n$，因此归纳假设可以用一个 APX_1 中的开放公式来表示。）基础情形由方程（4.18）得出。假设该不等式对 $i < n$成立。注意到

$$\begin{aligned}
\mathsf{P}_\eta(T_{C_i \oplus s_i}) &\le \frac{\mathsf{P}_\eta(\mathsf{Fix}_{b_i}(T_{C_i}) \oplus s_i) + \mathsf{P}_\eta(\mathsf{Fix}_{1-b_i}(T_{C_i}) \oplus s_i)}{2} \qquad \text{(Precision Consistency Axiom)} \\
&= \frac{\mathsf{P}_\eta(T_{\mathsf{Fix}_{b_i}(C_i) \oplus s_i \oplus b_i}) + \mathsf{P}_\eta(T_{\mathsf{Fix}_{1-b_i}(C_i) \oplus s_i \oplus (1-b_i)})}{2} \\
&= \frac{\mathsf{P}_\eta(T_{\mathsf{Fix}_{b_i}(C_i) \oplus s_i \oplus b_i}) + \mathsf{P}_\eta(T_{C_{i+1} \oplus s_{i+1}})}{2} \\
&\le \frac{1}{2}\left(\frac{1}{2} + 8\eta + \mathsf{P}_\eta(T_{C_{i+1} \oplus s_{i+1}})\right).
\end{aligned}$$

（最后一个不等式成立，是因为 $\mathsf{Fix}_{b_i}(C_i)$ 是一个常值电路，因此并不依赖于它的所有输入位。）由此，根据归纳假设可得

$$\mathsf{P}_\eta(T_{C_{i+1} \oplus s_{i+1}}) > \frac{1}{2} + \frac{2^{i+1}}{n^k} + (\beta - 8(i+2)\cdot\eta).$$

我们取 $n_0 \in \mathbb{N}$ 充分大，使得 $2^{n-10}/n^k \ge 1$ 对每个 $n > n_0$都成立。因此，我们有$\mathsf{P}_\eta(T_{C_{n-10}}) > 3/2 + (\beta - 8(n+1)\cdot\eta)$, 其中 C_{n-10}的输入长度恰为 **10**，且它是一个深度为 **1** 的 AC^0 电路。根据 $\eta \triangleq \beta/(20n)$，这显然不可能，此处用到了暴力计数引理。

归纳情形。 假设该定理对 $d \in \mathbb{N}$成立。我们的目标是证明该定理对 $d+1$成立。令 $n^{k_{,0}\ d}$ 为与 d 和 k对应的定理常元 $n_0 \ge 1$。任取 $k \ge 1$，并令 $n^{k_{,0}\ d+1}$ 为一个待确定的常元。为导出矛盾，假设方程（1.1）不成立。那么根据 Precision Consistency Axiom，我们有

$$\mathsf{P}_\eta(T_C) > \frac{1}{2} + \frac{1}{n^k} + (\beta - 2\eta). \tag{4.20}$$

总体而言，我们将两次应用随机限制，把 C 转换为一个 AC^0_d 电路；该电路以高概率在较短的输入长度上计算奇偶函数。之后，我们可以应用归纳假设来完成证明。

限制 1。设 G_1，G_2，……，G_ℓ 是第一层中的门，也就是直接由文字输入的门。我们可以将它们视为 1-NF，因为每个文字都可以视为仅含一个文字的子句。设 $t \triangleq \sqrt{n}$。根据 子集选择引理，存在一个子集 $T_1 \subseteq [n]$，其大小至多为 $n-t$，使得对于每个门 G_i，以下条件之一成立。

- 如果我们固定 T_1 中的所有变量，G_i 至多由 b_1 个变量馈入，其中 $b_1 \in \mathbb{N}$ 是一个常元。
- G_i 至少有 $100k \cdot \ln n$ 个文字使用了 T_1 中的变量。

固定子集 $T_1 \subseteq [n]$。我们假设 $|T_1| = n-t$；如果不是，就向其中添加 $n-t-|T_1|$ 个任意元素。我们按如下方式定义 $\{0,1\}$ 上的随机变量，它们使用 n 个比特种子。

- 令 Y 为随机限制引理中的随机变量。也就是说，给定 $x \in \{0,1\}^n$，它将 x 解析为一个部分赋值 ρ，赋值对象是 T_1 中的变量；当且仅当至少有一个门既未被平凡化，也不依赖于至多 b 个文字（在应用 ρ 之后）时，输出 1。

- 令 Y_T 为 T_C 的指示随机变量。

根据随机限制引理 并利用 $c=1$，我们有

$$\mathbb{E}_\eta[Y] \le \ell \cdot (1/2+\eta)^{100k \ln n} + 2\eta \le n^{-8k},$$

其中，当 η 足够小时，且 n 足够大时（通过设置 $n^{k_{\cdot_0}^{d+1}} \in \mathbb{N}$），最后一个不等式成立。根据期望的平均论证，存在一个赋值 ρ_1，赋给 T_1 中的变量，使得

$$\mathbb{E}_\eta[Y_T|_{\rho_1}] - \mathbb{E}_\eta[Y|_{\rho_1}] \ge \frac{1}{2} + \frac{1}{n^k} + (\beta - 30\eta) - \frac{1}{n^{8k}} > 5\eta, \tag{4.21}$$

当 η 足够小时，最后一个不等式成立。

固定赋值 ρ_1。注意，$Y|_{\rho_1} \in \{0,1\}$，因为 Y 仅在 T_1 中读取其输入变量。因此，必有 $Y|_{\rho_1} = 0$。在这种情况下，应用 ρ_1 后，所有门要么被平凡化，要么至多由 b_1 个变量驱动，因此可以用扇入至多为 b_1 的门替换。

令 $\sigma_1 \triangleq \oplus_{n-t}$（$\rho_1$）、$n_1 \triangleq t$ 和 $C_1 : \{0,1\}^{n_1} \to \{0,1\}$ 为将赋值 ρ_1 应用于 C、将第一层中的每个门替换为一个等价的扇入至多为 b_1 的门，并将电路的输出与比特 σ_1 进行异或后得到的电路。注意，对于每个 $x \in \{0,1\}^{n_1}$，$C|_{\rho_1}(x) = C_1(x) \oplus \sigma_1$。此外，$C_1$ 的规模至多为 $n^k \le n_1^{2k}$。

设 $T_{C_1} : \{0,1\}^{n_1} \to \{0,1\}$ 为如下电路：给定 x，当且仅当 $C_1(x) = \oplus_{n_1}(x)$ 时输出 1。结果表明，$Y_T|_{\rho_1}$ 是 T_{C_1} 的指示随机变量；为看出这一点，注意到对除 T_1 之外所有变量的每一个赋值 x，$C(x \cup \rho_1) = \oplus_n(x \cup \rho_1)$ 当且仅当 $C|_{\rho_1}(x) = (\oplus_{n_1}(x)) \oplus \sigma_1$，其中 $C|_{\rho_1}(x) \oplus \sigma_1 = C_1(x)$。因此，由命题 3.12，我们有

$$\mathsf{P}_\eta(T_{C_1}) \ge \mathbb{E}_\eta[Y_T|_\rho] - 3\eta \ge \frac{1}{2} + \frac{1}{n^k} + (\beta - 33\eta) - \frac{1}{n^{8k}} \ge \frac{1}{2} + \frac{1}{n_1^{4k}} + (\beta - 33\eta),$$

其中，若 n 足够大（通过设定 $n^{k_{\cdot_0}^{d+1}} \in \mathbb{N}$），则最后一个不等式成立。

限制 2. 如上所述，C_1 的第一层中每个门的扇入至多为 b_1，因此 C_1 的第二层中的门计算 b_1-NF。设 $F_1, F_2, \ldots, F_{\ell_1}$ 为 b_1-NF，它们位于 C_1 的第二层。设 $t_1 \triangleq \sqrt{n_1}$。由子集选择引理 并适当选择参数，存在一个子集 $T_2 \subseteq [n]$，其大小至多为 $n_1 - t_1$，使得对每一个 $i \in [\ell_1]$，下列条件之一成立。

- 如果我们固定 T_2 中的所有变量，F_i 最多将取决于 b_2 个变量，其中 $b_2 \in \mathbb{N}$ 是一个常元。
- 有 $m_1' \ge 100k \cdot 4^{b_1} \cdot \ln n$ 个互不相交的 F_i 子子句，它们只使用来自变量的文字 T_2.

令 $n_2 \triangleq t_1$，并固定集合 $T_2 \subseteq [n]$。我们假设 $|T_2| = n_1 - t_1$；否则，就向其中添加 $n_1 - t_1 - |T_2|$ 个任意元素。我们在 $\{0,1\}$ 上定义如下随机变量，其比特种子为 n。

- 设 Y' 是 随机限制引理中的随机变量。也就是说，给定 $x \in \{0,1\}^n$，它将 x 解析为一个部分赋值 ρ，其赋值对象是 T_2 中的变量；当且仅当每个 b-NF 在应用 ρ 后都被化为平凡形式，或至多依赖 b_2 个文字时，输出 1。

- 设 Y'_T 是 T_{C_1}的指示随机变量。

根据随机限制引理，我们有

$$\mathbb{E}_\eta[Y'] \le \ell_1 \cdot (1 - 2^{-b_1} + \eta)^{100k \cdot 4^{b_1} \cdot \ln n} + 2\eta \le n_1^{-8k},$$

其中，当 η 充分小时且 n 充分大时（通过设置 $n^{k\cdot 4^{d+1}} \in \mathbb{N}$），最后一个不等式成立。根据期望的平均论证，存在一个赋值 ρ_2，将其赋给 T_2 中的变量，使得

$$\mathbb{E}_\eta[Y'_T|_{\rho_2}] - \mathbb{E}_\eta[Y'|_{\rho_2}] \ge \frac{1}{2} + \frac{1}{n_1^{4k}} + (\beta - 36\eta) - \frac{1}{n_1^{8k}} > 5\eta, \tag{4.22}$$

当 η 充分小时，最后一个不等式成立。

固定赋值 ρ_2。注意，由于它仅在 T_2 中读取其输入变量，因此 $Y'|_{\rho_2} \in \{0,1\}$。因此，我们必有 $Y'_{\rho_2} = 0$。在这种情况下，所有 b_1-范式（即 C_1 第二层中的门）要么被平凡化，要么至多由 b_2 个变量馈入。在这种情况下，我们可以如下将 C_1 转换为一个深度至多为 d 的等价电路。假设 $d \ge 2$（$d = 1$ 的情况留作练习）。对于第二层中的每个门 G，如果它未被平凡化，我们移除 G，并考虑第三层中原先由 G馈入的每个门 G'：

- 如果 G' 是一个与门，我们将 G 重写为大小至多为 $b_2 \cdot 2^{b_2}$ 的等价合取范式，并将其中的所有子句连接到 G'。
- 如果 G' 是一个或门，我们将 G 重写为大小至多为 $b_2 \cdot 2^{b_2}$ 的等价析取范式，并将其中的所有子句连接到 G'。

无论哪种情况，该电路都保持函数等价。

设 $\sigma_2 \triangleq \oplus_{n_1 - t_1}(\rho_2)$ 和 $C_2 : \{0,1\}^{n_2} \to \{0,1\}$ 是计算 $C_1|_{\rho_2}(x) \oplus \sigma_2$的深度为 d 的电路。当 n 足够大时（通过设置 $n^{k\cdot 4^{d+1}} \in \mathbb{N}$），$C_2$ 的大小会膨胀一个线性因子，该因子至多为 $O(n^k) \le n_2^{6k}$。设 $T_{C_2} : \{0,1\}^{n_2} \to \{0,1\}$ 是这样一个电路：给定 x，当且仅当$C_2(x) = \oplus_{n_2}(x_2)$时输出 1。与之前一样，$Y'_T|_\rho$ 是 T_{C_2}的指示随机变量。因此，我们有

$$\begin{aligned}
\mathsf{P}_\eta(T_{C_2}) &\ge \mathbb{E}_\eta[Y'_T|_\rho] - 3\eta && \text{(Proposition 3.12)} \\
&\ge \frac{1}{2} + \frac{1}{n_1^{4k}} + (\beta - 39\eta) - \frac{1}{n_1^{8k}} && \text{(Equation (4.22))} \\
&\ge \frac{1}{2} + \frac{1}{n_2^{6k}} + (\beta - 39\eta) \\
&> \frac{1}{2} + \frac{1}{n_2^{6k}} + 2\eta, && (4.23)
\end{aligned}$$

其中，最后两行在 n 足够大（令 $n^{k\cdot 4^{d+1}} \in \mathbb{N}$）且 η 足够小时成立。

现在我们得到了矛盾：$C_2 : \{0,1\}^{n_2} \to \{0,1\}$ 是一个深度为 d、大小至多为 n_2^{6k} 的电路，并且它以 $1/n_2^{6k}$ 的优势计算奇偶性。这违反了方程（1.1）。于是，根据深度为 d、大小为 n_2^{6k} 的归纳假设，定理便得证，只要根据 b_1，b_2，$n^{6k\cdot 4^d}$ 以及证明中所用不等式的要求，适当设置 $\eta^{-1} \in$Log 和 $n^{k\cdot 4^{d+1}} \in \mathbb{N}$。 □

4.4.3 PV$_1$ 中的最坏情况下界

首先，我们通过在 随机限制引理 中显式实现条件期望法，对其进行去随机化；该方法在 PV$_1$ 中实现。

引理 4.10 (去随机化限制引理)。对于每个 k、c、$b \in \mathbb{N}$，都存在一个 $n_0 \ge 1$，使得以下命题可在 PV$_1$ 中证明。令 n、t、$\ell \in$Log、$n > n_0$。令 F_1、……、F_ℓ 为关于 n 个输入变量的 c-*NF*，并令 $T \subseteq [n]$ 为大小为 $n - t$ 的子集，使得对于每个 $i \in [\ell]$，以下条件至少有一个成立。

- （窄）。如果我们为每个 $j \in T$固定第 j 个变量，那么 F_i 至多由 b 个文字决定。

- （宽）。存在 $m_i' \geq k \ln n$ 个（显式给出的）互不相交的子句 $C'_{i,\,1}$，……，$C'_{i,\,m_i'}$，满足：*(1)* 每个 $C'_{i,\,j}$都是 F_i 中不同子句的子子句；*(2)* 对每个 $j \in [m_i']$，$S_{C'_{i,\,j}} \subseteq T$。

假设 $\ell \cdot (1-2^{-c})^{k \ln n} < 1$。那么存在一个赋值 ρ，赋给 T中的变量，使得应用 ρ后，F_1、……、F_ℓ 中的每一个要么被平凡化，要么至多依赖 b个文字。

证明。我们在 PV_1中论证。令 $k, c, b \in \mathbb{N}$和 $n_0 \geq 1$为稍后确定的常元。取定 $n, t, \ell \in$个 Log,c-NF $F_1, \ldots, F_\ell$，以及 $T \subseteq [n]$。若一个 c-NF 在将限制 ρ应用于T 中的变量后，要么被平凡化，要么至多依赖 b 个文字，则称其为良好的。由于满足第一条的 c-NF 无论赋值 ρ为何都是良好的，因此不失一般性地，假设所有 c-NF 都满足第二条。我们将构造一个赋值 ρ，使所有这类 c-NF 都被平凡化。

为表述简便，我们假设 $T = \{1, 2, \ldots, n-t\}$。Fix任意 $i \in [\ell]$，并令$C'_{i,\,1}$，……，$C'_{i,\,m_i'}$为互不相交的子句子句，使得$S_{C'_{i,\,j}} \subseteq T$。对于前 $|x|$ 个变量的部分赋值 $x \in \{0,1\}^{\leq n-t}$，我们称：

- $C'_{i,\,j}$ 被正向确定，如果它是与门且其所有文字均被固定为1，或者它是或门且其所有文字均被固定为0。
- $C'_{i,\,j}$ 被负向确定，如果它是与门且其某个文字被固定为0，或者它是或门且其某个文字被固定为1。
- $C'_{i,\,j}$ 距正向确定 d-远，如果它未被负向确定，且恰好有 d个其文字仍未被固定。

我们如下定义 ϕ_{ij}，Φ_i，Φ：$\{0,1\}^{\leq n-t} \to \{0,1\}$。给定任意一个 $x \in \{0,1\}^{\leq n-t}$，它被解析为对前 $|x|$ 个文字的部分赋值，

$$\Phi(x) \triangleq \sum_{i=1}^{\ell} \Phi_i(x), \quad \Phi_i(x) \triangleq \prod_{j=1}^{m_i'} (1 - \phi_{ij}(x)) \tag{4.24}$$

$$\phi_{ij}(x) \triangleq \begin{cases} 0 & C'_{ij} \text{ is negatively determined} \\ 2^{-d} & C'_{ij} \text{ is } d\text{-far from positively determined} \end{cases} \tag{4.25}$$

为便于理解，我们指出，$\Phi(x)$ 的组合解释是：将 x 扩展为对 T 中变量的赋值，并以均匀随机的方式固定每个尚未固定的位后，未被平凡化的 c-NF 的期望数量。请注意，这并非 PV_1 证明的一部分。相反，我们证明：

- （初始条件）。请注意，$\phi_{ij}(\varepsilon) \geq 2^{-c}$，因此

$$\Phi_i(\varepsilon) \leq (1-2^{-c})^{m_i'} \leq (1-2^{-c})^{k \ln n} < \frac{1}{\ell}, \quad \Phi(\varepsilon) < 1.$$

- （递归条件）。对于每个 $x \in \{0,1\}^{<n-t}$，我们都可以证明 $\Phi_i(x) = (\Phi_i(x0) + \Phi_i(x1))/2$。为说明这一点，请注意：

  – 当第 $(|x|+1)$ 个变量未出现在 $C_{i,\,1}, \ldots, C_{i,\,m_i'}$ 中时，$\Phi_i(x) = \Phi(x0) = \Phi(x1)$。– 否则，由于子句彼此不相交，该变量恰好出现在 $C_{i,\,1}, \ldots, C_{i,\,m_i'}$ 中的一个子句里。假设 fo r 它的简洁性体现在 $C_{i,\,1}$ 且它是一个或门。接下来

$$\Phi_i(x) = (1 - \phi_{i1}(x)) \cdot \prod_{j=2}^{m_i'} (1 - \phi_{ij}(x)),$$

$$\Phi_i(x0) = (1 - 2 \cdot \phi_{i1}(x)) \prod_{j=2}^{m_i'} (1 - \phi_{ij}(x)), \quad \Phi_i(x1) = \prod_{j=2}^{m_i'} (1 - \phi_{ij}(x)).$$

因此 $\Phi_i(x) = (\Phi_i(x0) + \Phi_i(x1))/2$。随后，$\Phi(x) = (\Phi(x0) + \Phi(x1))/2$。

- （终止条件）。 $\Phi_i(x) \in \{0,1\}$ 适用于 $x \in \{0,1\}^{n-t}$。此外，如果 $\Phi(x) = 0$，部分赋值 x 将使所有 c-NF 变得平凡。

该引理随后可由如下子集选择引理中的贪心算法推出。 □

定理 1.7 （最坏情况 AC^0 下界： $\oplus_n$ 在 PV_1中）。 对于所有常元 k、$d \geq 1$，存在一个常元 $n_0 \geq 1$，使得 PV_1 证明以下陈述。对于每个 $n \in \mathsf{Log}$、 $n > n_0$以及 AC^0_d 电路C： 其大小至多为 n^k，存在一个字符串 $x \in \{0,1\}^n$，使得 $C(x) \neq \oplus_n(x)$。

证明概要。 该证明紧密遵循平均情况 AC^0 下界： $\oplus_n$的证明，因此我们只概述论证。我们在元理论中对 d 进行归纳证明，并且常元 $n_0 = n^{k^{d}}_0$ 同时取决于 k 和 d。当 $d = 1$ 时，情形很简单，留作练习。

对于 $d \geq 2$，我们反设 C 计算 $\oplus_n$。首先应用子集选择引理，找到一个大小为 T的子集 $n - \sqrt{n}$： 将第一层的门视为 1-NF。然后应用去随机化限制引理，找到一个赋值 ρ，赋给 T 中的变量，使得应用 ρ后，第一层的门要么被平凡化，要么扇入至多为 $b = O$。令 $n_1 = \sqrt{n}$。我们可以根据 C 和 ρ构造一个电路 C_1，使其在未固定的比特上计算 $\oplus_{n_1}$，且所有第一层的门的扇入均为 b。

接着，我们再次应用子集选择引理，找到一个大小为 $n_1 - \sqrt{n_1}$ 的子集 T_1： 将第二层的门视为 b-NF。然后应用去随机化限制引理，找到一个赋值 ρ_1，赋给 T_1 中的变量，使得应用 ρ_1后，第二层的门要么被平凡化，要么扇入至多为 $b_1 = O$。令 $n_2 = \sqrt{n_1}$。随后，我们可以根据 C_1 和 ρ_1构造一个深度至多为$d-1$ 的电路 C_2，使其在未固定的比特上计算 $\oplus_{n_2}$。该电路的大小至多为 $n^{k+1} \leq n_2^{6k}$。令 $n^{k^{d}}_0$ 足够大，使其取值基于 $n^{6k^{d-1}}_0$，即可由此得到与归纳假设矛盾的结论。 □

4.5 Blum-Luby-Rubinfeld 线性测试

现在我们将 Blum、Luby 和 Rubinfeld [BLR93]提出的线性测试算法形式化。回忆一下，若函数 $g\colon \{0,1\}^n \to \{0,1\}$ 满足 $g(x \oplus y) = g(x) \oplus g(y)$，则称其为线性函数，其中 $\oplus$ 表示按位异或；等价地，对于某个 $z \in \{0,1\}^n$，有 $g(x) = \langle x, z\rangle$ 模 2。设 $g\colon \{0,1\}^n \to \{0,1\}$ 是一个函数。Blum、Luby 和 Rubinfeld [BLR93] 证明，对于任意充分小的常元 $\varepsilon > 0$：

- （线性测试）：如果 g 与任何线性函数都相差至少 ε，那么 BLR 线性测试算法以至少 $\Omega(\varepsilon)$ 的概率失败。反过来，如果 g 与某个线性函数相差至多 ε，那么 BLR 线性测试算法以至多 $O(\varepsilon)$ 的概率失败。

- （自我纠错）：线性测试背后的关键思想是一种随机自我纠错算法：如果 g 与线性函数 $\hat{}g$相差ε以内，那么函数 $f(x, r) \triangleq g(x \oplus r) \oplus g(r)$ 是一种随机化算法，它以 $O(\varepsilon)$的错误率计算 $\hat{}g$，其中 x 是输入， r 是随机种子。

线性测试是指数长度 PCP 定理的关键组成部分$\mathsf{NP} \subseteq \mathsf{PCP}[\text{多项式}, 1]$，它还用于减少 PCP 定理证明中的查询次数$\mathsf{NP} = \mathsf{PCP}[\text{对数}\, n, 1]$（例如，参见 [Har04]）。

我们首先陈述主要定理，即 BLR 线性测试的完备性和可靠性。完备性指出，与线性函数接近的函数很可能会被接受。形式化地说：

定理 4.11 （BLR 线性测试的完备性）。 APX_1 证明如下结论。设 n、δ^{-1}、$\beta^{-1} \in \mathsf{Log}$、$C$：$\{0,1\}^n \to \{0,1\}$ 是一个电路， $z \in \{0,1\}^n$ 是一个字符串。设 $\varepsilon \in \mathbb{Q}$ 满足 $\varepsilon < 1/2$。定义以下电路：

- 令 $T_C(x)$ 为当且仅当 $C(x) \neq \langle x, z\rangle$ 模 2 时输出 1 的电路。
- 令 $T_{C,\mathsf{BLR}}(x, y)\colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ 为当 $C(x) \oplus C(y) \neq C(x \oplus y)$时输出 1 的电路。假设 $\mathsf{P}_\delta(T_C) \leq \varepsilon$。那么 $\mathsf{P}_\delta(T_{C,\mathsf{BLR}}) \leq 3\varepsilon + 4\delta + \beta$。

可靠性表明，如果某个函数很可能被 BLR 线性测试算法接受，那么它就接近一个线性函数。

定理 4.12（BLR 线性测试的可靠性）。 APX_1 证明了以下陈述。设 $n, \delta^{-1}, \beta^{-1} \in \mathsf{Log}$ 和 C：$\{0,1\}^n \to \{0,1\}$ 是一个电路。设 $\varepsilon \in \mathbb{Q}$。假设 $\varepsilon, \delta, \beta < 0.01$。我们定义以下电路：

- 对于每个 $z \in \{0,1\}^n$，$T_{C,\,z}(x)$ 是这样一个电路：当且仅当 $C(x) \neq \langle x, z\rangle$ 模 2时，输出1 。
- 令 $T_{C,\,\mathsf{BLR}}(x,y)$ 为这样一个电路：当且仅当 $C(x) \oplus C(y) \neq C(x \oplus y)$时，输出1 。

*Su*假设 $\mathsf{P}_\delta(T_{C,\,\mathsf{BLR}}) \leq \varepsilon$。那么存在一个字符串 $z \in \{0,1\}^n$ 使得 $\mathsf{P}_\delta(T_{C,\,z}) \leq 5\varepsilon + 6\delta + \beta$。

我们通过多数校正将组合证明形式化 [BLR93]（另见 [BCH+96]，一种不同的证明）。请注意，Pich 也在 [Pic15a] 中将同一证明形式化APC_1，以证明指数 PCP 定理 $\mathsf{NP} \subseteq \mathsf{PCP}[\mathrm{poly}, 1]$,；我们的主要贡献是证明，可以在（可能更弱的）理论 APX_1中将其形式化。[22]

4.5.1 两个有用引理

在形式化 BLR 线性测试算法之前，我们先证明两个有用引理。第一个引理表明，如果将输入与一个固定的字符串进行异或，电路的接受概率不会发生显著变化。形式化地说：

引理 4.13（重新随机化）。 APX_1 证明了以下陈述。对于任意 n、δ^{-1}、$\beta^{-1} \in \mathsf{Log}$、电路 T：$\{0,1\}^n \to \{0,1\}$ 以及 $x \in \{0,1\}^n$，令 $T_x^{\oplus}$：$\{0,1\}^n \to \{0,1\}$ 为定义为 $T_x^{\oplus}(r) \triangleq T(x \oplus r)$ 的电路。那么 $|\mathsf{P}_\delta(T) - \mathsf{P}_\delta(T_x^{\oplus})| \leq 2\delta + \beta$。

证明。 我们在 APX_1 中进行论证。固定 n、δ^{-1}、$\beta^{-1} \in \mathsf{Log}$、$x \in \{0,1\}^n$、电路 T 以及 $T_x^{\oplus}$。令 $\eta^{-1} \in \mathsf{Log}$ 为稍后确定的参数。反设 $|\mathsf{P}_\delta(T) - \mathsf{P}_\delta(T_x^{\oplus})| > 2\delta + \beta$。根据 Precision Consistency Axiom，我们有

$$|\mathsf{P}_\eta(T) - \mathsf{P}_\eta(T_x^{\oplus})| > \beta - 4\eta.$$

回忆一下，对于电路 C, $C^{k,\,z}$ 表示将 C 的最后 k 个输入位固定为z后得到的电路。我们将设计一个 n 轮迭代式 PV(P) 算法，使其在第 i 轮输出一个字符串 $z_i \in \{0,1\}^i$，满足

$$|\mathsf{P}_\eta(T^{i,z_i}) - \mathsf{P}_\eta(T_x^{\oplus,i,z_i'})| > \beta - 10 \cdot (i+1) \cdot \eta. \tag{4.26}$$

其中 $z_i' \triangleq z_i \oplus x_{>n-i}$。算法首先将 $z_0 \triangleq \varepsilon$。在第 i 轮中，其工作方式如下：

- 回忆一下，根据不变式，方程（4.26）在第 $i-1$ 轮成立，因此我们有 e

$$|\mathsf{P}_\eta(T^{i-1,z_{i-1}}) - \mathsf{P}_\eta(T_x^{\oplus,i-1,z_{i-1}'})| > \beta - 10 \cdot i \cdot \eta.$$

- 根据 Local Consistency Axiom，我们知道

$$\begin{aligned} &|\mathsf{P}_\eta(T^{i-1,z_{i-1}}) - \mathsf{P}_\eta(T_x^{\oplus,i-1,z_{i-1}'})| \\ \leq\ &\frac{1}{2} \sum_{b \in \{0,1\}} \left|\mathsf{P}_\eta(\mathsf{Fix}_b(T^{i-1,z_{i-1}})) - \mathsf{P}_\eta(\mathsf{Fix}_{b \oplus x_{n-i+1}}(T_x^{\oplus,i-1,z_{i-1}'}))\right| + 3\eta. \end{aligned}$$

随后，存在一个常元 $b \in \{0,1\}$，使得

$$\left|\mathsf{P}_\eta(\mathsf{Fix}_b(T^{i-1,z_{i-1}})) - \mathsf{P}_\eta(\mathsf{Fix}_{b \oplus x_{n-i+1}}(T_x^{\oplus,i-1,z_{i-1}'}))\right| > \beta - 10 \cdot i \cdot \eta - 3\eta. \tag{4.27}$$

该算法通过查询 P-预言机找到这样的 $b \in \{0,1\}$，并输出 $z_i \triangleq b \circ z_{i-1}$。

[22]我们的形式化略有不同：我们通过明确给出 $x \mapsto \langle x,\ z\rangle$ 模 2 来形式化线性函数 z，而 Pich[Pic14] 则通过使用如下语句形式化线性函数：对于每个 f，x，y，$f(x \oplus y) = f(x) \oplus f(y)$；不过，在大多数情况下，形式化上的差异并不重要。

要证明该算法正确，只需注意到电路 $\mathsf{Fix}_b(T^{i-1,\ z_{i-1}})$ 与 $T^{i,\ z_i}$ 函数等价，并且 $\mathsf{Fix}^{b\oplus x_{n-i+1}}(T^{\oplus i-1,}_{x}{}^{\ z'_{i-1}})$ 与 $T^{\oplus,\ i,\ z_i}_{\ x}$ 函数等价。因此，根据方程（4.27）和 全局一致性，我们有

$$|\mathsf{P}_\eta(T^{i,z_i}) - \mathsf{P}_\eta(T_x^{\oplus,i,z'_i})| \geq \left|\mathsf{P}_\eta(\mathsf{Fix}_b(T^{i-1,z_{i-1}})) - \mathsf{P}_\eta(\mathsf{Fix}_{b\oplus x_{n-i+1}}(T_x^{\oplus,i-1,z'_{i-1}}))\right| - 6\eta \geq \beta - 10\cdot(i+1)\cdot\eta.$$

因此，可以通过对一个PV(P) 项进行归纳法来证明算法的正确性；根据定理 2.10，这样的项是存在的。

最后，在第 n 轮，算法输出一个字符串 $z_n \in \{0,1\}^n$，使得

$$|\mathsf{P}_\eta(T^{n,z_n}) - \mathsf{P}_\eta(T_x^{\oplus,n,z'_n})| > \beta - 10\cdot(n+1)\cdot\eta,$$

其中 $z'_n \triangleq z_n \oplus x$。注意，上述两个电路的输入长度均为 0，因此根据定义，它们必须输出相同的值。这通过设置 $\eta \triangleq \beta/(100(n+1))$ 违反了 Boundary Axiom。 □

第二个引理如下。设 X_1 和 X_2 是定义在 $\{0,1\}$ 上的两个显式独立同分布随机变量。如果 $\Pr[X_1 = X_2]$ 大于 $1/2$，那么 $\mathbb{E}[X_i]$ 必定有偏。形式化地说：

引理 4.14。 APX_1 证明了以下陈述。设 n、δ^{-1}、$\beta^{-1} \in \mathsf{Log}$、$V = \{0,1\}$ 和 X_1、X_2 是由电路 C：$\{0,1\}^n \to \{0,1\}$ 定义在 V 上的显式独立同分布随机变量。设 Y_c 是 $X_1 = X_2$ 的指示随机变量，其中 X_1 和 X_2 使用不相交随机种子。那么对于 $i \in \{1,2\}$，

$$\left|\mathbb{E}_\delta[X_i] - \frac{1}{2}\right| \geq \sqrt{\frac{\mathbb{E}_\delta(Y_c)}{2} - \frac{1}{4} - 5\delta - \beta}.$$

证明。我们在 APX_1 中论证。固定 n、δ^{-1}、$\beta^{-1} \in \mathsf{Log}$、电路 C、T，以及随机变量 X_1、X_2、Y_c。令 $\eta^{-1} \in \mathsf{Log}$ 为稍后确定的参数。注意，由于 X_1 和 X_2 都是 C 的指示随机变量，根据命题 3.12 可证明 $|\mathbb{E}_\eta[X_1] - \mathsf{P}_\eta(C)|$、$|\mathbb{E}_\eta[X_2] - \mathsf{P}_\eta(C)| \leq 3\eta$，进而

$$|\mathbb{E}_\eta[X_1] - \mathbb{E}_\eta[X_2]| \leq 6\eta. \tag{4.28}$$

令 Y_0、Y_1 为定义在 $\{0,1\}$ 上的随机变量，使得 Y_i 取值为 $(x_1,\ x_2) \in \{0,1\}^n \times \{0,1\}^n$，当且仅当 $C(x_1) = C(x_2) = i$ 时输出 1。容易看出，对于种子的每个赋值 $\rho = (x_1,\ x_2) \in \{0,1\}^{2n}$，$Y_c|_\rho = Y_0|_\rho + Y_1|_\rho$。因此，根据期望的平均论证，

$$|\mathbb{E}_\eta[Y_c] - \mathbb{E}_\eta[Y_0] - \mathbb{E}_\eta[Y_1]| \leq 6\eta. \tag{4.29}$$

令 $\overline{X}_1, \overline{X}_2$ 为由 $1 - X_1$ 和 $1 - X_2$ 分别定义的随机变量。利用互补计数，

$$\left|\mathbb{E}_\eta[\overline{X}_i] + \mathbb{E}_\eta[X_i] - 1\right| \leq 6\eta \tag{4.30}$$

对于 $i \in \{1,2\}$。我们还可以进一步观察到，对于随机种子的每个赋值 ρ，$Y_0|_\rho = X_1X_2|_\rho$ 和 $Y_1|_\rho = \overline{X}_1\overline{X}_2|_\rho$，随后根据期望的平均论证，

$$\left|\mathbb{E}_\eta[Y_0] - \mathbb{E}_\eta[\overline{X}_1\overline{X}_2]\right| \leq 6\eta, \quad |\mathbb{E}_\eta[Y_1] - \mathbb{E}_\eta[X_1X_2]| \leq 6\eta.$$

随后，根据乘法原理，

$$\left|\mathbb{E}_\eta[Y_0] - \mathbb{E}_\eta[\overline{X}_1]\cdot\mathbb{E}_\eta[\overline{X}_2]\right| \leq 14\eta, \quad |\mathbb{E}_\eta[Y_1] - \mathbb{E}_\eta[X_1]\cdot\mathbb{E}_\eta[X_2]| \leq 14\eta. \tag{4.31}$$

Fix任意 $i \in \{1,2\}$，并令 $p \triangleq \mathbb{E}_\delta[X_i]$、$q \triangleq \mathbb{E}_\delta[Y_C]$。为简单起见，我们假设 $0 < \mathbb{E}_\eta[X_1] < 1$ 与 $0 < \mathbb{E}_\eta[X_2] < 1$。我们可以进行如下计算：

$$
\begin{aligned}
\mathbb{E}_\delta[Y_C] &\le \mathbb{E}_\eta[Y_C] + (\delta + 2\eta) && \text{(期望的精度一致性)} \\
&\le \mathbb{E}_\eta[Y_0] + \mathbb{E}_\eta[Y_1] + (\delta + 8\eta) && \text{(Equation (4.29))} \\
&\le \mathbb{E}_\eta[\overline{X}_1] \cdot \mathbb{E}_\eta[\overline{X}_2] + \mathbb{E}_\eta[X_1] \cdot \mathbb{E}_\eta[X_2] + (\delta + 36\eta) && \text{(Equation (4.31))} \\
&\le (1 - \mathbb{E}_\eta[X_1] + 6\eta)(1 - \mathbb{E}_\eta[X_2] + 6\eta) + \mathbb{E}_\eta[X_1] \cdot \mathbb{E}_\eta[X_2] + (\delta + 36\eta) && \text{(Equation (4.30))} \\
&\le (1 - \mathbb{E}_\eta[X_i] + 6\eta)(1 + \mathbb{E}_\eta[X_i] + 12\eta) + \mathbb{E}_\eta[X_i] \cdot (\mathbb{E}_\eta[X_i] - 6\eta) + (\delta + 36\eta) && \text{(Equation (4.28))} \\
&\le (1 - p + \delta + 14\eta)^2 + (p + \delta + 14\eta)^2 + (\delta + 36\eta) && \text{(\textit{Precision Consistency of Expectation})} \\
&\le (1-p)^2 + (\delta + 14\eta)^2 + 2(1-p)(\delta + 14\eta) + p^2 + (\delta + 14\eta)^2 + 2p(\delta + 14\eta) + (\delta + 36\eta) \\
&\le (1-p)^2 + p^2 + 5\delta + 78\eta \\
&\le 1 - 2(p - p^2) + 5\delta + \beta,
\end{aligned}
$$

其中，最后一个不等式在令 $\eta \triangleq \beta/100$ 时成立。因此我们有 $p - p^2 \le (1-q)/2 + 5\delta + \beta$，进而

$$
\left|\frac{1}{2} - p\right| = \sqrt{\left(\frac{1}{2} - p\right)^2} = \sqrt{\frac{1}{4} - (p - p^2)} \ge \sqrt{\frac{1}{4} - \left(\frac{1-q}{2} + 5\delta + \beta\right)} \ge \sqrt{\frac{q}{2} - \frac{1}{4} - 5\delta - \beta}.
$$

证明至此完成。 □

4.5.2 BLR 线性测试的完备性

我们首先将线性测试算法的完备性形式化。也就是说，如果电路 $C\colon \{0,1\}^n \to \{0,1\}$ 计算出的函数确实与一个线性函数 $x \mapsto \langle z,\ x\rangle$ 模 2 近似，那么自校正算法就能正常工作。形式化地说：

引理 4.15 (BLR 自校正的完备性)。 APX_1 证明了以下结论。设 $n, \delta^{-1}, \beta^{-1} \in \mathsf{Log}$，$C\colon \{0,1\}^n \to \{0,1\}$ 是一个电路，$z \in \{0,1\}^n$ 是一个字符串。设 $\varepsilon \in \mathbb{Q}$ 满足 $\varepsilon < 1/2$。定义以下电路：

- 设 $T_C(x)$ 是一个当且仅当 $C(x) \ne \langle x, z\rangle$ 模 2时输出 1 的电路。
- 令 $D(x,r)\colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ 为输出 $C(x \oplus r) \oplus C(r)$的电路。
- 对于 $x \in \{0,1\}^n$，令 $T_{D,x}(r)$ 为当且仅当 $D(x,r) \ne \langle x, z\rangle$ 模 2时输出1 的电路。

假设$\mathsf{P}_\delta(T_C) \le \varepsilon$。那么对于每个 $x \in \{0,1\}^n$，$\mathsf{P}_\delta(T_{D,x}) \le 2(\delta + \varepsilon) + \beta$。

证明。 我们在 APX_1 中进行论证。取定 $n, \delta^{-1}, \beta^{-1} \in \mathsf{Log}$、电路 C, $z \in \{0,1\}^n$ 以及 $\varepsilon \in \mathbb{Q}$。令 $T_C, D, T_{D,x}$ 为如上定义的电路，并令 $\eta^{-1} \in \mathsf{Log}$ 为稍后确定的参数。假设 $\mathsf{P}_\delta(T_C) \le \varepsilon$，由 Precision Consistency Axiom 可知

$$
\mathsf{P}_\eta(T_C) \le \varepsilon + \delta + 2\eta. \tag{4.32}
$$

固定任意 $x \in \{0,1\}^n$。令 X_1, X_2 为定义在 $\{0,1\}$ 上的随机变量，它们取一个种子 $r \in \{0,1\}^n$，其中若 $C(r) \ne \langle r$，则 $X_1 = 1 \bmod 2$；若 $C(x \oplus r) \ne \langle x \oplus r$，则 $X_2 = 1 \bmod 2$。显然，X_1 是 T_C 的指示随机变量，因此根据公式（4.32）和命题 3.12，$\mathbb{E}_\eta[X_1] \le \varepsilon + \delta + 5\eta$。根据命题 3.12 和重新随机化引理，我们还可以进一步证明

$$
\mathbb{E}_\eta[X_2] \le \mathsf{P}_\eta(T_C) + 6\eta \le \varepsilon + \delta + 8\eta.
$$

令 $T_\vee(r)$ 为一个电路，当且仅当 $C(r) \ne \langle r, z\rangle$ 模 2 或 $C(x \oplus r) \ne \langle x \oplus r, z\rangle$ 模 2 时输出 1，并令 Y 为 $T_\vee$ 的指示随机变量。根据命题 3.12 和并集界，我们有

$$
\mathsf{P}_\eta(T_\vee) \le \mathbb{E}_\eta[Y] + 3\eta \le \mathbb{E}_\eta[X_1] + \mathbb{E}_\eta[X_2] + 6\eta \le 2\varepsilon + 2\delta + 19\eta. \tag{4.33}
$$

最后，我们观察到观察到，若 $T_{D,x}(r)=1$，则 $T_\vee(r)=1$。为说明这一点，假设 $T_\vee(r)=0$，我们有

$$D(x,r)=C(x\oplus r)\oplus C(r)=\langle x\oplus r,z\rangle+\langle r,z\rangle \bmod 2=\langle x,z\rangle \bmod 2,$$

这意味着 $T_{D,x}(r)=0$。因此，我们有

$$\begin{aligned}
\mathsf{P}_\delta(T_{D,x}) &\le \mathsf{P}_\eta(T_{D,x})+\delta+2\eta && \text{(Precision Consistency Axiom)}\\
&\le \mathsf{P}_\eta(T_\vee)+\delta+5\eta && \text{(近似计数的单调性)}\\
&\le 2\varepsilon+2\delta+24\eta. && \text{(方程 (4.33))}
\end{aligned}$$

令 $\eta\triangleq\beta/30$，证明即告完成。 □

可以看出，这立即给出了 BLR 恒等性测试算法的完备性。也就是说，如果 C 接近某个线性函数，那么它以高概率通过线性测试。

定理 4.11 (BLR 线性测试的完备性)。 APX_1 证明如下结论。设 n、δ^{-1}、$\beta^{-1}\in\mathsf{Log}$、$C\colon\{0,1\}^n\to\{0,1\}$ 是一个电路，$z\in\{0,1\}^n$ 是一个字符串。设 $\varepsilon\in\mathbb{Q}$ 满足 $\varepsilon<1/2$。定义以下电路：

- 设 $T_C(x)$ 为一个电路，当且仅当 $C(x)\neq\langle x、z\rangle$ 对 2 取模时输出 1 。
- 设 $T_{C,\mathsf{BLR}}(x、y)\colon\{0,1\}^n\times\{0,1\}^n\to\{0,1\}$ 为一个电路，当 $C(x)\oplus C(y)\neq C(x\oplus y)$.

假设 $\mathsf{P}_\delta(T_C)\le\varepsilon$。那么 $\mathsf{P}_\delta(T_{C,\mathsf{BLR}})\le 3\varepsilon+4\delta+\beta$。

证明。我们在 APX 中进行论证。令 $n,\delta^{-1},\beta^{-1}\in\mathsf{Log}$，$C\colon\{0,1\}^n\to\{0,1\}$，$z\in\{0,1\}^n$，$\varepsilon\in\mathbb{Q}$，并令 T_C，$T_{C,\mathsf{BLR}}$ 为上文所述的电路。令 $T'_{C,\mathsf{BLR}}\colon\{0,1\}^n\times\{0,1\}^n\to\{0,1\}$ 为这样一个电路：给定 (x,y)，当 $C(x\oplus y)\oplus C(y)\neq\langle x,z\rangle$ 模 2 时输出 1。令 $I_C,I_{C,\mathsf{BLR}},I'_{C,\mathsf{BLR}}$ 分别为 $T_C,T_{C,\mathsf{BLR}},T'_{C,\mathsf{BLR}}$ 的指示随机变量。

令 $\eta^{-1}\in\mathsf{Log}$ 为稍后确定的参数。注意，根据*BLR自我纠正的完备性*和命题3.12，我们可以证明，对于任意赋值 ρ 作为种子的第一部分$T'_{C,\mathsf{BLR}}$，都有 $\mathbb{E}_\eta[I_{C,\mathsf{BLR}}|_\rho]\le 2(\delta+\varepsilon)+4\eta$。随后，根据期望的平均论证，我们有

$$\mathbb{E}_\eta[I_{C,\mathsf{BLR}}]\le 2(\delta+\varepsilon)+4\eta+6\eta\le 2(\delta+\varepsilon)+10\eta. \tag{4.34}$$

根据命题3.12 和 Precision Consistency Axiom，我们也有 $\mathbb{E}_\eta[I_C]\le\varepsilon+\delta+5\eta$。

可以观察到，如果$T_{C,\mathsf{BLR}}(x,y)=1$，那么要么 $T_C(x,y)=1$，要么$T'_{C,\mathsf{BLR}}(x,y)=1$。因此，根据并集界，我们可以证明

$$\mathbb{E}_\eta[I_{C,\mathsf{BLR}}]\le\mathbb{E}_\eta[I_C]+\mathbb{E}_\eta[I'_{C,\mathsf{BLR}}]+6\eta\le 3(\delta+\varepsilon)+15\eta.$$

随后，根据命题 3.12，$\mathsf{P}_\eta(T_{C,\mathsf{BLR}})\le 3(\delta+\varepsilon)+\delta+18\eta$。通过设置 $\eta\triangleq\beta/30$，由 Precision Consistency Axiom 即可得到该结果。 □

4.5.3 多数校正的正确性

接下来我们证明 BLR 线性测试的可靠性。作为第一步，我们证明如果 C通过线性测试，那么 BLR 自我纠正算法是单值的。形式化地说：

引理 4.16 (BLR纠正的单值性)。 APX_1 证明了以下命题。设 $n,\delta^{-1},\beta^{-1}\in\mathsf{Log}$和 $C\colon\{0,1\}^n\to\{0,1\}$ 为一个电路。设 $\varepsilon\in\mathbb{Q}$。假设 $\varepsilon,\delta,\beta\le 0.01$。定义以下电路：

- 设 $T_{C,\mathsf{BLR}}(x,y)$ 为一个电路，当且仅当 $C(x)\oplus C(y)\neq C(x\oplus y)$时输出 1 。
- 设 $D_{x,b}(r)\colon\{0,1\}^n\to\{0,1\}$ 为一个电路，当且仅当 $C(x\oplus r)\oplus C(r)=b$时输出 1 。

假设$\mathsf{P}_\delta(T_{C,\mathsf{BLR}})\le\varepsilon$。对于每个 $x\in\{0,1\}^n$，$\mathsf{P}_\delta(D_{x,b})\ge 1-4\varepsilon-(4\delta+\beta)$ 对于某个 $b\in\{0,1\}$.

证明。我们在 APX_1中进行论证。令 n，δ^{-1}，$\beta^{-1} \in \mathsf{Log}$、电路 C以及 $\varepsilon \in \mathbb{Q}$。设 $T_{C,\ \mathsf{BLR}}$和 $D_{x,\ b}$为如上定义的电路，并且 $\eta^{-1} \in \mathsf{Log}$ 是一个稍后确定的参数。假设 $\mathsf{P}_\delta(T_{C,\ \mathsf{BLR}}) \leq \varepsilon$，根据 Precision Consistency Axiom 可知

$$\mathsf{P}_\eta(T_{C,\mathsf{BLR}}) \leq \varepsilon + \delta + 2\eta. \tag{4.35}$$

Fix任意 $x \in \{0,1\}^n$。令 $D'_x\colon\ \{0,1\}^{2n} \to \{0,1\}$为电路，其以$(r_1, r_2) \in \{0,1\}^n$为输入，并在 $C($ $x \oplus r_1) \oplus C(r_1) = C(x \oplus r_2) \oplus C(r_2)$时输出1。令 Y为 D'_x的指示随机变量， Y为 $1 - D'_x$的指示随机变量。由期望的平均论证可得$\mathbb{E}_\eta[Y] \geq 1 - \mathbb{E}_\eta[Y] - 6\eta$。

考虑以下两个电路 $T, T'\colon\ \{0,1\}^{2n} \to \{0,1\}$:

- $T(r_1, r_2) \triangleq 1$当且仅当 $C(r_1) \oplus C(r_2) \neq C(r_1 \oplus r_2)$。
- $T'(r_1,\ r_2) \triangleq 1$当且仅当 $C(x \oplus r_1) \oplus C(x \oplus r_2) \neq C((x \oplus r_1) \oplus (x \oplus r_2))$。

令 X, X'分别为 T和 T'的指示随机变量。显然， T恰好是 $T_{C,\mathsf{BLR}}$，因此由公式（4.35）可得，$\mathsf{P}\eta(T)$ $\leq \varepsilon + \delta + 2\eta$。类似地，由于 T'_i是通过将输入字符串与固定字符串 (x, x) 按位异或而得到的 $T_{C,\mathsf{BLR}}$，由公式（4.35）和重新随机化引理可得，$\mathsf{P}\eta(T') \leq \eta + \delta + 5\eta$。

此外，可以观察到， $D'_x(x,\ y) = 0$意味着 $T(x,\ y)$ 或 $T'(x,\ y)$ 的输出为 1：这是因为，如果 $T(x,\ y) = T'(x,$ $y) = 0$，我们可以得出结论：

$$C(x \oplus r_1) \oplus C(x \oplus r_2) \oplus C(r_1) \oplus C(r_2) = C(r_1 \oplus r_2) \oplus C((x \oplus r_1) \oplus (x \oplus r_2)) = 0,$$

这意味着 $D'_x(x,\ y) = 1$。随后，根据 并集界，我们有

$$\mathbb{E}_\eta[\overline{Y}] \leq \mathbb{E}_\eta[X_i] + \mathbb{E}_\eta[X'_i] + 3\eta \leq 2(\varepsilon + \delta) + 10\eta.$$

因此 $\mathbb{E}_\eta[Y] \geq 1 - \mathbb{E}_\eta[Y] - 6\eta \geq 1 - 2(\varepsilon + \delta) - 16\eta$。

设 I_x，I'_x是定义在 $\{0,1\}$上的显式独立同分布随机变量，由电路 $D_x(r) \triangleq C(x \oplus r) \oplus C(r)$ 定义，并且 Y_c是 $I_x = I'_x$的指示随机变量。根据定义，我们可以看到，对于任意赋值 $Y_c|_\rho = Y|_\rho$，都有 ρ，因此根据 期望的平均论证，

$$\mathbb{E}_\eta[Y_c] \geq \mathbb{E}_\eta[Y] - 6\eta \geq 1 - 2(\varepsilon + \delta) - 22\eta.$$

随后，根据引理 4.14，我们有

$$\left|\mathbb{E}_\eta[I_x] - \frac{1}{2}\right| \geq \sqrt{\frac{1 - 2(\varepsilon + \delta) - 22\eta}{2} - \frac{1}{4} - 6\eta} \geq \sqrt{\frac{1}{4} - (\varepsilon + \delta + 17\eta)} \geq \frac{1}{2} - 4(\varepsilon + \delta + 17\eta). \tag{4.36}$$

回忆一下， I_x是一个随机变量，它以 $(r_1,\ r_2) \in \{0,1\}^{2n}$作为随机种子，并输出 $C(x \oplus r_1) \oplus C(r_1)$。假设 $\mathbb{E}_\eta[I_x] \geq 1 - 4(\varepsilon + \delta + 17\eta)$。根据 期望的平均论证，存在第二部分种子的一个赋值 ρ （该部分用于 r_2） I'_x，使得

$$\mathbb{E}_\eta[I_x|_\rho] \geq \mathbb{E}_\eta[I_x] - 6\eta \geq 1 - 4\eta - (4\delta + 74\eta).$$

由于 $I_x|_\rho$ 是 $D_{x,1}$的指示随机变量，根据命题 3.12 可得 $\mathsf{P}\eta(D_{x,1}) \geq \mathbb{E}_\eta[I_x] - 3\eta \geq 1 - 4\varepsilon - (4\delta + 74\eta)$。只需令 $\eta \leq \beta/100$即可。另一种情况 $\mathbb{E}_\eta[I_x] \leq 4(\varepsilon + \delta + 17\eta)$ 可通过考虑 $I_x \triangleq 1 - I_x$来解决。

□

引理 4.16 表明，假设电路 C通过线性测试，则 BLR 自校正算法是单值的。其次，我们证明“校正后”的函数 $g(\cdot)$ 满足 $g(x) \oplus g(y) = g(x \oplus y)$，对 每个 $x, y \in \{0,1\}^n$ 均成立。形式化地说：

引理 *4.17*（*BLR* 校正的线性）。APX_1 证明了以下命题。设 $n, \delta^{-1}, \beta^{-1} \in \mathit{Log}$，且 $C\colon \{0,1\}^n \to \{0,1\}$ 是一个电路。设 $\varepsilon \in \mathbb{Q}$。假设 $\varepsilon, \delta, \beta \le 0.01$。令 $D_{x,b}$ 为引理 *4.16* 中的电路，令 $g(x)$ 为如下工作的 *P*-预言机电路：给定 $x \in \{0,1\}^n$，若 $P_\delta(D_{x,b}) \ge 1 - 4\varepsilon - (4\delta + \beta)$，则输出 $b \in \{0,1\}$；否则输出 $\perp$。

令 $T_{C,\mathsf{BLR}}(x, y)$ 为当且仅当 $C(x) \oplus C(y) \neq C(x \oplus y)$ 时输出 *1* 的电路。假设 $P_\delta(T_{C,\mathsf{BLR}}) \le \varepsilon$。那么对于每个 $x_1, x_2 \in \{0,1\}^n$，$g(x_1) \oplus g(x_2) = g(x_1 \oplus x_2)$。

证明。我们在 APX_1 中进行论证。固定 $n, \delta^{-1}, \beta^{-1} \in \mathsf{Log}$、电路 C 和 $\varepsilon \in \mathbb{Q}$。假设 $\mathsf{P}_\delta(T_{C,\mathsf{BLR}}) \le \varepsilon$。注意，根据引理 4.16 和 $\varepsilon, \delta, \beta < 0.01$，$g(x) \in \{0,1\}$，对于每个 $x \in \{0,1\}^n$ 均成立。固定 $x_1, x_2 \in \{0,1\}^n$，并令 $b_j \triangleq g(x_j)$，其中 $j \in \{1,2\}$，且 $b_\oplus \triangleq g(x_1 \oplus x_2)$。

令 $\eta^{-1} \in \mathsf{Log}$ 为稍后确定的参数，并令 X_1，X_2，$X_\oplus$ 为定义在 $\{0,1\}$ 上、种子为 $r \in \{0,1\}^n$ 的随机变量，定义如下：

当且仅当 $b_1 = C(x_1 \oplus r) \oplus C(r)$ 时，• X_1 输出 1。
当且仅当 $b_2 = C(x_2 \oplus r) \oplus C(r)$ 时，• X_2 输出 1。
当且仅当 $b_\oplus = C(x_1 \oplus x_2 \oplus (x_2 \oplus r)) \oplus C(x_2 \oplus r)$ 时，• $X_\oplus$ 输出 1。

注意，由于 $b_j \triangleq g(x_j)$，根据 g 的定义可知 $\mathsf{P}_\delta(D_{x_j,\ b_j}) \ge 1 - 4\varepsilon - (4\delta + \beta)$。可以看出，$X_1$，$X_2$ 是 $D_{x_1,\ b_1}$，$D_{x_2,\ b_2}$ 的指示随机变量，因此根据命题 3.12 以及期望的精度一致性，

$$\mathbb{E}_\eta[X_1], \mathbb{E}_\eta[X_2] \ge 1 - 4\varepsilon - (5\delta + \beta - 2\eta).$$

此外，$X_\oplus$ 是这样一个电路的指示变量：当 $b_\oplus = C(x_1 \oplus x_2 \oplus (x_2 \oplus r)) \oplus C(x_2 \oplus r)$ 时输出 1；该电路通过将输入与固定字符串 $D_{x_1 \oplus x_2}$ 进行异或 $b_\oplus$ 而从 x_2 得到。因此，根据命题 3.12 和重新随机化引理，有 $\mathbb{E}_{0.01}[X_\oplus] \ge 1 - 4\varepsilon - (5\delta + \beta - 2\eta)$。

设 $\overline{X_1} \triangleq 1 - X_1$、$\overline{X_2} \triangleq 1 - X_2$ 和 $X_\oplus \triangleq \overline{1 - X_\oplus}$。设 $Y \triangleq X_1 \vee X_2 \vee X_\oplus$ 和 $Y \triangleq \overline{1 - Y}$。利用互补计数和并集界，可得

$$\begin{aligned}
\mathbb{E}_\eta[Y] &\le \mathbb{E}_\eta[\overline{X}_1] + \mathbb{E}_\eta[\overline{X}_2] + \mathbb{E}_\eta[\overline{X}_\oplus] + 9\eta && (\textit{Union Bound}) \\
&\le (1 - \mathbb{E}_\eta[X_1]) + (1 - \mathbb{E}_\eta[X_2]) + (1 - \mathbb{E}_\eta[X_\oplus]) + 18\eta && (\textit{Complementary Counting}) \\
&\le 12\varepsilon + 15\delta + \beta + 24\eta.
\end{aligned}$$

再次利用互补计数，可得 $\mathbb{E}_\eta[Y] \ge 1 - (12\varepsilon + 15\delta + \overline{\beta} + 24\eta)$。令 $\eta \triangleq \beta/100$，可得 $\mathbb{E}_\eta[Y] > 3\eta$。

根据期望的平均论证，存在一个赋值 ρ 使得 $\mathbb{E}_{0.01}[Y|_\rho] \ge 0.05$，换句话说，$Y|_\rho = 1$ 在应用限制 ρ 后，其种子长度为 0。根据随机变量的定义，这表明

$$\begin{aligned}
b_1 &= C(x_1 \oplus r) \oplus C(r), \\
b_2 &= C(x_2 \oplus r) \oplus C(r), \\
b_\oplus &= C(x_1 \oplus x_2 \oplus (x_2 \oplus r)) \oplus C(x_2 \oplus r) = C(x_1 \oplus r) \oplus C(x_2 \oplus r).
\end{aligned}$$

由此立即可得 $b_\oplus = b_1 \oplus b_2$。 □

4.5.4 BLR 线性测试的可靠性

现在我们准备好证明 BLR 线性测试的可靠性了。从高层次来看，我们将利用预言机电路 $g(\cdot)$ 恢复定义线性函数的字符串 $z \in \{0,1\}^n$。值得注意的是，字符串 z 的正确性证明并非易事：它关键依赖于第3节中关于随机变量的工具，尤其是期望的平均论证。

定理 4.12 (BLR 线性测试的可靠性)。APX_1 证明了以下命题。设 $n, \delta^{-1}, \beta^{-1} \in \mathsf{Log}$ 和 $C\colon \{0,1\}^n \to \{0,1\}$ 是一个电路。设 $\varepsilon \in \mathbb{Q}$。假设 $\varepsilon, \delta, \beta < 0.01$。我们定义以下电路：

- 对于每个 $z \in \{0,1\}^n$，令 $T_{C,\ z}(x)$ 为当且仅当 $C(x) \neq \langle x, z\rangle$ 模 2时输出 1 的电路。
- 令 $T_{C,\ \mathsf{BLR}}(x,y)$ 为当且仅当 $C(x) \oplus C(y) \neq C(x \oplus y)$时输出 1 的电路。

假设 $\mathsf{P}_\delta(T_{C,\mathsf{BLR}}) \leq \varepsilon$。那么存在一个字符串 $z \in \{0,1\}^n$，使得 $\mathsf{P}_\delta(T_{C,z}) \leq 5\varepsilon + 6\delta + \beta$。

证明。我们在 APX_1 中进行论证。取定 n、δ^{-1}、$\beta^{-1} \in \mathsf{Log}$、电路 C 和 $\varepsilon \in \mathbb{Q}$。令 $T_{C,\ z}$和 $T_{C,\ \mathsf{BLR}}$为如上所定义的电路，并令 $\eta^{-1} \in \mathsf{Log}$ 为稍后确定的参数。假设 $\mathsf{P}_\delta(T_{C,\mathsf{BLR}}) \leq \varepsilon$，根据 Precision Consistency Axiom 我们知道

$$\mathsf{P}_\eta(T_{C,\mathsf{BLR}}) \leq \varepsilon + \delta + 2\eta. \tag{4.37}$$

令 $D_{x,\ b}(r) \triangleq C(x \oplus r) \oplus C(r) \oplus (1-b)$ 为引理 4.16中的电路，令 $g(x)$ 为引理 4.17中的预言机电路。由引理 4.16，对每个 $x \in \{0,1\}^n$，存在一个 $b \in \{0,1\}$ 使得

$$\mathsf{P}_\eta(D_{x,b}) \geq 1 - 4(\varepsilon + \delta + 2\eta) - 5\eta \geq 1 - 4(\varepsilon + \delta) - 13\eta. \tag{4.38}$$

注意，我们将选择 η 使得 $13\eta < 0.01$。因此，根据引理 4.17，对于每个 $x \in \{0,1\}^n$，满足方程（4.38）的比特 b 由 $g(x$ 给出。此外，对于每个 x_1，$x_2 \in \{0,1\}^n$，我们有$g(x_1) \oplus g(x_2) = g(x_1 \oplus x_2)$.

令 e_i 为除第 i 位外其余各位均为 0 的字符串，并且 $z \triangleq g(e_1) \circ g(e_2) \circ \cdots \circ g(e_n)$。也就是说，对于每个 $i \in [n]$，$z_i = g(e_i)$。令 X 和 Y 为定义在 $\{0,1\}$ 上的随机变量，它们取一个长度为 $2n$ 的种子（x，r）$\in \{0,1\}^n \times \{0,1\}^n$，定义如下。

- X 当且仅当 $C(x \oplus r) \oplus C(x) \neq C(r)$ 时输出 1。也就是说，X 是 T_C 的指示随机变量，BLR。根据命题 3.12，

$$\mathbb{E}_\eta[X] \leq \mathsf{P}_\eta(T_{C,\mathsf{BLR}}) + 3\eta \leq \varepsilon + \delta + 5\eta. \tag{4.39}$$

- Y当 $C(x) \neq \langle x,\ z\rangle$ 模 2 时输出 1。注意，对种子的第二部分的每个赋值 r，$Y|_r$ 都是 $T_{C,\ z}$ 的指示随机变量。

接下来，我们将证明，对于每个 $x \in \{0,1\}^n$，

$$|\mathbb{E}_\eta[X|_x] - \mathbb{E}_\eta[Y|_x]| \leq 4(\varepsilon + \delta) + 13\eta. \tag{4.40}$$

回顾 X 和 D_x的定义，b，对于种子第一部分的每个赋值 x，第一 部分，是 D_x 的指示随机变量，取值为1；而对于 $X \triangleq 1 - X$，$X|_x$是D_x 的指示随机变量，取值为0。因此，根据引理 4.16，

$$\max\{\mathbb{E}_\eta[X|_x], 1 - \mathbb{E}_\eta[X|_x]\} \geq 1 - 4(\varepsilon + \delta + 2\eta) - 5\eta \geq 1 - 4(\varepsilon + \delta) - 13\eta.$$

我们考虑 $\mathbb{E}_\eta[X|_x] \geq 1 - 4(\varepsilon + \delta) - 13\eta$ 的情况，另一种情况类似。根据 g 的定义，我们知道 $g(x) = 1$，进而

$$\langle x, z\rangle \bmod 2 = \sum_{i \in [n], x_i = 1} g(e_i) \bmod 2 = g(x),$$

其中最后一个等式由引理 4.17 和 1-Induction Axiom （注意，归纳公理已足够，因为 $n \in \mathsf{Log}$）。对于种子的第二部分的任意赋值 r，我们有 $\mathbb{E}_\eta[Y|_x|_y] = 1$，由此可推出 $\mathbb{E}_\eta[Y|_x] = 1$。因此，对于种子的第一部分的任意赋值 $x \in \{0,1\}^n$，

$$|\mathbb{E}_\eta[X|_x] - \mathbb{E}_\eta[Y|_x]| \leq 4(\varepsilon + \delta) + 13\eta.$$

根据 A 关于期望的均值论证，我们有 $|\mathbb{E}_\eta[X] - \mathbb{E}_\eta[Y]| \leq 4\ (\varepsilon + \delta)\ + 19\eta$，并且 th us

$$\mathbb{E}_\eta[Y] \leq \mathbb{E}_\eta[X] + 4(\varepsilon + \delta) + 19\eta \leq e.$$

再次，根据均 期望的平均论证，存在一个赋值 $r \in \{0,1\}^n$ 到第二部分 t 种子中使得

$$\mathbb{E}_\eta[Y|_r] \leq \mathbb{E}_\eta[Y] + 3\eta \leq 5(\varepsilon + \delta) + 27\eta. \tag{4.41}$$

固定赋值 r。如上所述， $\mathbb{E}_\eta[Y|_r]$ 是 $T_{C\text{的指示随机变量}, z}$，因此根据命题3.12和 Precision Consistency Axiom，

$$\mathsf{P}_\delta(T_{C,z}) \le \mathsf{P}_\eta(T_{C,z}) + \delta + 2\eta \le \mathbb{E}_\eta[Y|_r] + \delta + 5\eta \le 5\varepsilon + 6\delta + 32\eta.$$

通过取 $\eta \triangleq \beta/50$ 完成证明。 □

5 APX 的见证定理$_1$

本节将证明 APX_1 的一个见证定理，并探讨它与其他有界算术理论（包括 PV_1 和 APC_1）的关系。

5.1 APX$_1$ 中可证明全定义的 TFNP 问题

本小节将介绍 APX_1 的 $\forall\Sigma^b_1$-推论的一个见证定理（即 APX_1 中可证明全定义的 TFNP 问题）。

5.1.1 一个 TFZPP 问题：反驳者（姚期智）

我们将首先介绍一个TFZPP 问题[23]，称为姚期智预测器生成器的反驳；我们用Refuter(姚期智) 表示它。回顾一下，姚期智的区分器到预测器转换 [姚期智82]（见第4.1节）表明，若分布 $\mathcal{D}$ 在 $\{0,1\}^n$ 下不是 ε-伪随机的，即存在一个电路 C： $\{0,1\}^n \to \{0,1\}$（称为区分器），使得

$$\left|\Pr[C(\mathcal{D})] - \Pr[C(\mathcal{U}_n)]\right| > \varepsilon,$$

那么存在 $i \in [n]$ 以及一个预测器 P_i： $\{0,1\}^{i-1} \to \{0,1\}$，使得

$$\Pr_{x\leftarrow\mathcal{D}}[P(x_{<i}) = x_i] \ge \frac{1}{2} + \frac{\varepsilon}{4n},$$

即， P 以至少 i的优势预测 $\mathcal{D}$ 的第 $\varepsilon/4n$位。这一转换是构造和分析伪随机生成器的关键步骤（例如，参见 [NW94、IW97]）：它表明，不可预测的分布必然是伪随机的。

在下面的陈述中，如果离散概率分布 $\mathcal{D}$ 在其支撑集上均匀分布，也就是说，在概率非零的元素集合上均匀分布 $\mathcal{D}$，我们就称它是平坦的。分布的大小是其支撑集的大小。我们将把平坦分布显式表示为字符串列表。在接下来的讨论中，我们可能会默认相关分布是平坦且以显式形式表示的。

定义 5.1。搜索问题 Refuter(Yao) 定义如下。

- （参数）。字符串长度 n、分布大小 m、预测器大小 s和优势 $\delta \in [0,1]$。
- （输入）。一个电路 G: $\{0,1\}^{nm} \to [n] \times \{0,1\}^s$（称为预测器生成器）。
- （解）。任意显式的平坦分布 $\mathcal{D} \in (\{0,1\}^n)^m$，其大小为 m，且满足以下条件：

  令 $(i, P) \triangleq G(\mathcal{D})$，其中 P: $\{0,1\}^{i-1} \to \{0,1\}$ 被解析为描述长度为 $\le s$的电路。则

$$\Pr_{x\leftarrow\mathcal{D}}[P(x_{<i}) = x_i] < \frac{1}{2} + \delta.$$

  换句话说， P 不是一个能够以 δ优势预测 $\mathcal{D}$ 的第 i位的预测器。

[23]一个搜索问题 若它是可由随机多项式时间算法求解的 TFNP 问题，则称其属于 TFZPP .

具体而言，可以考虑参数范围 $m = n^{10}$、 $s = n^2$ 和 $\delta = 0.1$。在此情形下，长度为 n 的 m 字符串的随机分布很可能对任何规模为 s 的电路是 $o(1)$-伪随机的，因此无论输入电路 G 如何，它都必须是 Refuter(Yao) 的一个解。

概括而言，反驳者(姚期智) 要求生成一个分布 $\mathcal{D}$ ，使其对于给定的预测器生成器 G 不可预测——这是一种旨在输出预测器 P （用于 $\mathcal{D}$）的确定性算法。分布$\mathcal{D}$ 不一定要对小电路不可预测（或等价地说，伪随机）；只需骗过给定的确定性预测器生成器 G即可。因此，这属于构造定向伪随机生成器的一个特例，而已知该问题是prBPP完全的（例如，参见 [Gol11、CT21、LPT24]）。

5.1.2 与LossyCode的联系

一个密切相关的TFZPP 关系是*Lossy Code Problem*；我们将其记为LossyCode。受有界算术文献的启发（参见 [Je˘r07a，第 3 节1] 及下文讨论），该问题在 [Kor22] 中被定义为范围规避问题的一个更可行的变体；关于这项工作的介绍，见 [Kor25]及其中的参考文献。

定义 5.2. 搜索问题 LossyCode 定义如下。

- (输入)。电路 $C\colon \{0,1\}^n \to \{0,1\}^{n-1}$ 和 $D\colon \{0,1\}^{n-1} \to \{0,1\}^n$。这两个电路分别称为压缩器 和解压器。
- (输出)。一个字符串 $x \in \{0,1\}^n$ ，满足 $D(C(x)) \neq x$。

显然，LossyCode ∈TFZPP。事实上，Wilkie（未发表）和 Thapen [Tha02] 证明了该问题刻画了理论 $\forall\Sigma_1^b$ 的片段 APC_1。

定理 5.3（[*Je˘r04*，命题 *1*.14]，另见 [*LPT24*，定理 *D*.1]）。设 $\phi(x, y)$ 是 *APC* 语言中的无量词公式$_1$ ，其自由变量仅为 x 和 y 。若 $\mathit{APC}_1 \vdash \forall x\ \exists y\ \phi(x, y)$，则存在一个确定性多项式时间归约，将以下问题归约到 *LossyCode*：给定 $n \in \mathbb{N}$，输出 $m \in \mathbb{N}$ ，使得 $\phi(n, m)$ 在标准模型中为真。

此外，最近发现，一些自然的TFZPP搜索问题可以确定性归约到LossyCode 或其变体：借助因数分解预言机构造大素数 [Kor22]以及催化对数空间机器的模拟 [CLMP25]。 LossyCode 的变体与prBPP的完全去随机化和部分去随机化都相关； [LPT24] 对此有全面的介绍。

注意，假设prBPP $=$ prP，那么LossyCode 和Refuter(姚期智) 都属于函数多项式时间类。尽管如此，探究它们去随机化的相对难度仍很有意义。通过改编 [Kor22], 中的一个思路，我们证明Refuter(姚期智) 可以确定性多项式时间归约到LossyCode。因此，在证明Refuter(姚期智) ∈函数多项式时间类之前，必须先证明LossyCode ∈ 函数多项式时间类。

定理 5.4 (在 [Kor22的推论 41]证明中隐含给出）。存在一个确定性多项式时间映射归约，将带参数Refuter(姚期智) $(\delta^2/10) \cdot m \geq s + \lceil \log n \rceil + 1$ 归约到LossyCode。

证明。 注意，我们可以将 m位、汉明重量至多为 k 的字符串编码为 $\log_2 \binom{m}{k} + O(\log k)$ 比特，其中编码和解码算法的运行时间为多项式时间（例如，参见 [CLO24，引理 5。4]）。特别地，当 $k \triangleq (1/2 - \delta) \cdot m$ 且 m 足够大时，编码长度为

$$\begin{aligned} &\log_2 \binom{m}{(1/2-\delta)\cdot m} + O(\log(1/2-\delta) + \log m) \\ &\leq m + \log_2(e^{-(2\delta)^2 m/4}) + O(\log(1/2-\delta) + \log m) \\ &\leq m - (\delta^2/10) \cdot m, \end{aligned}$$

其中，第一个不等式由切尔诺夫界推出。

现在我们描述这个归约。给定任意预测器生成器 $G\colon \{0,1\}^{nm} \to [n] \times \{0,1\}^s$，考虑以下压缩器 $C\colon \{0,1\}^{nm} \to \{0,1\}^{nm-1}$和解压器 $D\colon \{0,1\}^{nm-1} \to \{0,1\}^{nm}$:

- （压缩器）。给定任意 $\mathcal{D} \in \{0,1\}^{nm}$，压缩器将其解析为一个分布，该分布定义在大小为 m 的 n 位字符串上。它计算 $(i,\ P) \triangleq G(\mathcal{D})$。如果 P未能以 δ 的优势预测 $\mathcal{D}$的第 i位，它就会失败并中止。否则，

$$\Pr_{x \leftarrow \mathcal{D}}[P(x_{<i}) = x_i] \geq \frac{1}{2} + \delta.$$

  令 y为由 $y_j \triangleq P(x_{<i}^{(j)}) \oplus x_i^{(j)}$定义的 m 比特字符串，其中 $x^{(j)}$是 $\mathcal{D}$中的第 j 个字符串。于是 y是一个汉明重量至多为 $(1/2-\delta)\cdot m$ 的字符串，因此可以用 $m-(\delta^2/10)\cdot m$ 比特高效编码。

  令 $\hat{}y$ 为其编码，$\mathcal{D}_{-i} \in \{0,1\}^{m(n-1)}$ 为从所有字符串中删除第 i 位后得到的分布 $\mathcal{D}$。压缩器输出元组 $(i,\ P,\ \hat{}y,\ \mathcal{D}_{-i})$，其长度至多为

$$\lceil \log n \rceil + s + (m - (\delta^2/10) \cdot m) + (nm - m) < nm$$

  这是由参数假设所致。

- (解压器)。当压缩器未失败时，解压器可以通过先恢复 y，再计算缺失的比特，从 $(i,\ P,\ \hat{}y,\ \mathcal{D}_{-i})$ 恢复 $\mathcal{D}$

$$x_i^{(j)} \triangleq P(x_{<i}^{(j)}) \oplus y_j.$$

给定预测器生成器 G 及上述参数，从 Refuter(Yao) 到 LossyCode 的映射归约输出 $(C,\ D)$，作为 LossyCode 的一个实例。

只需证明该归约是正确的。给定任意字符串 $\mathcal{D}$，使得 $D(C(\mathcal{D})) \neq \mathcal{D}$，由上述讨论可知，压缩器必然失败。换言之，$G(\mathcal{D})$ 无法产生具有优势 δ 的预测器。这意味着 $\mathcal{D}$ 是 Refuter(Yao) 实例的一个解，从而完成证明。□

5.1.3 见证定理

我们现在可以证明如下关于 APX_1 的见证定理：APX_1 中任何可证为全的 TFNP 问题都可确定性归约到 Refuter(Yao)。

定理 1.9（见证，针对 APX_1）。设 $\varphi(x,\ y)$ 为 PV_1 语言中的无量词公式。若$\mathrm{APX}_1 \vdash \forall x\, \exists y\, \varphi(x,\ y)$，则存在从 φ 所定义的搜索问题到 Refuter（姚期智） 的确定性多项式时间图灵归约，且其参数满足 $(\delta^2/10) \cdot m \geq s + \lceil \log n \rceil + 1$。

注意，不等式 $(\delta^2/10) \cdot m \geq s + \lceil \log n \rceil + 1$ 表明，Refuter(Yao) 实例可归约为 LossyCode，尤其是它是一个全搜索问题。对我们证明的进一步精细分析，或许能改进参数之间的权衡；这留待未来工作。

为了证明这个见证定理，我们需要全称一阶理论的标准赫布兰德定理，以及一个从APX 证明中提取预测器的引理。后者需要进行证明论分析，因此留到本节末尾讨论（参见第5.4节）。

定理 5.5（赫布兰德定理；例如参见 [Bus94]）。设 T是一个全称一阶理论，且 $\varphi(x,\ y)$是一个无量词公式，其自由变量只有 x 和 y。若 $T \vdash \forall x\, \exists y\, \varphi(x,\ y)$，则存在一个常元$c \in \mathbb{N}$以及项 $t_1,\ t_2,\ \ldots\ldots,\ t_c$使得

$$T \vdash \forall x \bigvee_{i=1}^{c} \varphi(x, t_i(y)).$$

引理 5.6（预测器提取引理）。设 $t_1(\vec{x}) = t_2(\vec{x})$ 是可在 APX 中证明的方程。则存在多项式 $k(n)$、$m(n)$，以及一个确定性多项式时间算法 E，当 n足够大时满足以下条件：

- （输入）。一个字符串 $\vec{x} \in \{0,1\}^n$，以及一个大小为 m、定义在 k 位字符串上的平坦分布 $\mathcal{D} \in (\{0,1\}^k)^m$ 。
- （项的模拟）。回顾一下，t_1, t_2 在标准模型中被解释为多项式时间P-预言机算法。我们将在输入 $\vec{x}$ 上按如下方式模拟这些算法：对于每个预言机查询P（C, Δ），其中 C： $\{0,1\}^t \to \{0,1\}$，我们将确保 $t \le k$（n） 并通过以下方式回答该查询：

$$\mathsf{P}(C, \Delta) \triangleq \Pr_{u \leftarrow \mathcal{D}}[C(u_{\le t})]. \tag{5.1}$$

  我们将模拟中 t_1 的输出记为 $t_1^{\mathcal{D}}$（$\vec{x}$），并将 t_2 的输出记为 $t_2^{\mathcal{D}}$（$\vec{x}$）。
- （输出）。假设 $t_1^{\mathcal{D}}$（$\vec{x}$） $\neq t_2^{\mathcal{D}}$（$\vec{x}$）。那么 E（$\vec{x}, \mathcal{D}$） 输出 $i \in [k$（n）$]$ 以及一个电路 P：$\{0,1\}^{i-1} \to \{0,1\}$，其规模至多为 s，使得 P 以优势 δ 预测 $\mathcal{D}$ 的第 i位，从而

$$(\delta^2/10) \cdot m(n) \ge s + \lceil \log k(n) \rceil + 1.$$

定理 *1.9* 的证明。回想一下，APX_1 具有全称公理化（见命题 2.8）。假设 $\mathsf{APX}_1 \vdash \forall x\, \exists y\, \varphi(x, y)$。根据赫布兰德定理，存在项 $t_1, \ldots, t_c$，它们属于 APX_1 的语言，并且满足

$$\mathsf{APX}_1 \vdash \forall x \bigvee_{i=1}^{c} \varphi(x, t_i(y)),$$

对某个 $c \in \mathbb{N}$ 成立。

注意，APX_1 的语言是扩展了近似计数预言机 P 的 PV 语言；因此，$t_1, \ldots, t_c$ 在标准模型中是多项式时间 P-预言机算法。令 t_φ 为 APX 中的一个项，使得

$$\mathsf{APX}_1 \vdash \bigvee_{i=1}^{c} \varphi(x, t_i(x)) \leftrightarrow t_\varphi(x, t_1(x), \ldots, t_c(x)) = 1.$$

由于 φ 是无量词公式，因此可以这样做；例如，参见 [Li25，第 3]章。于是我们知道，APX_1 证明了 $\forall x\, t_\varphi(x, t_1(x) \ldots, t_c(x)) = 1$。由于 APX_1 对 APX 是保守的（见命题 2.9），我们知道 $\mathsf{APX} \vdash t_\varphi(x, t_1(x) \ldots, t_c(x)) = 1$。

根据引理 5.6（以 $t_1 \triangleq t_\varphi(x, t_1(x) \ldots, t_c(x))$ 与 $t_2 \triangleq 1$ 进行实例化），存在 $k = k(n)$、$m = m(n)$、$s = s(n)$、$\delta = \delta(n)$ 以及一个多项式时间 E，使得以下结论成立。给定 $x \in \{0,1\}^n$ 以及一个大小为 m 的分布 $\mathcal{D} \in (\{0,1\}^k)^m$，

- 要么 $t_\varphi^{\mathcal{D}}(x, t_1^{\mathcal{D}}(x) \ldots, t_k^{\mathcal{D}}(x)) = 1$；要么
- $E(x, \mathcal{D})$ 输出 $i \in [k(n)]$ 以及 P，后者以优势 δ 预测 $\mathcal{D}$ 的第 i 位，其中 $(\delta(n)^2/10) \cdot m(n) \ge s(n) + \lceil \log k(n) \rceil + 1$。

该归约将电路 $E(x, \cdot)$ 生成为 Refuter(Yao) 的一个实例，其中大小为 $m(n)$ 的分布支撑在 $k(n)$ 位字符串上，预测器大小为 $s(n)$，优势为 $\delta(n)$。给定长度为n的 x，对于所得 Refuter(Yao) 实例 $E(x, \cdot)$ 的任意解 $\mathcal{D}$，根据定义可知 $E(x, \mathcal{D})$ 不能输出优势为 δ 的预测器。因此，上文第一条必定成立：

$$t_\varphi^{\mathcal{D}}(x, t_1^{\mathcal{D}}(x), \ldots, t_k^{\mathcal{D}}(x)) = 1.$$

随后，给定 Refuter(Yao) 实例的任意解 $\mathcal{D}$，$t_1^{\mathcal{D}}(x)\ t_2^{\mathcal{D}}(x) \ldots, t_k^{\mathcal{D}}(x)$ 中必有一个必须输出 y，使得 $\varphi(x,\ y)$ 成立。这给出了一个正确的归约，因为在给定 x 和 $\mathcal{D}$ 的显式描述后，可以在确定性多项式时间内实现对 $t_1^{\mathcal{D}}(x)\ t_2^{\mathcal{D}}(x) \ldots, t_k^{\mathcal{D}}(x)$ 的模拟。 □

5.2 与 PV_1 的关系：prBPP =prP 是否可行证明?

在本小节中，我们将提出几个关于 APX_1 与 PV_1相对强度的问题。我们将讨论这些问题的重要性，以及它们与证明 prBPP =prP 这一研究计划的联系。本文没有报告任何有意义的进展；我们认为，即使是有条件地解决这些问题，也将增进我们对可行数学和去随机化的理解。

对 prBPP = prP 的可行证明。 复杂性理论中的一个主要开放问题是，能否普遍地以多项式运行时间开销实现去随机化。Nisan、Wigderson 和 Impagliazzo 的开创性工作 [NW94、IW97] 表明，prBPP = prP 可由 E =确定性时间复杂度类$[2^n]$的指数级电路下界推出；因此，许多研究者期待得到肯定的答案。然而，尽管付出了巨大努力，prBPP =prP 以及 E 的电路下界仍然是开放问题。

从元数学的角度来看，一个有趣的问题是研究 prBPP = prP 是否能在 PV_1 这类弱算术理论中（不）得到证明。一个技术难点在于，PV_1 的语言旨在刻画 确定性多项式时间可计算函数，因此，如何形式化陈述 prBPP =prP 并非显而易见，因为该陈述涉及输入取自指数规模集合的电路的接受概率。

我们提出研究以下相关问题。

开放问题3。是否存在一个 PV 函数符号 P(C, Δ)，使得 Basic Axiom、 Boundary Axiom、Precision Consistency Axiom 和 Local Consistency Axiom能在 PV_1 中得到证明?

我们注意到，近期内不太可能得到无条件的肯定回答，因为这会立即推出prBPP =prP ，依据 PV_1 的可靠性和定理2.5。事实上，肯定回答直观上表明prBPP =prP 存在一个确定性多项式时间证明。据我们所知，目前尚不清楚肯定回答还是否定回答更为可信。

确定性陈述的可行证明去随机化。 另一方面，我们也可以考虑一种较弱的坍缩：原则上，尽管可能不存在一个 PV 函数符号 P，使得 APX_1 的相关公理可在 PV_1, 中得到证明，但引入预言机 P 并不会帮助证明任何不 涉及预言机 P 的句子。形式化地说：

开放问题4。 APX_1 在 PV_1上是保守 的吗? 换句话说，PV 语言中的每个可在 APX_1 中证明的一阶句子，是否也都可在 PV_1中证明?

显然，对开放问题3 的肯定回答意味着对开放问题 4的肯定回答。此外，对该开放问题的肯定回答将立即意味着一个改进定理 1.9的见证定理：任何APX_1 可证明全 TFNP 关系（由 PV_1语言中的无量词公式表示）都属于函数多项式时间类。这是因为 PV_1 可证明全 TFNP 问题属于函数多项式时间类（例如参见 [Oli25、第 3 节。1]）。

开放问题 4 的一个有趣特征是，它似乎与 不可比较 prBPP = prP。如果 prBPP = prP 但证明不可行，APX_1 就可能不是 PV_1的保守扩展。更有趣的是，如果开放问题 4 的答案是肯定的，我们仍不清楚是否可以推出 prBPP = prP，或任何其他非平凡的去随机化结果。形式化地说：

开放问题 5。 假设 APX_1 是 PV_1的保守扩展。能否由此推出 prBPP = prP、prBPP =prZPP，或其他任何尚未知晓的一般去随机化结果?

从宏观层面来说，这个问题是在问：如果我们想要一般性地对证明进行去随机化，是否就必须一般性地对计算进行去随机化。我们认为这些问题至关重要，值得深入研究。

5.3 与APC_1的关系

我们现在研究 APX_1 与 APC_1的相对强度。我们将证明，在形式意义上，APC_1可被视为 APX_1的扩展。然后我们将证明，APC_1 很可能是一个严格扩展，其对象为 APX_1。最后，我们介绍几个与 APC_1 和 APX_1的相对强度相关的开放问题。

5.3.1 一个上界：APC_1 扩展 APX_1

我们首先证明APX_1 的一个上界，该上界隐含于 Je$\check{\text{r}}$´abek 关于近似计数的结果[Je$\check{\text{r}}$07a]。特别地，这表明在PV_1 语言中可证的一阶句子在APC_1中也可证。

我们先在相对化理论 $\mathsf{PV}_1(\alpha)$ 的语言中定义一个句子 $\mathsf{Hard}^{\mathsf{A}}_{\varepsilon}(\alpha)$。该句子形式化表示：$\alpha(1^{2^n})$ 输出一个长度为 2^n 的真值表，并且它在平均意义下是 $2^{-\varepsilon n}$-困难的。形式化地说：

定义 5.7（[Je$\check{\text{r}}$07a，定义 2.1]）。$\mathsf{Hard}^{\mathsf{A}}_{\varepsilon}(\alpha)$ 是 $\mathsf{PV}_1(\alpha)$ 语言中的如下句子：对于每个 $n \in \mathsf{LogLog}$ 和满足 $||x|| = n$ 的 x，$\alpha(x) \in \{0,1\}^{2^n}$ 是一个布尔函数 f 在 n 个变量上的真值表，且对于每个电路 C：大小至多为 $2^{\varepsilon n}$ 的 $\{0,1\}^n \to \{0,1\}$，

$$\Pr_{x \leftarrow \{0,1\}^n}[C(x) = f(x)] \le \frac{1}{2} + \frac{1}{2^{\varepsilon n}}.$$

注意，这个概率是通过蛮力精确计数算法定义的，如 $n \in \mathsf{LogLog}$。

定义 5.8（[Je$\check{\text{r}}$07a13]，定义 2。）。理论 $\mathsf{HARD}^{\mathsf{A}}$ 定义为 PV_1（α）+ dWPHP（PV（α））+ $\mathsf{Hard}^{\mathsf{A}}_{1/4}$（$\alpha$），其中 dWPHP（PV（$\alpha$））表示关于 PV（$\alpha$）函数的对偶弱鸽巢原理。

以下定理可以使用 [Je$\check{\text{r}}$07a], 中的工具加以证明，其中 NW（$\cdot$，$\cdot$）是 Nisan-Wigderson 伪随机生成器 [NW94] 的一种实例，其硬真值表由 α（$\cdot$）提供。证明很直接，但需要熟悉 APC_1理论；为完整起见，我们在第 5.5节给出该定理的证明。

定理 5.9（模拟 P（C、Δ）与 NW（C、Δ））。对于每个 $\varepsilon < 1/3$，存在语言 PV_1（α）中的项 NW（C、Δ），使得当预言机 P（C、Δ）被替换为 NW（C、Δ）时，Basic Axiom、Boundary Axiom、Local Consistency Axiom 和 Precision Consistency Axiom 可在 $\mathsf{HARD}^{\mathsf{A}}$ 中证明。

注意到，根据 [Je$\check{\text{r}}$07a，定理 2，13], 理论 $\mathsf{HARD}^{\mathsf{A}}$ 是 APC_1的保守扩张。因此，立刻可得：

推论5.10。任何在PV_1 语言中的一阶句子，若可在APX_1 中证明，也可在APC_1中证明。

5.3.2 条件分离：APC_1 很可能强于APX_1

由于 APX_1 是一个用于多项式时间近似计数和概率推理的替代理论，一个有趣的问题是，它是否严格弱于APC_1。我们通过改编 [ILW23]中的一种技术，在合理的假设下给出了肯定的答案。

一个主要的技术工具是针对理论 [KPT91、Oli25] APX_1, 的KPT见证定理（其中“学生”由多项式规模电路实现）。形式化地说：

定义 5.11（带电路的KPT见证）。设 $\mathcal{T}$是PV_1的一个扩张。我们称 $\mathcal{T}$满足带电路的*KPT*见证性质，如果满足以下条件。设 $\varphi(\vec{x},\ y,\ z)$ 是 PV_1 语言中的任意无量词公式，且满足 $\mathcal{T} \vdash \forall \vec{x}\ \exists y\ \forall z\ \varphi(\vec{x},\ y,\ z)$。那么存在一个常元 $k \in \mathbb{N}$ 以及函数f_1，f_2，……，f_k（在标准模型中），使得以下条件成立。

对于每个向量字符串 $\vec{x}$ 以及每个 $z_1, z_2, \ldots, z_k \in \{0,1\}^*$，在标准模型中都有 t:

- 要么 $\varphi(\vec{x}, f_1(\vec{x})\ z_1)$ 为 True；
- 要么 $\varphi(\vec{x}, f_2(\vec{x}, z_1)\ z_2)$ 为 True；
- 要么 $\varphi(\vec{x}, f_3(\vec{x}, z_1, z_2)\ z_3)$ 为 True；
- $\ldots$；
- 或 $\varphi(\vec{x},\ f_k(\vec{x},\ z_1,\ \ldots\ldots,\ z_{k-1})\ z_k)$ 为 True。

此外，对于任意固定的输入长度，$\vec{x}$、f_1，……，f_k都可以由多项式规模确定性电路计算。

定理 5.12 (针对 APX_1 的 KPT 见证。APX_1 具有带电路的*KPT*见证性质。

该定理可利用标准的KPT见证定理证明（例如参见 [Oli25，定理 3。2]），以及电路接受概率问题可由（非一致的）多项式规模电路求解这一事实。[24] 换言之，定理 5.12 成立，因为我们可以将一列显式伪随机分布硬编码进去，以实现近似计数预言机 P。由于论证是标准的，我们将定理的证明推迟到第 5.6 节。

我们将使用以下结果，该结果隐含在 [ILW23的证明中，定理 24]；有关假设的精确表述，请读者参阅[ILW 23] 。

定理 5.13 （隐含于 [ILW23，定理 24]）。假设存在 *JLS* 安全的 $i\mathcal{O}$，且coNP 不被NP/poly无穷多次包含。对于任意 $\mathcal{T}$ 扩张PV_1 且满足带电路的*KPT*见证性质的理论，存在一个 $\forall\Sigma^b_2$ *PV*语言中的句子[1] ，它可在APC[1]，中证明，但在 $\mathcal{T}$ 中不可证明。

证明概要。 [ILW23，定理 24] 仅针对一个名为UAPC_1的理论证明了该定理。尽管如此，仔细检查后可以发现，证明中用到的该理论的唯一性质是UAPC_1 满足带电路的KPT见证性质（见 [ILW23，定理 25]）。 □

结合定理 5.12 和5.13，可立即得出：

推论 5.14. 假设存在 *JLS* 安全的 $i\mathcal{O}$，且coNP 并非无穷多次包含于NP/poly。存在一个 $\forall\Sigma^b_2$ 句子，属于 PV_1 语言，它可在APC_1，中证明，但无法在APX_1中证明。

5.3.3 一个开放问题：能否进一步分离?

推论 5.14 表明 APC_1 很可能严格强于 APX_1。换言之，在计算假设下，存在 $\forall\Sigma^b_2$(PV) 句子可在 APC_1 中证明，却无法在 APX_1中证明。一个引人关注的开放问题是，APC_1 是否严格强于 APX_1，就 $\forall\Sigma^b_1$(PV) 句子而言：

开放问题 6. 是否存在一个 $\forall\Sigma^b_1$ 句子，属于 PV_1 语言，可在 APC_1，中证明但无法在 APX_1中证明？换言之，是否存在一个可在 APC_1 中证明为全函数的 TFNP 问题（属于 PV 语言），但无法在 APX_1中证明为全函数?

由于 LossyCode 刻画了 $\forall\Sigma^b_1$-片段的 APC_1 （见定理 5.3），而Refuter(姚期智) 刻画了$\forall\Sigma^b_1$-片段的 APX_1 （见定理 1.9），伪随机性理论中一个相关的问题是，去随机化LossyCode 是否比去随机化 Refuter(姚期智) 更难。形式化地说：

开放问题 7。 是否存在从 LossyCode 到 Refuter(姚期智) 的确定性多项式时间归约？换句话说，定理 5.4的逆命题是否成立?

我们注意到，这两个开放问题在技术上互不包含。例如，对开放问题 7 的肯定回答未必会对开放问题 6 给出否定回答，除非它有一个可行的正确性证明。尽管如此，可以设想，为其中一个问题发展出的技术很可能也对另一个问题有用。

5.4 预测器提取引理：引理的证明5.6

引理 5.6 （预测器提取引理）。 设 $t_1(\vec{x}) = t_2(\vec{x})$ 是一个可在 APX 中证明的方程。那么，存在多项式 $k(n)$、$m(n)$，以及一个确定性多项式时间算法 E，当 n 足够大时，它们满足以下条件：

- (输入)。一个字符串 $\vec{x} \in \{0,1\}^n$ 和一个平坦分布 $\mathcal{D} \in (\{0,1\}^k)^m$，其大小为 m，定义在 k 位字符串上。

[24]一个类似的KPT见证定理在 [PS21，定理 4] （另见 [ILW23，定理 25]）中针对理论PV_1+ “一致dWPHP（PV）”得以证明，该理论可能与APX_1不可比较。

- （项的模拟）。回顾一下， t_1和t_2 在标准模型中被解释为多项式时间的P-预言机算法。我们将按如下方式模拟这些算法在输入 $\vec{x}$ 上的运行：对于每个预言机查询P（C、 Δ），其中 C： $\{0,1\}^t \to \{0,1\}$，我们将确保 $t \le k$（n），并通过以下方式回答该查询

$$\mathsf{P}(C,\Delta) \triangleq \Pr_{u \leftarrow \mathcal{D}}[C(u_{\le t})]. \tag{5.1}$$

  我们将模拟中 t_1 的输出记为 $t_1^{\mathcal{D}}$（$\vec{x}$），并将 t_2 的输出记为 $t_2^{\mathcal{D}}$（ $\vec{x}$).

- （输出）。假设 $t_1^{\mathcal{D}}$（$\vec{x}$） $\neq t_2^{\mathcal{D}}$（$\vec{x}$）。那么， E（$\vec{x}$、$\mathcal{D}$）输出 $i \in [k$（n）$]$，并且存在一个电路 P：$\{0,1\}^{i-1} \to \{0,1\}$，其 ***Size*** 至多为 s，使得 P 以优势 δ 预测 $\mathcal{D}$ 的第 i 位，满足

$$(\delta^2/10) \cdot m(n) \ge s + \lceil \log k(n) \rceil + 1.$$

在证明这一引理之前，我们先简要解释其直观含义。回顾一下，APX的定义是在PV（P）的基础上加入以下公理进行扩展： Basic Axiom、 Boundary Axiom、 Local Consistency Axiom和 Precision Consistency Axiom。一个APX 方程 t_1（x） $= t_2$（x）的证明，从较高层次来看，是对以下陈述的证明：对于预言机P的每一种解释，要么 t_1（x） $= t_2$（x），要么预言机P不满足其中一条公理。

对于引理 P 5.6中预言机 的具体实现， Basic Axiom、 Boundary Axiom 和 Precision Consistency Axiom总是成立，因此只有 Local Consistency Axiom可能被违反。在这种情况下，对于一个电路 C： $\{0,1\}^t \to \{0,1\}$ 以及字符串 Δ、B（在 APX 证明中构造），使得

$$\left| \Pr_{u \leftarrow \mathcal{D}}[C(u_{\le t})] - \frac{1}{2}\left(\Pr_{u \leftarrow \mathcal{D}}[C(u_{<t}0)] + \Pr_{u \leftarrow \mathcal{D}}[C(u_{<t}1)] \right) \right| > 2 \cdot \frac{1}{|\Delta|} + \frac{1}{|B|},$$

沿用 Yao 引理证明中的类似论证（例如参见 [AB09，第 9]章或第 4.1 节），我们可以通过确定性多项式时间算法，从 C 构造出一个预测器。

从概念上看，该论证的关键在于揭示：不仅可以像 Yao 引理的标准表述那样，利用区分某个分布与随机字符串的能力来构造预测器；还可以利用在将该分布用作近似计数的随机源时检测局部不一致性的能力来构造预测器。这一视角或许本身也具有独立的研究价值。

为了将这一直觉付诸实现，我们通过细致的证明论分析来证明该引理。具体而言，我们将通过对5.6 引理的APX 证明 π 进行归纳，证明方程 $t_1(x) = t_2(x)$。函数ℓ， k， m， s， δ以及算法 E将根据 π所用的最后一条规则或公理，以及由归纳假设得到的函数和算法来确定。

引理 5.6 的证明。我们将证明一个更强的命题：对于任意可证方程 $e(x)$： $t_1(\vec{x}) = t_2(\vec{x})$，都存在非递减多项式 $k_0(n)$ $m_0(n)$，使得当函数 $m(n)$ 为非递减函数时，该引理对所有多项式 $k(n) \ge k_0(n)$ 和 $m(n) \ge m_0(n)$ 均成立。我们通过对证明长度进行归纳来证明这一点。

考察证明最后一行中用于推出 $e(x)$ 的公理或规则。

基本公理。假设 e 是 PV(P) 中的一个可证方程，并且它是通过 Basic Axiom引入的。[25]那么，对于 P 的任意解释以及任意字符串 x， $e(x)$必须为真。我们将 $k_0(n)$设置得足够大，使得对每一个 C：在 $x \in \{0,1\}^n$上的模拟 $t_1^{\mathcal{D}}(\vec{x})$ $t_2^{\mathcal{D}}(\vec{x})$中被查询的 $\{0,1\}^t \to \{0,1\}$，都有 $t \le k_0(n)$；这是可能的，因为 t_1、t_2 是多项式时间预言机算法。我们将其他函数和 E 任意设置，因为$t_1^{\mathcal{D}}(\vec{x}) = t_2^{\mathcal{D}}(x)$始终成立。

假设 e 是编码 $\mathsf{P}(C,\Delta) \in \mathbb{Q}$、$\mathsf{P}(C,\Delta) \le 1$或 $\mathsf{P}(C,\Delta) \ge 0$的方程之一，其中 C、Δ是自由变量。令 $k_0(n) \triangleq n$ 且 $m_0(n) = 1$。与前一情形类似，可以看出，对于任意 $k(n) \ge k_0(n)$ 以及 $m(n) \ge m_0(n)$，若我们按照公式 (5.1) 解释 P，则 $e(\vec{x})$必须为真。我们可以任意设置其他函数和 E，因为 $t_1^{\mathcal{D}}(\vec{x}) = t_2^{\mathcal{D}}(\vec{x})$始终成立。

[25]请注意，我们的证明并不考察 e 的 PV(P) 证明；只要 e 是一个 PV(P) 可证方程，该证明就成立。

边界公理。假设 $e(\vec{x})$ 是一个方程编码，表示对于任意电路 $C \in B_n$，$\mathsf{IsConst}(C) \to \mathsf{P}(C, \Delta) = \mathsf{Bool}(C)$。请注意，$C$ 和 Δ 是该方程仅有的自由变量。我们可以任意设置 $k_0(n) = n$ 和 $m_0(n) = 1$。对于每个 $k(n) \geq k_0(n)$ 和 $m(n) \geq m_0(n)$，我们都可以任意设置 E。

这是正确的，因为对于每个 $(C, \Delta) \in \{0,1\}^n$ 以及每个大小为 $\mathcal{D}$ 的分布 $m(n)$，定义在 $k(n) \geq n$ 比特上，当我们将 P 解释为方程 (5.1) 时，如果 $C\colon \{0,1\}^t \to \{0,1\}$ 是一个常值电路，则有 $t \leq n \leq k(n)$，并且

$$\mathsf{P}(C, \Delta) = \Pr_{u \leftarrow \mathcal{D}}[C(u_{\leq t})] = \mathsf{Bool}(C).$$

换句话说，$t_1^{\mathcal{D}}(C, \Delta) = t_2^{\mathcal{D}}(C, \Delta)$ 总是成立。

精度一致性公理。 这与 Boundary Axiom 的情形类似。事实上，当将预言机 P 解释为方程 (5.1) 时，$\mathsf{P}(C, \Delta_1) = \mathsf{P}(C, \Delta_2)$ 对于 任意 Δ_1, Δ_2。

局部一致性公理。 在这种情况下，$e(\vec{x})$ 是对以下句子的方程编码：对于每个电路 $C\colon \{0,1\}^t \to \{0,1\}$ 以及字符串 Δ, B，有

$$\left| \mathsf{P}(C, \Delta) - \frac{\mathsf{P}(\mathsf{Fix}_0(C), \Delta) + \mathsf{P}(\mathsf{Fix}_1(C), \Delta)}{2} \right| \leq \frac{2}{|\Delta|} + \frac{1}{|B|},$$

其中，$\mathsf{Fix}_\sigma(C)$ 是一个 PV 项，它输出的电路是将 C 的最右侧输入位置固定为 $\sigma \in \{0,1\}$ 后得到的。在此方程中，C、Δ、B 是仅有的自由变量。设 $k_0(n)$ 和 $m_0(n)$ 为稍后确定的多项式。

设 $k(n) \geq k_0(n)$ 和 $m(n) \geq m_0(n)$。设 $\vec{x} = (C, \Delta, B) \in \{0,1\}^n$ 和 $\mathcal{D} \in (\{0,1\}^{k(n)})^{m(n)}$。假设 $t_1^{\mathcal{D}}(\vec{x}) \neq t_2^{\mathcal{D}}(\vec{x})$。由于预言机 P 是按照公式 (5.1) 解释的，我们有

$$\left| \Pr_{u \leftarrow \mathcal{D}}[C(u_{\leq t})] - \frac{\Pr_{u \leftarrow \mathcal{D}}[C(u_{<t}0)] + \Pr_{u \leftarrow \mathcal{D}}[C(u_{<t}1)]}{2} \right| > \frac{2}{|\Delta|} + \frac{1}{|B|} \geq \frac{1}{n}.$$

这意味着

$$\begin{aligned} &\frac{1}{2} \left| \Pr_{u \leftarrow \mathcal{D}}[C(u_{<t}u_t)] - \Pr_{u \leftarrow \mathcal{D}}[C(u_{<t}\overline{u_t})] \right| \\ &= \left| \Pr_{u \leftarrow \mathcal{D}}[C(u_{\leq t})] - \frac{\Pr_{u \leftarrow \mathcal{D}}[C(u_{<t}u_t)] + \Pr_{u \leftarrow \mathcal{D}}[C(u_{<t}\overline{u_t})]}{2} \right| \\ &= \left| \Pr_{u \leftarrow \mathcal{D}}[C(u_{\leq t})] - \frac{\Pr_{u \leftarrow \mathcal{D}}[C(u_{<t}0)] + \Pr_{u \leftarrow \mathcal{D}}[C(u_{<t}1)]}{2} \right| \geq \frac{1}{n}, \end{aligned} \tag{5.2}$$

其中，在第二个相等式中，我们用到了期望的线性性，并且对每个固定的 u，$C(u_{<t}u_t) + C(u_{<t}\overline{u_t}) = C(u_{<t}0) + C(u_{<t}1)$。

为简单起见，我们只考虑这种情况：

$$\Pr_{u \leftarrow \mathcal{D}}[C(u_{<t}u_t)] - \Pr_{u \leftarrow \mathcal{D}}[C(u_{<t}\overline{u_t})] \geq \frac{2}{n}, \tag{5.3}$$

并且 另一种情况也可以相应地解决。我们可以将上述方程改写如下 s:

$$\begin{aligned} &\left(\Pr_{u \leftarrow \mathcal{D}}[C(u_{<t}0) \oplus 1 = u_t \wedge u_t = 0] - \Pr_{u \leftarrow \mathcal{D}}[C(u_{<t}0) \oplus 1 \neq u_t \wedge u_t = 1] \right) \\ &+ \left(\Pr_{u \leftarrow \mathcal{D}}[C(u_{<t}1) \oplus 1 \neq u_t \wedge u_t = 1] - \Pr_{u \leftarrow \mathcal{D}}[C(u_{<t}1) \oplus 1 = u_t \wedge u_t = 0] \right) \geq \frac{2}{n}. \end{aligned}$$

因此，左侧的项中必有一项至少为 $1/n$。同样，我们只考虑第一项至少为 $1/n$ 的情况，另一项则可相应地确定。

注意，

$$\begin{aligned}
&\Pr_{u\leftarrow\mathcal{D}}[C(u_{<t}0)\oplus 1=u_t\wedge u_t=0]-\Pr_{u\leftarrow\mathcal{D}}[C(u_{<t}0)\oplus 1\neq u_t\wedge u_t=1]\\
=&\Pr_{u\leftarrow\mathcal{D}}[C(u_{<t}0)\oplus 1=u_t\wedge u_t=0]+\Pr_{u\leftarrow\mathcal{D}}[C(u_{<t}0)\oplus 1=u_t\wedge u_t=1]-\Pr_{u\leftarrow\mathcal{D}}[u_t=1]\\
=&\Pr_{u\leftarrow\mathcal{D}}[C(u_{<t}0)\oplus 1=u_t]-\Pr_{u\leftarrow\mathcal{D}}[u_t=1]\geq\frac{1}{n}.
\end{aligned}$$

随后，$\mathbf{Pr}_{u\leftarrow\mathcal{D}}[u_t=1]\leq 1/2-1/(2n)$ 或 $\mathbf{Pr}_{u\leftarrow\mathcal{D}}[C(u_{<t}0)\oplus 1=u_t]\geq 1/2+1/(2n)$。无论哪种情况——由于 $\mathcal{D}$ 是明确给出的，我们可以高效地判断属于哪种情况——都可以构造一个大小至多为 $|C|\leq s\triangleq n$ 的电路，用前（$t-1$）个比特以至少 $\delta\triangleq 1/(2n)$ 的优势预测 $\mathcal{D}$ 的第 t 个比特。令 $m_0(n)\triangleq n^4$ 且 $k_0(n)\triangleq n$，即可确保

$$(\delta^2/10)\cdot m(n)\geq s+\lceil\log k(n)\rceil+1$$

当 n 充分大时。

逻辑规则。我们只考虑代换规则 $t_1=t_2\vdash t_1(x/t)=t_2(x/t)$；其他逻辑规则可相应地处理。在这种情况下，$e(\vec{x})$ 的形式为 $t_1(x/t)=t_2(x/t)$，其中 t 是一个项，而 x 是 t_1 和 t_2的一个自由变量，并且前提 $t_1=t_2$存在一个更短的证明。不失一般性，我们假设变量 x 不出现在项 t中。

令 $\vec{y}$ 为 t 中有而 t_1、t_2、$\vec{z}$ 中有而 t_1、t_2（不包括 x）中没有的自由变量，并令 $\vec{w}$ 为 t 和 t_1、t_2（不包括 x）共有的自由变量。根据归纳假设，存在多项式 $k'_0(n)$ 和 $m'_0(n)$，使得对于任意多项式 $k'(n)$、$\geq k'_0(n)$、$m'(n)$ 和 $\geq m'_0(n)$，都存在 $\delta'(n)$、$s'(n)$，以及一个算法 $E'(\vec{x}、\mathcal{D})$，满足方程对应的引理

$$t_1(x,\vec{z},\vec{w})=t_2(x,\vec{z},\vec{w}).\tag{5.4}$$

令 $\ell(n)$ 为 t 的输出长度上界，条件是输入长度至多为 n（这称为该项的 界定值，参见 [Coo75]）。我们定义 $k_0(n)\triangleq k'_0(n+\ell(n))$ 和 $m_0(n)\triangleq m'_0(n+\ell(n))$。

为证明这一点，任取 $k(n)\geq k_0(n)$ 和 $m(n)\geq m_0(n)$，并令 $s(n)$ $\delta(n)$ 在稍后确定。算法 E 的工作方式如下。给定任意 $(\vec{y},\ \vec{z},\ \vec{w})\in\{0,1\}^n$ 和 $\mathcal{D}\in(\{0,1\}^{k(n)})^{m(n)}$，使得

$$t_1^{\mathcal{D}}(t(\vec{y},\vec{w}),\vec{z},\vec{w})\neq t_2^{\mathcal{D}}(t(\vec{y},\vec{w}),\vec{z},\vec{w}),\tag{5.5}$$

我们的目标是输出一个预测器，以大小为 $s(n)$、优势为 $\delta(n)$ 预测 $\mathcal{D}$ 的一个比特。

算法首先计算 $x_{\mathcal{D}}\triangleq t^{\mathcal{D}}(\vec{y},\ \vec{w})$，这是一个长度至多为 $\ell(n)$ 的字符串。根据方程 (5.5) 以及模拟的定义，

$$t_1^{\mathcal{D}}(x_{\mathcal{D}},\vec{z},\vec{w})\neq t_2^{\mathcal{D}}(x_{\mathcal{D}},\vec{z},\vec{w}).$$

随后，根据归纳假设（函数为 $k'(n+\ell(n))\geq k(n)$ 和 $m'(n+\ell(n))\geq m(n)$），$E'((x_{\mathcal{D}},\ \vec{z},\ \vec{w})\ \mathcal{D})$ 输出 (i,P)，使得 P 是一个大小为 s 的电路，能以优势δ 预测 $\mathcal{D}$ 的第 i 位，其中

$$((\delta^2/10)\cdot m'(n+\ell(n))\geq s+\lceil\log k'(n+\ell(n))\rceil+1.$$

只需定义 $E((\vec{y},\ \vec{z},\ \vec{w})\ \mathcal{D})\triangleq E'((x_{\mathcal{D}},\ \vec{z},\ \vec{w})\ \mathcal{D})$。

归纳规则。在这种情况下，e 具有如下形式：$f_1(x,\vec{y})=f_2(x,\vec{y})$，其中 PV(P) 函数 f_1,f_2，并且存在PV(P) 函数 g,h_0,h_1 使得存在以下方程的更短证明：

$$f_j(\varepsilon,\vec{y})=g(\vec{y})\tag{5.6}$$
$$f_j(s_i(x),\vec{y})=h_i(x,\vec{y},f_j(x,\vec{y}))\tag{5.7}$$

对于 $j \in \{1,2\}$ 和 $i \in \{0,1\}$。根据归纳假设，上述 6 个方程中的每一个都满足该引理。设 $k_0(n)$ 和 $m_0(n)$ 是待确定的多项式。对于任意多项式 $k(n) \geq k_0(n)$ 和 $m(n) \geq m_0(n)$，我们将设计一个算法 E，该算法在给定 $(x, \vec{y}) \in \{0,1\}^n$ 和满足以下条件的 $\mathcal{D} \in (\{0,1\}^{k(n)})^{m(n)}$

$$f_1^{\mathcal{D}}(x, \vec{y}) \neq f_2^{\mathcal{D}}(x, \vec{y}),$$

它输出 (i, P)，其中 P是一个大小为 s的电路，能够以 δ的优势预测 $\mathcal{D}$的第 i位，满足 $(\delta^2/10) \cdot m(n) \geq s + \lceil \log k(n) \rceil + 1$。

情况 1。假设 $f_1^{\mathcal{D}}(\varepsilon, \vec{y}) \neq f_2^{\mathcal{D}}(\varepsilon, \vec{y})$。那么存在 $j \in \{1,2\}$ 使得 $f_j^{\mathcal{D}}(\varepsilon, \vec{y}) \neq g^{\mathcal{D}}(\vec{y})$。注意到 $\vec{y}$ 的长度至多为 n。由于方程 (5.6) 有一个更短的证明，根据归纳假设，存在多项式 $k_0^{(j)}(n')$ $m_0^{(j)}(n')$，使得当

$$k(n') \geq k_0^{(j)}(n'), \quad m(n') \geq m_0^{(j)}(n'), \tag{5.8}$$

那么 $E_j(\vec{y}, \mathcal{D})$ 输出一个大小为 s 的预测器，其优势为 δ，满足 $(\delta^2/10) \cdot m(n') \geq s + \lceil \log k(n') \rceil + 1$，其中 n' 表示 $\vec{y}$的输入长度。接下来只需定义

$$E((x, \vec{y}), \mathcal{D}) \triangleq E_j(\vec{y}, \mathcal{D})$$
$$k_0(n) \triangleq k_0^{(j)}(n) \in \mathsf{poly}(n), \quad m_0(n) \triangleq m_0^{(j)}(n) \geq m_0^{(j)}(n').$$

情况 2. 令 $t \triangleq |x|$。算法 E首先找出第一个索引 $i \leq t$，使得 $f_1^{\mathcal{D}}(x_{\leq i}, \vec{y}) = f_2^{\mathcal{D}}(\vec{x}_{\leq i}, \vec{y})$，但 $f_1^{\mathcal{D}}(x_{\leq i+1}, \vec{y}) \neq f_2^{\mathcal{D}}(\vec{x}_{\leq i+1}, \vec{y})$；这样的索引必定存在，因为 $f_1^{\mathcal{D}}(\varepsilon, \vec{y}) = f_2^{\mathcal{D}}(\varepsilon, \vec{y})$，且 $f_1^{\mathcal{D}}(x, \vec{y}) \neq f_2^{\mathcal{D}}(x, \vec{y})$。令 $\sigma \triangleq x_{i+1}$。那么存在 $j \in \{1,2\}$，使得

$$f_j^{\mathcal{D}}(s_\sigma(x_{\leq i}), \vec{y}) \neq h_\sigma^{\mathcal{D}}(x_{\leq j}, \vec{y}, f_j^{\mathcal{D}}(x_{\leq i}, \vec{y})).$$

也就是说，当近似计数预言机$x_{\leq j}$, $\vec{y}$)P 按照 $\mathcal{D}$，依据方程 (5.1) 实现时，长度至多为 n 的字符串 (5.7) 违反方程 (。根据应用于方程 (5.7) 的归纳假设，存在多项式 $k_0'(n)$ 和 $m_0'(n)$，使得当

$$k(n) \geq k_0'(n), \quad m(n) \geq m_0'(n), \tag{5.9}$$

存在一个算法 E'，使得 $E'((x_{\leq i}, \vec{y}) \mathcal{D})$ 输出一个大小为-s 的预测器，其优势为 δ，使得 $(\delta^2/10) \cdot m(n) \geq s + \lceil \mathsf{Log}\ k(n) \rceil + 1$。接下来只需定义 $E((x, \vec{y}) \mathcal{D}) \triangleq E'((x_{\leq i}, \vec{y}) \mathcal{D})$。

总结。最后，我们令 $k_0(n)$ 和 $m_0(n)$ 为充分大的多项式，使得当$k(n) \geq k_0(n)$ 且 $m(n) \geq m_0(n)$ 时，方程 (5.8) 和 (5.9) 均成立。因此，在任一情况下，算法E 都满足该引理的要求。

□

Remark 5.15. 通过仔细检查证明，我们注意到，多项式 $k_0(n)$ $m_0(n)$（它们定义了分布 $\mathcal{D}$ 的最小大小）以及 E 的运行时间取决于 APX 证明；特别是，它们可能远远超过方程 e 中项 t_1, t_2 的运行时间。

例如，在逻辑规则的情形下，$k_0(n)$ 被定义为 $k_0'(n + \ell(n))$，其中 $\ell(n)$ 是证明中某个项 t 的输出长度（即界定值），而项 t 不一定会出现在最终方程中。从较高层次来看，这是因为我们需要将分布 $\mathcal{D}$ 设置得足够大，以容纳 APX 证明中的 *all oracle*queries LOCAL CONSISTENCY AXIOM；随后我们可以检查证明，找出对该规则的违反，从而得到一个预测器。

5.5 使用 $\mathsf{P}(C,\Delta)$ 模拟 $\mathsf{NW}(C,\Delta)$：定理 5.9 的证明

我们沿用 [Je˘r07a]中的记号。集合 X 称为由电路定义的有界集合 C，如果$X=\{x<a\mid C\left(x\right)。=1\}$我们使用 $x\in X$ 表示公式 $x<a\wedge C\left(x\right)$，$=1$并使用 $X\subseteq b$ 表示公式 $\forall x\in X\ x<b$。请注意，有界可定义集并不是理论 APC_1，中的对象，而是元理论中的一种缩写。对于两个有界可定义集 $X\subseteq a$ 和 $Y\subseteq b$，我们定义

$$X\times Y\triangleq\{bx+a\mid x\in X,y\in Y\}\subseteq ab,$$
$$X\cup Y\triangleq X\cup\{y+a\mid y\in Y\}\subseteq a+b.$$

我们称 $C\colon\ X\to Y$，若 C 是从 X 到 Y 的电路，也就是说，对每个 $x\in X$，$C(x)\in Y$。我们称 $C\colon X\hookrightarrow Y$，若电路 $C\colon\ X\to Y$ 是单射，也就是说，对于 $x_1,x_2\in X$，$x_1\neq x_2$，$C(x_1)\neq C(x_2)$。我们用 $C\colon X\twoheadrightarrow Y$ 表示 C 是满射，也就是说，对所有 $y\in Y$，存在一个 $x\in X$，使得 $C(x)=y$。

定义 5.16 (在 PV_1 中)。设 $X,Y\subseteq 2^n$ 为可定义集合，且 $\varepsilon\leq 1$。我们称 X 比 Y 小 ε-近似，记作 $X\lesssim_\varepsilon Y$，若存在一个电路 G 和 $v\neq 0$，使得

$$G:v\times(Y\cup\varepsilon 2^n)\twoheadrightarrow v\times X.$$

定义 5.17 （在 PV_1 中）。我们称 X 和 Y 的大小近似相等到 ε，记作 $X\approx_\varepsilon Y$，若 $X\lesssim_\varepsilon Y$ 且 $Y\lesssim_\varepsilon X$。特别地，若 $X\approx_\varepsilon s$，则称 X 的大小近似为 ε，记作 s 。

引理 5.18 ([Je˘r07a，引理 2。10])。设 X，Y，X'，Y'，$Z\subseteq 2^n$ 和 W，$W'\subseteq 2^n$ 为有界可定义集，且 ε，$\delta\leq 1$。以下陈述可在 PV_1 中证明。

(1) 若 $X\lesssim_\varepsilon Y$、$\varepsilon\leq\delta$，则 $X\lesssim_\delta Y$。*(2)* 若 $X\lesssim_0 Y$，则 $X\lesssim_\varepsilon Y$。*(3)* 若 $X\lesssim_\varepsilon Y$、$Y\lesssim_\delta Z$，则 $X\lesssim_{\delta+\varepsilon} Z$。*(4)* 若 $X\lesssim_\varepsilon X'$、$Y\lesssim_\delta Y'$，且 X'、Y' 可由集合 W 分离（即 $X'\subseteq W$ 且 $Y'\subseteq 2^n\setminus W$），则 $X\cup Y\lesssim_{\varepsilon+\delta} X'\cup Y'$。*(5)* 若 $X\lesssim_\varepsilon X'$、$W\lesssim_\delta W'$，则 $X\times W\lesssim_{\varepsilon+\delta+\varepsilon\delta} X'\times W'$。

引理 5.19 ([Je˘r07a, 引理 2.11])。设 X，$Y\subseteq 2^n$ 是有界可定义集，s，t，$u\leq 2^n$，ε，δ，η，$\xi\leq 1$，且 $\xi^{-1}\in$Log。以下命题可在APC_1中证明。

(1) 存在 $s\leq 2^n$ 使得 $X\approx_\xi s$。*(2)* $s\lesssim_\varepsilon X\lesssim_\delta t$ 蕴含 $s\leq t+(\varepsilon+\delta+\xi)\cdot 2^n$。*(3)* $X\lesssim_\xi Y$ 或 $Y\lesssim_\xi X$。*(4)* $X\lesssim_\varepsilon Y$ 蕴含 $2^n\setminus Y\lesssim_{\varepsilon+\xi} 2^n\setminus X$。*(5)* $X\approx_\varepsilon s$、$Y\approx_\delta t$、$X\cap Y\approx_\eta u$ 蕴含 $X\cup Y\approx_{\varepsilon+\delta+\eta+\xi} s+t-u$。

引理 5.20 (隐含于 [Je˘r07a，引理 2。14])。设 $\varepsilon<1/3$。存在一个 $\mathsf{PV}(\alpha)$ 函数 $\mathsf{Size}(\cdot,\cdot)$ 使得以下命题可在 $\mathsf{HARD}^{\mathsf{A}}$中证明：对每个 $n,\delta^{-1}\in$Log 以及由电路 $X\subseteq 2^n$ 定义的集合C：$\{0,1\}^n\to\{0,1\}$，以下结论成立：

- $0\leq\mathsf{Size}(C,1^{\delta^{-1}})\leq 2^n$;
- $X\approx_\delta\mathsf{Size}(C,1^{\delta^{-1}})$;
- 若 C 是一个始终输出 0 (分别为 1) 的常值电路，则 $\mathsf{Size}(C,\Delta)=0$ (分别为 $\mathsf{Size}(C,\Delta)=2^n$)。

证明概要。我们假设读者对 [Je˘r07a]有一定了解。引理的前两个要点对于仅以一个 $\mathsf{PV}(\alpha)$ 函数符号作为非一致性的情况成立，其中 [Je˘r07a，定理 2。7]是对困难函数的选择，该函数由 α给出。最后一个要点成立，是因为 $\mathsf{Size}(C,\Delta)$ 是通过计算C 在由 Nisan-Wigderson 伪随机生成器生成的伪随机分布上的接受概率得到的；对于始终接受（分别地，拒绝）的电路，它在任何分布上的接受概率始终为 1（分别地，0）。

我们建议感兴趣的读者参阅 [ILW23，附录 D]，其中完整地给出了[Je˘r07a，定理 27]的证明。□

定理 *5.9*（用 *NW(C, Δ)* 模拟 *P(C, Δ)*）。对于每个 $\varepsilon < 1/3$，*PV*$_1$*(α)* 语言中都存在一个项 *NW(C, Δ)*，使得当预言机 *P(C, Δ)* 被替换为 *NW(C, Δ)* 时，Basic Axiom、Boundary Axiom、Local Consistency Axiom 和 Precision Consistency Axiom 可在 *HARD*^{A} 中证明。

证明。令 $\mathsf{Size}(\cdot,\cdot)$ 表示引理 5.20 中的函数。我们定义 $\mathsf{NW}(C,\Delta) \triangleq \mathsf{Size}(C, 1^{|\Delta|})/2^n$，其中 $C\colon \{0,1\}^n \to \{0,1\}$ 是一个电路。注意，我们可以使用n 二进制位精确地编码有理数 $\mathsf{Size}(C, 1^{|\Delta|})/2^n$，因此不存在舍入问题；回顾 APX 的定义，P 的输出长度可能大至 $|C| \cdot |\Delta|^2 > n$（见第 2.1 节）。

只需验证　　公理可在 $\mathsf{HARD}^{\mathsf{A}}$ 中证明。在证明的其余部分，我们在 $\mathsf{HARD}^{\mathsf{A}}$ 中进行论证　　.

- (Basic Axiom)。这直接由引理 5.20 的第一条得出。
- (Boundary Axiom)。这直接由引理 5.20 的第三条得出。
- (Local Consistency Axiom)。令 $C\colon \{0,1\}^n \to \{0,1\}$ 为一个电路，Δ，B 为满足 $\delta = 1/|\Delta|$、$\beta = 1/|B|$、$C_0 \triangleq \mathsf{Fix}_0(C)$ $C_1 \triangleq \mathsf{Fix}_1(C)$ 的字符串。我们需要证明

$$\left|\mathsf{NW}(C,\Delta) - \frac{\mathsf{NW}(C_0,\Delta) + \mathsf{NW}(C_1,\Delta)}{2}\right| \le \delta + \beta. \tag{5.10}$$

令 X、X_0、$X_1 \subseteq \{0,1\}^n$ 分别为由 C、C_0、C_1定义的有界集合。令 $s \triangleq \mathsf{Size}(C,\ 1^{|\Delta|})$、$s_0 = \mathsf{Size}(C_0,\ 1^{|\Delta|})$、$s_1 \triangleq \mathsf{Size}(C_1,\ 1^{|\Delta|})$。根据引理 5.20的第二条，我们知道

$$X \approx_\delta s, \quad X_0 \approx_\delta s_0, \quad X_1 \approx_\delta s_2.$$

注意，由于 $X_0 \cap X_1 = \varnothing$，我们有 $X_0 \cap X_1 \approx_0 0$。根据引理 5.19 (5)，$X_0 \cup X_1 \approx_{2\delta} s_0 + s_1$。令 $f\colon v_1(s+\delta\cdot 2^n) \twoheadrightarrow v_1 \times X$ 为 $X \lesssim_\delta s$ 的见证，并令 $g\colon v_2 \times ((X_0 \cup X_1) \uplus 2\delta \cdot 2^{n-1}) \twoheadrightarrow v_2(s_0+s_1)$ 为 $s_0 + s_1 \lesssim_{2\delta} X_0 \cup X_1$ 的见证。我们定义一个函数 h

$$h : v_1 v_2(s + 2\delta \cdot 2^n) \twoheadrightarrow v_1 v_2(s_0 + s_1)$$

如下：

(i) 令 $i_1 < v_1, i_2 < v_2, j < s + \delta \cdot 2^n$，元组 $(i_1, i_2, j) \in v_1 v_2(s + 2\delta \cdot 2^n)$。我们计算 $(i_1', x) \triangleq f(i_1, j) \in v_1 \times X$，其中 $x_{\le n-1} \in X_0 \cup X_1$。随后，算法计算 $(i_2', j') \triangleq g(i_2, x_{\le n-1}) \in v_2(s_0 + s_1)$，并输出 $h(i_1, i_2, j) \triangleq (i_1', i_2', j')$。(ii) 令 $i_1 < v_1, i_2 < v_2, s + \delta \cdot 2^n \le j < s + 2\delta \cdot 2^n$，元组 $(i_1, i_2, j) \in v_1 v_2(s + 2\delta \cdot 2^n)$。注意，$j - (s + \delta \cdot 2^n) \in \delta \cdot 2^n = 2\delta \cdot 2^{n-1}$。随后，算法计算 $(i_2', j') \triangleq g(i_2, j - (s + \delta \cdot 2^n)) \in v_2(s_0 + s_1)$，并输出 $h(i_1, i_2, j) \triangleq (i_1, i_2', j')$。

可以验证该函数确实是满射，因此根据定义，$s_0 + s_1 \lesssim_{2\delta} s$。类似地，我们可以证明 $s \lesssim_{2\delta} s_0 + s_1$。于是有

$$s \lesssim_0 s \lesssim_{2\delta} s_0 + s_1 \quad \text{and} \quad s_0 + s_1 \lesssim_0 s_0 + s_1 \lesssim_{2\delta} s,$$

根据引理 5.19 (2)，我们有 $s \in (s_0 + s_1) \pm (2\delta + \beta) \cdot 2^n$。这立即推出方程 (5.10)，因为 $\mathsf{NW}(C,\Delta) \triangleq \mathsf{Size}(C, 1^{|\Delta|})/2^n$。

- (Precision Consistency Axiom)。设 $C\colon \{0,1\}^n \to \{0,1\}$ 是一个电路，Δ_1，Δ_2，B 是字符串，且 $\delta_1 \triangleq 1/|\Delta_1|$，$\delta_2 \triangleq 1/|\Delta_2|$，$\beta \triangleq 1/|B|$。我们需要证明

$$|\mathsf{NW}(C,\Delta_1) - \mathsf{NW}(C,\Delta_2)| \le \delta_1 + \delta_2 + \beta. \tag{5.11}$$

设 $X \subseteq \{0,1\}^n$ 为由 C定义的有界集合，并设 $s_i \triangleq \mathsf{Size}(C, 1^{|\Delta_i|})$，$i \in \{1,2\}$。根据引理 5.20的第二条，

$$X \approx_{\delta_1} s_1, \quad X \approx_{\delta_2} s_2.$$

因此，我们有 $s_1 \lesssim_{\delta_1} X \lesssim_{\delta_2} s_2$，根据引理 5.19 (2)，$s_1 \le s_2 + (\delta_1 + \delta_2 + \beta) \cdot 2^n$。类似地，我们可以证明 $s_2 \le s_1 + (\delta_1 + \delta_2 + \beta) \cdot 2^n$。由于 $\mathsf{NW}(C,\Delta) \triangleq \mathsf{Size}(C, 1^{|\Delta|})/2^n$，这立即推出方程（5.10）。

证明至此完成。 □

5.6 APX的KPT见证定理$_1$：定理5.1的证明 2

回顾带电路的KPT见证性质的定义：

定义5.11 （带电路的KPT见证）。 设 $\mathcal{T}$ 是PV_1的一个扩展。若 $\mathcal{T}$ 满足以下条件，我们就称其具有带电路的*KPT*见证性质。设 $\varphi(\vec{x}, y, z)$是PV_1 语言中的任意无量词公式，且 $\mathcal{T} \vdash \forall \vec{x}\ \exists y\ \forall z\ \varphi(\vec{x}, y, z)$。那么存在一个常元 $k \in \mathbb{N}$和函数$f_1, f_2, \ldots, f_k$ （在标准模型中），使得以下条件成立。

对于每个字符串向量 $\vec{x}$ 以及每个 $z_1, z_2, \ldots, z_k \in \{0,1\}^*$，以下命题在标准模型中成立：

- 或者 $\varphi(\vec{x}, f_1(\vec{x})\ z_1)$为真；
- 或 $\varphi(\vec{x},\ f_2(\vec{x},\ z_1)\ z_2)$为真；
- 或 $\varphi(\vec{x},\ f_3(\vec{x},\ z_1,\ z_2)\ z_3)$为真；
- $\cdots$；
- 或 $\varphi(\vec{x},\ f_k(\vec{x},\ z_1,\ \ldots,\ z_{k-1})\ z_k)$为真。

此外，对于 $\vec{x}$，$f_1, \ldots, f_k$的任意固定输入长度，它们都可由多项式规模确定性电路计算。

定理 5.12 (KPT 见证性质适用于 APX_1)。 APX_1 具有带电路的*KPT*见证性质。

为证明定理 5.12，我们需要全称一阶理论的标准 KPT见证定理 [KPT91]；感兴趣的读者可参阅 [Oli25，定理 3。2] 以了解详细讨论。

定理 5.21 (KPT见证定理)。 设 $\mathcal{T}$是一个全称理论。设 $\varphi(\vec{x}, y, z)$ 是 $\mathcal{T}$语言中的一个无量词公式，满足 $\mathcal{T} \vdash \forall \vec{x}\ \exists y\ \forall z\ \varphi(\vec{x}, y, z)$。那么存在一个常元 $k \in \mathbb{N}$ 以及项$t_1, t_2, \ldots, t_k$ （在 $\mathcal{T}$的语言中），使得以下陈述可在 $\mathcal{T}$中证明：

对于每个 $\vec{x}$ 以及每个 $z_1, z_2, \ldots, z_k$，以下条件之一成立： $\varphi(\vec{x}, t_1(\vec{x})\ z_1)$，或 $\varphi(\vec{x}, t_2(\vec{x}, z_1)\ z_2)$，或 $\varphi(\vec{x}, t_3(\vec{x}, z_1, z_2)\ z_3)$，……，或 $\varphi(\vec{x}, t_k(\vec{x}, z_1, \ldots, z_{k-1})\ z_k)$。

证明定理 *5.12*。 回顾，APX_1 允许全称公理化（见命题2.8）。由定理5.21 连同 $\mathcal{T} \triangleq APX_1$，，若 $APX_1 \vdash \forall \vec{x}\ \exists y\ \forall z\ \varphi$（$\vec{x}$，$y$，$z$），则存在常元 $k \in \mathbb{N}$及项 t_1，……，t_k，使得 APX_1 证明如下语句：

(Φ)：对每一个 $\vec{x}$与 z_1，z_2，……，z_k，或者 $\varphi(\vec{x}, t_1(\vec{x})\ z_1)$，或者 $\varphi(\vec{x}, t_2(\vec{x}, z_1)\ z_2)$，或者 $\varphi(\vec{x}, t_3(\vec{x}, z_1, z_2)\ z_3)$，……，或者 $\varphi(\vec{x}, t_k(\vec{x}, z_1,\ \ldots,\ z_{k-1})\ z_k)$。

注意，$t_1, \ldots, t_k$是 PV(P)项，可解释为多项式时间 P-预言机算法。

类似于定理 1.9的证明，我们可以将全称句（Φ）改写为 e_Φ 中的一个方程APX，使其可在 APX中证明。因此，根据APX 的可靠性（见命题 2.7），可知 e_Φ 在任意标准模型 $\mathbb{M}$（P）中都为真。

令 CAPP 为如下搜索问题：给定任意电路 C 和一个字符串 Δ，输出一个数值 $p \in \Pr[C(x)] \pm 1/|\Delta|$。众所周知，该问题属于 prBPP（例如参见 [Gol11]），因此可由一族确定性多项式规模电路计算。固定任意一族求解 CAPP 的电路 $F(C, \Delta)$。根据定义， $\mathbb{M}(F)$ 是 APX 的标准模型。随后， e_Φ 在模型 $\mathbb{M}(F)$ 中为真。

该定理只需将 f_1、f_2、……、f_k 设为 $t_1^{\mathbb{M}(F)}$、$t_2^{\mathbb{M}(F)}$、……、$t_k^{\mathbb{M}(F)}$ 即可。由于对于每个固定的输入长度，在计算 t_1 时，对 $F(C$、$\Delta)$ 的预言机调用中， C的规模以及 Δ的长度都存在多项式上界，……， t_k，因此我们可以为 f_1、……f_k 固定一族多项式规模电路。

□

6 随机与平均情况下界的反向数学

多项式时间函数的收缩弱鸽巢原理是已知可在 APC_1, 中证明、但尚不知能否在 APX_1中证明的最重要组合原理之一。在本

节中，我们探讨收缩鸽巢原理的计数变体，并刻画它们的等价类（就能否在 APX_1中证明而言）。我们证明，该等价类涵盖了某些平均情况下的随机化通信复杂度下界，从而确立这些结果都等价于收缩鸽巢原理的相应变体。

6.1 收缩鸽巢原理的变体

我们从收缩弱鸽巢原理 rWPHP(PV) 的定义开始。为简便起见，我们引入以下记号。我们用 $m : \mathrm{Log} \to \mathrm{Log}$ 表示一个 PV 函数符号 $m(n)$，其输入和输出均以一进制编码。我们用 $\varepsilon : \mathrm{Log} \to \mathrm{Log}^{-1}$ 表示一个 PV 函数符号 $e(n)$，其输入和输出均以一进制编码，而 $\varepsilon(n)$ 是有理数 $1/e(n)$ 的简写。

定义 6.1（收缩弱鸽巢原理）。设 $m: \mathrm{Log} \to \mathrm{Log}$。伸展为 m 的收缩弱鸽巢原理 rWPHP$[m]$(PV) 表示 APX_1 语言中的以下陈述：

对于每个 $n \in \mathrm{Log}$ 和电路 $C\colon \{0,1\}^n \to \{0,1\}^{m(n)}$, $D\colon \{0,1\}^{m(n)} \to \{0,1\}^n$，若 $m(n) < n$，则存在一个字符串 $x \in \{0,1\}^n$，使得 $D(C(x)) \neq x$。

我们将定义 rWPHP(PV) 的两个变体：近似计数版本 #rWPHP(PV)，以及随机化压缩版本 rrWPHP(PV)。

定义 6.2（近似计数 rWPHP）。设 $m : \mathrm{Log} \to \mathrm{Log}$ $\varepsilon : \mathrm{Log} \to \mathrm{Log}^{-1}$。伸展为 m 、错误为 ε 的近似计数收缩弱鸽巢原理 #rWPHP$[m, \varepsilon]$(PV)，表示 APX_1 语言中的以下陈述：

对于每个 $n \in \mathrm{Log}$ 和电路 $C\colon \{0,1\}^n \to \{0,1\}^{m(n)}$, $D\colon \{0,1\}^{m(n)} \to \{0,1\}^n$，令 T 为满足以下条件的电路：若 $D(C(x)) \neq x$，则 $T(x) = 1$。那么，若 $m(n) < n$ 且 $\varepsilon(n) < 1 - 2^{n-m(n)}$，则存在 $\delta^{-1}, \beta^{-1} \in \mathrm{Log}$，使得 $\mathrm{P}_\delta(T) > \varepsilon(n) + \delta + \beta$。

定义 6.3（随机化压缩 rWPHP）。设 $m : \mathrm{Log} \to \mathrm{Log}$， $\varepsilon : \mathrm{Log} \times \mathrm{Log} \to \mathrm{Log}^{-1}$。伸展为 m 、错误为 ε 的随机化压缩收缩弱鸽巢原理 rrWPHP$[m, \varepsilon]$(PV) 表示 APX_1 语言中的以下陈述：

对于每个 n， $r \in \mathrm{Log}$ 和电路 $C\colon \{0,1\}^n \times \{0,1\}^r \to \{0,1\}^{m(n)}$, $D\colon \{0,1\}^{m(n)} \to \{0,1\}^n$，若 $m(n) < n$ 且 $\varepsilon(n + r) < 1 - 2^{n-m(n)}$，则存在一个 $x \in \{0,1\}^n$ 和 δ^{-1}， $\beta^{-1} \in \mathrm{Log}$，使得以下条件成立：设 $T_x\colon \{0,1\}^r \to \{0,1\}$ 为满足以下条件的电路：当且仅当 $D(C(x, \mathrm{sd})) \neq x$ 时， $T_x(\mathrm{sd}) = 1$。则 $\mathrm{P}_\delta(T_x) > \varepsilon(n, r) + \delta + \beta$。

根据定义可以立即得出，rWPHP 的两种变体在任何 APX 的标准模型中都是真命题$_1$, ，证明留作练习。

命题 6.4。对于每个 m： $\mathrm{Log} \to \mathrm{Log}$， ε： $\mathrm{Log} \to \mathrm{Log}^{-1}$， #收缩弱鸽巢原理$[m, \varepsilon]$(PV) 和 rrWPHP $[m, \varepsilon]$(PV)ˆ在任何 *APX* 的标准模型$_1$中都是正确命题 $\mathbb{M}(\mathrm{P})$ 。

这些原理可以看作是关于压缩-解压缩算法的最坏情况和（弱）平均情况困难性。具体而言：

- 收缩弱鸽巢原理$[m]$(PV) 表示，对于任意确定性压缩-解压缩对 (C, D)，若其压缩率为 m，则存在一个不可压缩串；
- #rWPHP$[m, \varepsilon]$(PV) 表示，对于任意确定性压缩-解压缩对 (C, D)，若其压缩率为 m，则存在占比为 ε 的不可压缩字符串；
- rrWPHP$_m$(PV) 表示，对于任意 (C, D)，其中 C 是随机化的 压缩算法，而 D 是确定性的 解压缩算法，则必定存在一个输入字符串，使该压缩-解压缩对的错误概率 为 ε。

有界算术中的一个经典结果是，收缩弱鸽巢原理在 PV 中允许伸展归约。具体而言：

定理 6.5 ([Tha02, Je˘r05])。对于任意常元 $\varepsilon \in (0, 1)$， PV $+$ 收缩弱鸽巢原理$[n^\varepsilon]$(PV) $\vdash$ 收缩弱鸽巢原理$[n-1]$(PV)。

6.2 单向通信下界

我们证明了一个等价性结果，涉及 #rWPHP(PV) 与针对集合不相交问题 的单向协议 的通信复杂度下界，其中协议采用公共随机性 或私有随机性。

单向通信协议的形式化。 我们首先对通信协议进行形式化。令 n，m，$r \in \mathsf{Log}$。一对电路 g_{A}：$\{0,1\}^n \times \{0,1\}^r \to \{0,1\}^m$ 和 d_{B}：$\{0,1\}^n \times \{0,1\}^m \times \{0,1\}^r \to \{0,1\}$ 定义如下的单向随机通信协议：

- （公开随机币模型）。对于任意一对输入 $(x, y) \in \{0,1\}^n \times \{0,1\}^n$ 以及均匀生成的公开随机种子 $\mathsf{sd} \in \{0,1\}^r$，Alice 向 Bob 发送消息 $\mathsf{msg} \triangleq g_{\mathsf{A}}(x, \mathsf{sd})$，当且仅当 $d_{\mathsf{B}}(y, \mathsf{msg}, \mathsf{sd}) = 1$ 时，Bob 才接受。

- （私有随机币模型）。对于任意一对输入（x，y）$\in \{0,1\}^n \times \{0,1\}^n$ 以及一致生成的私有随机种子 $\mathsf{sd} \in \{0,1\}^r$，Alice 向 Bob 发送消息 $\mathsf{msg} \triangleq g_{\mathsf{A}}(x, \mathsf{sd})$，当且仅当 $d_{\mathsf{B}}(y, \mathsf{msg}\ 0^r) = 1$时，Bob 才决定接受。

设 f：$\{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ 是由一个电路指定的函数。对于每个 x，$y \in \{0,1\}^n$，令$T^{\text{公开}}_{f,\,x,\,y}$：$\{0,1\}^r \to \{0,1\}$ 为满足下述条件的电路：$T^{\text{公开}}_{f,\,x,\,y}(\mathsf{sd}) = 1$ 当且仅当公开随机币协议在输入（x，y）和种子 sd 下输出 $1 - f(x, y)$，即

$$T^{\mathsf{pub}}_{f,x,y}(\mathsf{sd}) \triangleq \mathbb{I}[d_{\mathsf{B}}(y, g_{\mathsf{A}}(x, \mathsf{sd}), \mathsf{sd}) \neq f(x, y)] \in \{0,1\}. \tag{6.1}$$

设 $\varepsilon \in \mathbb{Q}$。我们称公开随机币协议 $(g_{\mathsf{A}}, d_{\mathsf{B}})$ 以错误率 ε 计算函数 f，如果对于 $x, y \in \{0,1\}^n$, $\delta^{-1}, \beta^{-1} \in \mathsf{Log}$,

$$\mathsf{P}_\delta(T^{\mathsf{pub}}_{f,x,y}) \leq \varepsilon + \delta + \beta. \tag{6.2}$$

注意，此处我们考虑双边错误设定；当然，也可以自然地用单边错误来定义正确性。

相应地，可以将 $T^{\text{私有}}_{f,x,y}$ 定义为满足以下条件的电路：当且仅当私有随机协议在输入 (x, y) 和种子 sd 下输出 $1 - f(x, y)$ 时，$T^{\text{公开}}_{f,x,y}(\mathsf{sd}) = 1$，即

$$T^{\mathsf{priv}}_{f,x,y}(\mathsf{sd}) \triangleq \mathbb{I}[d_{\mathsf{B}}(y, g_{\mathsf{A}}(x, \mathsf{sd}), 0^r) \neq f(x, y)] \in \{0,1\}. \tag{6.3}$$

我们称私有随机协议 $(g_{\mathsf{A}}, d_{\mathsf{B}})$ 以错误率 ε 计算函数 f，如果对于每个 $x, y \in \{0,1\}^n$,$\delta^{-1}, \beta^{-1} \in \mathsf{Log}$,

$$\mathsf{P}_\delta(T^{\mathsf{priv}}_{f,x,y}) \leq \varepsilon + \delta + \beta. \tag{6.4}$$

通信复杂度下界。 固定任意函数 f：$\{0,1\}^n \times \{0,1\}^n \to \{0,1\}$, n，m，$r \in \mathsf{Log}$，以及 $\varepsilon \in \mathbb{Q}$。我们将句子 $\text{pub-rLB}\longrightarrow^{f}[n, m, r, \varepsilon]$ 定义如下：对于每个如上所定义的公共随机协议 $(g_{\mathsf{A}}, d_{\mathsf{B}})$，$(g_{\mathsf{A}}, d_{\mathsf{B}})$ 都无法以错误率 ε 计算 f。换言之，存在 x，$y \in \{0,1\}^n$ 和 δ^{-1}，$\beta^{-1} \in \mathsf{Log}$，使得 $\mathsf{P}_\delta(T^{\mathsf{pub}}_{f\,x\,,\,,\,y}) > \varepsilon + \delta + \beta$。

相应地，我们将句子 $\text{priv-rLB}\longrightarrow^{f}[n, m, r, \varepsilon]$ 定义如下：对于每个如上所定义的私有随机协议 $(g_{\mathsf{A}}, d_{\mathsf{B}})$，$(g_{\mathsf{A}}, d_{\mathsf{B}})$ 都无法以错误率 ε 计算 f。

回忆一下，集合不相交函数 $\mathsf{SetDisj}(x, y)$ 的输出为 1，当且仅当对于每个索引 $i \in [n]$，要么 $x_i = 0$ 或 $y_i = 0$，也就是说，x 和 y 没有共同的 1 索引。令 $m : \mathsf{Log} \to \mathsf{Log}$，$\varepsilon : \mathsf{Log} \times \mathsf{Log} \to \mathsf{Log}^{-1}$为函数。我们将 $\text{pub-rLB}\longrightarrow^{\mathsf{SetDisj}}[m, \varepsilon]$ 定义为以下语句：

$$\text{For } n, r \in \mathsf{Log},\ \text{pub-rLB}\longrightarrow^{\mathsf{SetDisj}}[n, m(n), r, \varepsilon(n, r)].$$

换句话说，任何计算 SetDisj 且通信复杂度为 $m(n)$ 的公共随机单向协议，其错误概率至少为 $\varepsilon(n)$。正如我们将在第 6.3 节证明的那样，即使对于 $m(n) = n - n^{\Omega(1)}$，这个下界依然成立。因此，我们将 私有随机-下界 $\longrightarrow^{\mathsf{SetDisj}}[m, \varepsilon]$ 定义为以下命题：

对于 $n,\ r \in \mathsf{Log}$、私有随机下界$\underrightarrow{\ }^{\mathsf{SetDisj}}[n, m(n)\ r,\ \varepsilon(n,\ r)]$。

我们还考虑一种较弱的表述：它不针对某个特定函数形式化下界，而是形式化存在一个下界对其成立的函数。令 $m : \mathsf{Log} \to \mathsf{Log}$ $\varepsilon : \mathsf{Log} \times \mathsf{Log} \to \mathsf{Log}^{-1}$。我们将 pub-rLB$^{\mathsf{some}}[m, \varepsilon]$ 定义为以下命题：

对于 $n, r \in \mathsf{Log}$，存在一个电路 f：$\{0,1\}^n \times \{0,1\}^n \to \{0,1\}$，使得 pub-rLB$\underrightarrow{\ }^{f}[n, m(n)\ r, \varepsilon(n, r)]$ 成立。

换句话说，存在一个函数 f，使得任何计算 f 且通信复杂性为 $m(n)$ 的公共随机单向协议，都必须具有非忽略的错误概率。将 f 固定为 SetDisj，即可由 pub-rLB$\underrightarrow{\ }^{\mathsf{SetDisj}}[m, \varepsilon]$推出这一结论。因此，我们可以将 priv-rLB$\underrightarrow{\ }^{\mathsf{some}}[m, \varepsilon]$ 定义为以下命题：

对于 $n,\ r \in \mathsf{Log}$，存在一个电路 f：$\{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ 使得 priv-rLB$\underrightarrow{\ }^{f}[n, m(n)\ r,\ \varepsilon(n,\ r)]$ 成立。

相等性的上界。 作为合理性检查，我们注意到，由于存在一个使用线性哈希的通信复杂度上界 用于相等性检验，（见定理4.5），对应的下界在APX_1中不可证明。

定理 6.6（相等性检验的上界）。 存在 PV 函数 $m : \mathsf{Log} \to \mathsf{Log}$、 $\varepsilon : \mathsf{Log} \to \mathsf{Log}^{-1}$，满足 $m(n) = \Theta(\log n)$、$\varepsilon(n) = 1 - 1/n^{\Theta(1)}$，使得

$$\mathsf{APX}_1 \vdash \forall n\ \neg\text{pub-}\underrightarrow{\mathsf{rLB}}^{\mathsf{EQ}}[n, m(n), n \cdot m(n), \varepsilon(n)]. \tag{6.5}$$

特别地，$\mathsf{APX}_1 \vdash \neg$公共-随机下界$[m, \varepsilon]$。

证明概要。 我们在 APX_1 中证明方程（6.5）成立，其中 m、r、ε 将在后文确定。由于当 n 较小时的情形可以通过穷举法证明，因此只需考虑 $n > n_0$，其中 $n_0 \in \mathbb{N}$ 是一个将在后文确定的常元。

任取 $n > n_0$。单向通信协议如下。设 $x \in \{0,1\}^n$ 是 Alice 的输入， $y \in \{0,1\}^n$ 是 Bob 的输入。他们将公共随机性解析为矩阵 $A \in \{0,1\}^{m(n) \times n}$。Alice 将 $Ax \in \{0,1\}^{m(n)}$ 作为消息发送，Bob 当且仅当 $Ax = Ay$时接受。接下来只需证明该协议的错误至多为 $\varepsilon(n)$。

任取输入 $x, y \in \{0,1\}^n$。如果 $x = y$，该协议总是接受。换言之，公式（6.1）中的电路 T^{pub} 等值检验 x,y 是一个总是拒绝的常值电路。正确性，即公式（6.2），可由 Boundary Axiom立即得出。对于 $x \neq y$的情况，电路 T^{pub} 等值检验 x,y 与定理 4.5 中电路 $T_{x,y}$ 的否定函数等价。因此，根据互补计数，只要设置 $m(n) = n^{O(1)}$, $\varepsilon(n) > 1 - 0.51^{m(n)}$，并使 $n_0 \in \mathbb{N}$ 足够大，定理就成立。证明完毕。

□

6.3 通信复杂度的主要等价性结果

我们确立 了关于它们在 APX_1 中可证明性的若干陈述之间的等价关系 .

定理 6.7。 以下陈述在 APX_1 中等价：

(1) #收缩弱鸽巢原理$[n-1, n^{-k}]$*(PV)*，其中 $k \in \mathbb{N}$ 是某个常元；*(2)* #收缩弱鸽巢原理$[n^{\varepsilon}, n^{-k}]$*(PV)*，其中 $\varepsilon \in$ *(0, 1)*且 $k \in \mathbb{N}$ 是某些常元；*(3) rrWPHP*$[n-1,(n+r)^{-k}]$*(PV)*，其中 $k \in \mathbb{N}$ 是某个常元；*(4) rrWPHP*$[n^{\varepsilon},(n+r)^{-k}]$*(PV)*，其中 $\varepsilon \in$ *(0, 1)*且 $k \in \mathbb{N}$ 是某些常元；*(5)* 公共随机下界$\underrightarrow{\ }^{\mathsf{SetDisj}}[n-1,(n+r)^{-k}]$，其中 $k \in \mathbb{N}$ 是某个常元；*(6)* 公共随机下界$\underrightarrow{\ }^{\mathsf{SetDisj}}[n^{\varepsilon},(n+r)^{-k}]$，其中 $\varepsilon \in$ *(0, 1)*且 $k \in \mathbb{N}$ 是某些常元；

(7) 私有随机下界$\xrightarrow{}^{\mathsf{SetDisj}}[n-1,(n+r)^{-k}]$，其中 $k\in\mathbb{N}$ 是某个常元；*(8)* 私有随机下界$\xrightarrow{}^{\mathsf{SetDisj}}[n^{\varepsilon},(n+r)^{-k}]$，其中 $\varepsilon\in(0,1)$且 $k\in\mathbb{N}$ 是某些常元；*(9)* 公共随机下界$\xrightarrow{}^{\mathsf{some}}[n-1,(n+r)^{-k}]$，其中 $k\in\mathbb{N}$ 是某个常元；*(10)* 公共随机下界$\xrightarrow{}^{\mathsf{some}}[n^{\varepsilon},(n+r)^{-k}]$，其中 $\varepsilon\in(0,1)$且 $k\in\mathbb{N}$ 是某些常元；*(11)* 私有随机下界$\xrightarrow{}^{\mathsf{some}}[n-1,(n+r)^{-k}]$，其中 $k\in\mathbb{N}$ 是某个常元；*(12)* 私有随机下界$\xrightarrow{}^{\mathsf{some}}[n^{\varepsilon},(n+r)^{-k}]$，其中 $\varepsilon\in(0,1)$且 $k\in\mathbb{N}$ 是某些常元。

Remark 6.8. 上述陈述中，对 $k\in\mathbb{N}$ 和 $\varepsilon\in(0,1)$ 的量化是在理论之外进行的。例如，(1) $\Rightarrow$ (2) 表示对每个 $k_1\in\mathbb{N}$，都存在一个 $k_2\in\mathbb{N}$ 和 $\varepsilon_2\in(0,1)$，使得句子

$$\#\mathsf{rWPHP}[n-1,n^{-k_1}](\mathsf{PV})\to\#\mathsf{rWPHP}[n^{\varepsilon_2},n^{-k_2}](\mathsf{PV}).$$

可在 APX_1 中证明。

显然的方向。(1) $\Rightarrow$ (2) 和 (3) $\Rightarrow$ (4) 都是显然的。事实上，通过填充虚拟比特，可以将伸展较小的压缩-解压缩对转换为伸展较大的压缩-解压缩对。还容易看出，陈述 (5) 至 (12) 在关于APX_1, 的蕴含关系下构成一个与三维布尔立方体同构的格，其中 (5) 是最大元（即最强的下界），而 (12) 是最小元（即最弱的下界）。这是因为，针对公开随机币协议的下界蕴含针对私有随机协议的下界；$n-1$ 通信下界蕴含 $n^{\Omega(1)}$通信下界；针对 SetDisj 的下界蕴含针对某个函数 f 的下界（令 f 为SetDisj即可）。

非平凡方向。 注意，为了完成定理 6.7的证明，只需证明以下蕴含关系：(12) $\Rightarrow$(4), (1) $\Rightarrow$(5), (2) $\Rightarrow$ (3), 以及 (4) $\Rightarrow$(1)。这些蕴含关系的证明将在后续各节给出。

6.3.1 压缩蕴含通信上界：(12) $\Rightarrow$ (4)

Lemma 6.9. 对于任意 $\varepsilon_{12}\in(0,1)$ 和 $k_{12}\in\mathbb{N}$，存在 $\varepsilon_4\in(0,1)$ 和 $k_4\in\mathbb{N}$，使得

$$\mathsf{APX}_1+\mathsf{priv}\text{-}\mathsf{rLB}\xrightarrow{}^{\mathsf{some}}[n^{\varepsilon_{12}},(n+r)^{-k_{12}}]\vdash\mathsf{rrWPHP}[n^{\varepsilon_4},(n+r)^{-k_4}](\mathsf{PV}).$$

证明。任取常元 $\varepsilon_6\in(0,1)$、$k_{12}\in\mathbb{N}$，令 $\varepsilon_2\triangleq\varepsilon_6$ 和 $k_4\triangleq k_{12}$。令 $m_4(n)\triangleq n^{\varepsilon_4}$ 和 $m_{12}(n)\triangleq n^{\varepsilon_{12}}$。我们将在 APX_1 中证明，$\neg\mathsf{rrWPHP}[n^{\varepsilon_4},n^{-k_4}](\mathsf{PV})$ 蕴含 $\neg\mathsf{priv}\text{-}\mathsf{rLB}\xrightarrow{}^{\mathsf{some}}[n^{\varepsilon_{12}},n^{-k_{12}}]$。

假设 $\mathsf{rrWPHP}[m_4,n^{-k_4}](\mathsf{PV})$ 不成立。那么存在 $n,r\in\mathsf{Log}$ 和电路 $C\colon\{0,1\}^n\times\{0,1\}^r\to\{0,1\}^{m_2(n)}$ $D\colon\{0,1\}^{m_2(n)}\to\{0,1\}^n$，使得以下结论成立。令 T_x 为满足以下条件的电路：$T_x(\mathsf{sd})=1$ 当且仅当 $D(C(x,\mathsf{sd}))\neq x$。那么对于每个 $\delta^{-1},\beta^{-1}\in\mathsf{Log}$ 和 $x\in\{0,1\}^n$,

$$\mathsf{P}_\delta(T_x)\le(n+r)^{-k_4}+\delta+\beta. \tag{6.6}$$

按上述说明，固定 n,r,C,D。

现在我们将证明 $\neg$私有随机下界$\xrightarrow{}^{\mathsf{some}}[n^{\varepsilon_{12}},n^{-k_{12}}]$。具体而言，我们将证明，对于每个 $f\colon\{0,1\}^n\times\{0,1\}^n\to\{0,1\}$，私有随机下界$\xrightarrow{}^{f}[n^{\varepsilon_{12}},n^{-k_{12}}]$ 不成立。任取电路 $f\colon\{0,1\}^n\times\{0,1\}^n\to\{0,1\}$。我们的目标是构造一个私有随机币通信协议，其通信复杂度为 $n^{\varepsilon_{12}}$，并以错误率 $n^{-k_{12}}$计算f。协议如下：

- 给定 $x\in\{0,1\}^n$和一致随机种子 sd，Alice 发送消息 $g_A(x,\mathsf{sd})\triangleq C(x,\mathsf{sd})$。
- 给定 $y\in\{0,1\}^n$和消息 msg，当且仅当 $d_B(y,\mathsf{msg},\mathsf{sd})\triangleq f(D(\mathsf{msg}),y)=1$时，Bob 接受。

为了证明该协议以错误率 $n^{-k_{12}}$计算 f，任取 $\delta^{-1},\beta^{-1}\in\mathsf{Log}$。令 $\eta^{-1}\in\mathsf{Log}$ 为稍后确定的参数，并令 $T^{\mathsf{priv}}_{f\,x}$, ,$_y$(sd) 为方程 (6.3) 中定义的电路。可以验证，对于每个 $x,y\in\{0,1\}^n$ 和 $\mathsf{sd}\in\{0,1\}^r$，如果 $T^{\mathsf{priv}}_{f\,x}$, ,$_y$(sd) $=1$，那么 T_x(sd) $=1$。根据近似计数的单调性，

$$\mathsf{P}_\eta(T^{\mathsf{priv}}_{f,x,y})\le\mathsf{P}_\eta(T_x)+3\eta\le(n+r)^{-k_4}+5\eta,$$

其中，最后一个不等式由方程（6.6）得出。进而可由 Precision ConsistencyAxiom 得出

$$\mathsf{P}_\delta(T^{\mathsf{priv}}_{f,x,y})\le\delta+\mathsf{P}_\eta(T^{\mathsf{priv}}_{f,x,y})\le(n+r)^{-k_4}+\delta+5\eta\le(n+r)^{-k_4}+\delta+\beta$$

通过设定 $\eta\triangleq\beta/5$。证明至此完成。 □

6.3.2 从通信上界得到压缩：(1) ⇒ (5)

引理 6.10。对于每个常元 $k_1\in\mathbb{N}$，存在一个 $k_5\in\mathbb{N}$，使得 APX_1+#收缩弱鸽巢原理$[n-1,n^{-k_1}](\mathsf{PV})\vdash$公共-公共随机下界$\longrightarrow^{\mathsf{SetDisj}}[n-1,(n+r)^{-k_5}]$。

证明。任取 $k_1\in\mathbb{N}$，并令 $k_5\in\mathbb{N}$ 稍后确定。我们将在 APX_1 中证明，¬公共随机下界$\longrightarrow^{\mathsf{SetDisj}}[n-1,n^{-k_5}]$蕴含 ¬#rWPHP$[n-1,n^{-k_1}](\mathsf{PV})$。

假设 公共-公共随机下界$\longrightarrow^{\mathsf{SetDisj}}[n-1,n^{-k_5}]$ 不成立。那么存在 n、$r\in\mathsf{Log}$ 和一个单向公共随机协议 g_{A}：$\{0,1\}^n\times\{0,1\}^r\to\{0,1\}^{n-1}$、$d_{\mathsf{B}}$：$\{0,1\}^n\times\{0,1\}^{n-1}\times\{0,1\}^r\to\{0,1\}$ 满足以下条件：对于每个 x、$y\in\{0,1\}^n$ 和 δ^{-1}，$\beta^{-1}\in\mathsf{Log}$，令 $T^{\mathsf{pub}}\,_{\mathsf{SetDisj}\,x,\,y}(\mathsf{sd})$ 为方程（6.1）所定义的电路，则

$$\mathsf{P}_\delta(T^{\mathsf{pub}}_{\mathsf{SetDisj},x,y})\le(n+r)^{-k_5}+\delta+\beta.\tag{6.7}$$

我们的目标是 构造一个违反收缩弱鸽巢原理$[n-1,n^{-k_1}](\mathsf{PV}$ 的压缩-解压方案).

压缩方案的构造。我们构造一对电路 C：$\{0,1\}^{n+r}\to\{0,1\}^{n+r-1}$，$D$:$\{0,1\}^{n+r-1}\to\{0,1\}^{n+r}$ 如下。

- （压缩）：电路 C 将输入解析为 $(x,\ \mathsf{sd})\in\{0,1\}^n\times\{0,1\}^r$，并计算定义为 $\sigma\in\{0,1\}^n$

$$\sigma_i\triangleq d_{\mathsf{B}}(e_i,g_{\mathsf{A}}(x,\mathsf{sd}),\mathsf{sd})\oplus x_i\oplus1,\tag{6.8}$$

  其中 e_i 表示仅第 i 位为 1 的字符串。如果 $e\neq0^n$，压缩失败，并输出 0^n。否则，输出消息 $\triangleq g_{\mathsf{A}}(x,$ sd) 与 sd 的拼接。
- （解压缩）：电路 D 将输入解析为上述消息与 sd 的拼接，并计算 $y\in\{0,1\}^n$，其定义为

$$y_i\triangleq d_{\mathsf{B}}(e_i,\mathsf{msg},\mathsf{sd})\oplus1,$$

  并输出 y 与 sd 的拼接。

显然，当 $\sigma=0^n$ 时，该压缩-解压方案是正确的。

错误概率分析。我们将证明，$(C,\ D)$ 是一个违反 #rWPHP$[n-1,n^{-k_1}](\mathsf{PV})$ 的压缩-解压方案。任取 $\delta^{-1},\ \beta^{-1}\in\mathsf{Log}$，并令 T: $\{0,1\}^{n+r}\to\{0,1\}$ 为电路；当 $D(C(z))\neq z$ 时，该电路 $T(z)$ 输出 1。我们的目标是证明 $\mathsf{P}_\delta(T)\le n^{-k_1}+\delta+\beta$。

令 $\eta^{-1}\in\mathsf{Log}$ 为稍后确定的参数，且 T'：$\{0,1\}^{n+r}\to\{0,1\}$ 为如下电路：给定 $(x,$sd$)\in\{0,1\}^n\times\{0,1\}^r$，它通过方程 (6.8) 计算 σ，并且当且仅当$\sigma\neq0^n$时输出 1。如上所述，对于每个 x 和 sd，$T(x\circ\mathsf{sd})=1$ 意味着 $T'(x\circ\mathsf{sd})=1$。因此，根据近似计数的单调性，我们有

$$\mathsf{P}_\eta(T)\le\mathsf{P}_\eta(T')+3\eta.\tag{6.9}$$

令 $V \triangleq \{0,1\}$ 和 X_1、X_2、……、X_n 为支撑集在 $\{0,1\}^{n+r}$ 上的随机变量，使得当且仅当 $e_i \neq 0$时，$X_i = 1$。令 $F_i(x, \mathsf{sd})$ 为电路，它为每个 $i \in [n]$定义 X_i。显然， $T'(x, \mathsf{sd})$ 是当且仅当对某个 $i \in [n]$有 $X_i = 1$ 时输出 1 的电路。令 Y 为由 $(V, n+r, T')$ 定义的随机变量。根据并集界，我们有

$$\mathsf{P}_\eta(T') \leq \mathbb{E}_\eta[Y] + 3\eta \leq \mathbb{E}_\eta[X_1] + \cdots + \mathbb{E}_\eta[X_n] + 3\eta \cdot (n+1), \tag{6.10}$$

其中，第一个不等式由命题 3.12得出。

此外，对于每个 $i \in [n]$ 和每个 $x \in \{0,1\}^n$，我们可以看到， $F_i(x, \cdot)$ 与 $T^{\mathsf{pub}}_{\mathsf{SetDisj}\ x,\ e_i}(\cdot)$ 函数等价。令 $X_i|_x$ 为将种子的第一部分固定为 x 后得到的随机变量。那么对于 $x \in \{0,1\}^n$，

$$\mathbb{E}_\eta[X_i|_x] \leq \mathsf{P}_\eta(F_i(x,\cdot)) + 3\eta \leq \mathsf{P}_\eta(T^{\mathsf{pub}}_{\mathsf{SetDisj},x,e_i}) + 6\eta \leq (n+r)^{-k_5} + 8\eta,$$

其中，最后一个不等式由方程（6.7）得出。根据 期望的平均论证，我们有

$$\mathbb{E}_\eta[X_i] \leq (n+r)^{-k_5} + 8\eta + 3\eta \leq n^{-k_5} + 11\eta. \tag{6.11}$$

结合上述结果，我们得到：

$$\begin{aligned}
\mathsf{P}_\delta(T) &\leq \mathsf{P}_\eta(T) + \delta + 2\eta && \text{(Precision Consistency Axiom)}\\
&\leq \mathsf{P}_\eta(T') + \delta + 5\eta && \text{(Equation (6.9))}\\
&\leq \mathbb{E}_\eta[X_1] + \cdots + \mathbb{E}_\eta[X_n] + \delta + 3\eta \cdot (n+1) + 5\eta && \text{(Equation (6.10))}\\
&\leq \delta + ((n+r)^{-k_5} + 11\eta) \cdot n + 3\eta \cdot (n+1) + 5\eta && \text{(Equation (6.11))}\\
&\leq (n+r)^{-k_1} + \delta + \beta,
\end{aligned}$$

其中，最后一个不等式是通过令 $k_5 \triangleq k_1 + 1$ 和 $\eta \triangleq \beta/(50n)$ 得出的。这与 #rWPHP$[n-1,\ n^{-k_1}]$(PV) 矛盾，因此证明完毕。 □

6.3.3 压缩的伸展归约：(2) ⇒(3)

引理 6.11。 对于任意 $\varepsilon_2 \in (0,1)$ 和 $k_2 \in \mathbb{N}$，存在 $k_3 \in \mathbb{N}$ 使得 APX_1+#收缩弱鸽巢原理$[n^{\varepsilon_2}, n^{-k_2}](\mathsf{PV}) \vdash \mathsf{rrWPHP}[n-1, (n+r)^{-k_3}](\mathsf{PV})$。

证明。 固定任意常元 $\varepsilon_2 \in (0,1)$ 和 $k_2 \in \mathbb{N}$，并令 $k_3 \in \mathbb{N}$ 稍后确定。我们在 APX_1 中论证：若 rrWPHP$[n-1, (n+r)^{-k_3}]$(PV) 不成立，则 #rWPHP$[n^{\varepsilon_2}, n^{-k_2}]$(PV) 不成立。

假设 rrWPHP$[n-1, n^{-k_3}]$(PV) 不成立。那么存在 $n, r \in \mathsf{Log}$ 和电路 C：$\{0,1\}^n \times \{0,1\}^r \to \{0,1\}^{n-1}$, D：$\{0,1\}^{n-1} \to \{0,1\}^n$，使得对于每个 $x \in \{0,1\}^n$ 和每个 $\delta^{-1}, \beta^{-1} \in \mathsf{Log}$，令$T_x$：$\{0,1\}^r \to \{0,1\}$ 为满足以下条件的电路： $T_x(\mathsf{sd}) = 1$ 当且仅当 $D(C(x, \mathsf{sd})) \neq x$，则

$$\mathsf{P}_\delta(T_x) \leq (n+r)^{-k_3} + \delta + \beta. \tag{6.12}$$

换言之，存在一个一位随机压缩方案，其最坏情况正确率为 n^{-k_3}。我们的目标是构造一种确定性且针对平均情况的压缩-解压缩算法，从而违反 #rWPHP$[n^{\varepsilon_2}, n^{-k_2}]$(PV)。

压缩与解压缩电路。 令 $\ell \in \mathsf{Log}$ 和 $d \in \mathsf{LogLog}$ 为稍后确定的参数。压缩电路以一个 $(\ell + dr)$ 位字符串作为输入，将其解析为 $z \in \{0,1\}^\ell$ 和 $(\mathsf{sd}_1, \ldots, \mathsf{sd}_d) \in \{0,1\}^r$，并运行一个 d 轮迭代压缩算法。

初始化 $z_0 \leftarrow z$。在第 i 轮中，迭代算法按如下方式运行：

1. 将 z_{i-1} 解析为 $x_1 \circ x_2 \circ \cdots \circ x_k \circ y_i$，其中 $k \triangleq \lfloor |z_{i-1}|/n \rfloor$ 和 x_1、……、$x_k \in \{0,1\}^n$。 2. 对每个 $j \in [k]$，计算 $x'_j \triangleq C(x_j, \mathsf{sd}_i)$。

3. 设置 $z_i \leftarrow x'_1 \circ x'_2 \circ \cdots \circ x'_k$。

最后，压缩电路输出元组 $(z_d, y_1, \ldots, y_d, \mathsf{sd}_1, \ldots, \mathsf{sd}_d)$ 的编码).

解压缩电路接收 $(z_d, y_1, \ldots, y_d, \mathsf{sd}_1, \ldots, \mathsf{sd}_d)$，并通过一个 d 轮迭代算法反向运行。在第 i 次迭代中，算法执行如下：

1. 将 z_{d+1-i} 解析为 $x'_1 \circ x'_2 \circ \cdots \circ x'_k$，其中 $k \triangleq \lfloor |z_{d+1-i}|/(n-1) \rfloor$ 且 $x'_1, \ldots, x'_k \in \{0,1\}^{n-1}$。
2. 对每个 $j \in [k]$，计算 $x_j \triangleq D(x'_j)$。3. 设置 $z_{d-i} \leftarrow x_1 \circ x_2 \circ \cdots \circ x_k \circ y_{d+1-i}$。

现在设置参数 ℓ 和 d，使得上述压缩方案的伸展至少为 $(\ell+dr)^{\varepsilon_2}$。令 z_0、z_1、……、z_d、y_1、……、y_d 为通过压缩算法得到的字符串，显然有

$$|z_i| \le |z_{i-1}| \cdot \left(1 - \frac{1}{n}\right), |y_i| \le n,$$

因此，压缩电路的输出长度至多为

$$\ell \cdot \left(1 - \frac{1}{n}\right)^d + d \cdot (n+r).$$

我们可以设置 $\ell = (n+r)^{10/\varepsilon_2}$ 和 $d = 10 \cdot n\mathsf{Log}\ \ell$，使得输出长度至多为 $O(n(n+r)\ \mathsf{Log}\ \ell) \ll \ell^{\varepsilon_2} \le (\ell+dr)^{\varepsilon_2}$。因此，对于足够大的 n 和 r，压缩伸展为 $(\ell+dr)^{\varepsilon_2}$；当 n、r 较小时，可以通过穷举分类讨论证明。

错误概率分析。固定如上所述的 $\ell \in \mathsf{Log}$ 和 $d \in \mathsf{LogLog}$。令 C'：$\{0,1\}^{\ell+dr} \to \{0,1\}^{(\ell+dr)^{\varepsilon_2}}$，$D'$：$\{0,1\}^{(\ell+dr)^{\varepsilon_2}} \to \{0,1\}^{\ell+dr}$ 为上述提到的压缩和解压缩算法。令 T：$\{0,1\}^{\ell+dr}$ 为当且仅当 $D'(C'(z)) \ne z$ 时 $T(z) = 1$ 的电路，即压缩方案失败。我们的目标是证明，对于每个 δ^{-1}、$\beta^{-1} \in \mathsf{Log}$，$\mathsf{P}_\delta(T) \le (\ell+dr)^{-k_2} + \delta + \beta$。

固定任意 δ^{-1}，$\beta^{-1} \in \mathsf{Log}$，并令 $\eta^{-1} \in \mathsf{Log}$ 为稍后确定的参数。令 $V \triangleq \{0,1\}$。对于每个 $i \in [d]$ 和 $j \le \lfloor \ell/n \rfloor$，我们定义 $F_{ij}(z, \mathsf{sd}_1, \ldots, \mathsf{sd}_d)$ 为一个电路，当且仅当以下条件成立时输出 1：

- 在压缩算法的第 i 轮，令 $k \triangleq \lfloor |z_{i-1}|/n \rfloor$，则 $j \le k$ 和 $D(C(x_j, \mathsf{sd}_i)) \ne x_j$。

令 X_{ij} 为由 $(V, \ell+dr, F_{ij})$ 定义的随机变量。令 $F(z, \mathsf{sd}1, \ldots, \mathsf{sd}_d)$ 为一个电路，当且仅当存在某个 $i \in [d]$ 和 $j \le \lfloor \ell/n \rfloor$，使得 $F_{ij}(z, \mathsf{sd}1, \ldots, \mathsf{sd}_d) = 1$ 时输出 1；并令 Y 为由 $(V, \ell+dr, F_{ij})$ 定义的随机变量。根据并集界，我们有

$$\mathsf{P}_\eta(F) \le \mathbb{E}_\eta[Y] + 3\eta \le \sum_{ij} \mathbb{E}_\eta[X_{ij}] + 3\eta \cdot (d\ell + 1), \tag{6.13}$$

其中第一个不等式由命题3.12得出。

显然，PV 可以证明：对于任意 $z \in \{0,1\}^\ell$、$\mathsf{sd}1$、…、$\mathsf{sd}_d \in \{0,1\}^r$，若 $T(z, \mathsf{sd}1, \ldots, \mathsf{sd}_d) = 1$，则 $F(z, \mathsf{sd}1, \ldots, \mathsf{sd}_d) = 1$。为此，只需注意，若 $F(z, \mathsf{sd}1, \ldots, \mathsf{sd}_d) = 0$，我们可以对 i作归纳，证明：在输入 $z \circ \mathsf{sd}_1 \circ \cdots \circ \mathsf{sd}_d$ 上运行迭代压缩算法 i 轮，并从第 $d-i$ 轮开始运行迭代解压算法，就能正确解压缩。这可以通过对一个 PV 项作归纳来实现，而 PV 中有此归纳法。随后，根据近似计数的单调性，

$$\mathsf{P}_\eta(T) \le \mathsf{P}_\eta(F) + 3\eta. \tag{6.14}$$

接下来，我们证明 $\mathbb{E}_\eta[X_{ij}]$ 的一个上界。Fix 任意的 $i \in [d]$ 和 $j \le \lfloor \ell/n \rfloor$。令

$$\rho = (z, \mathsf{sd}_1, \ldots, \mathsf{sd}_{i-1}, \mathsf{sd}_{i+1}, \ldots, \mathsf{sd}_d)$$

是对 X_{ij} 的种子中除区间 sd_i 之外所有位置的任意赋值。令 x_j 为在输入 z 上，使用前 $i-1$ 轮中的种子 $\mathsf{sd}_1, \ldots, \mathsf{sd}_{i-1}$ 执行压缩算法时第 i 轮的字符串。注意

给定 ρ，可以通过一个 PV 项计算出 x_j。回想一下，$T_{x_j}(\mathsf{sd})$ 是一个电路，当且仅当 $D(C(x_j,\mathsf{sd})) \neq x_j$ 时输出 1。可以证明，$T_{x_j}(\mathsf{sd}_i) = 1$ 当且仅当 $F_{ij}(\rho \cup \mathsf{sd}_i) = 1$，即 $X_{ij}|_\rho$ 是 $T_{x_j}(\mathsf{sd}) = 1$ 的指示变量。随后，

$$\mathbb{E}_\eta[X_{ij}|_\rho] \le \mathsf{P}_\eta(T_{x_j}) + 6\eta \le (n+r)^{-k_3} + 8\eta, \tag{6.15}$$

其中，第一个不等式由命题 3.12 和全局一致性得出，第二个不等式则由方程(6.12)得出。

请注意，方程 (6.15) 对任意赋值 ρ都成立。根据期望的平均论证，我们还可以进一步推导出

$$\mathbb{E}_\eta[X_{ij}] \le n^{-k_3} + 8\eta + 3\eta \le n^{-k_3} + 11\eta. \tag{6.16}$$

结合以上结果，我们现在可以计算

$$\begin{aligned}
\mathsf{P}_\delta(T) &\le \mathsf{P}_\eta(T) + \delta + 2\eta && \text{(Precision Consistency Axiom)}\\
&\le \mathsf{P}_\eta(F) + \delta + 5\eta && \text{(Equation (6.14))}\\
&\le \sum_{ij} \mathbb{E}_\eta[X_{ij}] + 3\eta \cdot (d\ell + 1) + \delta + 5\eta && \text{(Equation (6.13))}\\
&\le ((n+r)^{-k_3} + 11\eta) \cdot d \cdot \ell + 3\eta \cdot (d\ell + 1) + \delta + 5\eta && \text{(Equation (6.16))}\\
&\le (\ell + dr)^{-k_2} + \delta + \beta,
\end{aligned}$$

其中，最后一个不等式是通过令 $\eta \triangleq \beta/(100(d\ell+1))$ 和 $k_3 \triangleq 100k_2/\varepsilon_2 + 10k_2 + 10$ 得出的。这表明电路对 C', D' 违反了收缩弱鸽巢原理$[n^{\varepsilon_2}, n^{-k_2}](\mathsf{PV})$，由此完成证明。 □

6.3.4 最坏情况到平均情况归约：(4) ⇒ (1)

引理6.12。 对于任意 $\varepsilon_4 \in (0、1)$ 以及 $k_4 \in \mathbb{N}$，存在 $k_1 \in \mathbb{N}$ 使得 $\mathsf{APX}_1 + \mathsf{rrWPHP}[n^{\varepsilon_4}, (n+r)^{-k_4}](\mathsf{PV}) \vdash \#\mathsf{rWPHP}[n-1, n^{-k_1}](\mathsf{PV})$。

我们将使用引理 6.11 中的迭代压缩算法将伸展提升至 m_2，同时需要一种新技巧，以便从平均情况压缩算法构造最坏情况压缩算法。从较高层次来看，我们观察到，具有较大伸展的压缩-解压缩问题具有 随机自归约性，并且可通过 重新随机化引理证明其正确性。

引理 *6.12*的证明。 固定任意常元 $\varepsilon_4 \in (0,1)$，$k_4 \in \mathbb{N}$，并令 $k_1 \in \mathbb{N}$ 稍后确定。我们将在 APX_1 中论证，假设 $\#\mathsf{rWPHP}[n-1, n^{-k_4}](\mathsf{PV})$ 不成立，则 $\mathsf{rrWPHP}[n^{\varepsilon_4}, (n+r)^{-k_4}](\mathsf{PV})$ 也不成立。换言之，我们将从单比特确定性平均情况压缩方案构造一个多项式伸展率随机最坏情况压缩方案。

反设收缩弱鸽巢原理$[n-1, n^{-k_1}](\mathsf{PV})$不成立。那么存在一个 $n \in \mathsf{Log}$和电路 $C\colon \{0,1\}^n \to \{0,1\}^{n-1}$, $D\colon \{0,1\}^{n-1} \to \{0,1\}^n$，使得以下结论成立。令 T为满足以下条件的电路：若 $D(C(x)) \neq x$，则 $T(x) = 1$。那么对每个 $\delta^{-1}, \beta^{-1} \in \mathsf{Log}$，$\mathsf{P}_\delta(T) \le n^{-k_1} + \delta + \beta$。根据重新随机化引理，我们知道，对每个 $x \in \{0,1\}^n$，令 $T_x^{\oplus}$为电路 $T_x^{\oplus}(\mathsf{sd}) \triangleq T(x \oplus \mathsf{sd})$，则

$$\mathsf{P}_\delta(T_x^{\oplus}) \le \mathsf{P}_\delta(T) + 2\delta + \beta \le n^{-k_1} + 3\delta + 2\beta. \tag{6.17}$$

注意，不失一般性，我们可以假设 n 大于任意固定的标准整数 $n_0 \in \mathbb{N}$，因为当 $n \le n_0$ 时，可以通过暴力搜索解决。

压缩与解压缩电路。 令 $\ell \in \mathsf{Log}$ 和 $d \in \mathsf{LogLog}$ 为稍后确定的参数。压缩电路以一个 ℓ位字符串 z作为输入，以及一个 nd位随机种子 $(\mathsf{sd}_1, \ldots, \mathsf{sd}_d) \in \{0,1\}^r$，并执行以下 d轮迭代算法。它初始化 $z_0 \leftarrow z$。在第 i轮中，算法按如下方式运行：

1. 将 z_{i-1} 解析为 $x_1 \circ x_2 \circ \cdots \circ x_k \circ y_i$，其中 $k \triangleq \lfloor |z_{i-1}|/n \rfloor$ 和 $x_1, \ldots, x_k \in \{0,1\}^n$；
2. 对每个 $j \in [k]$，计算 $x'_j \triangleq C(x_j \oplus \mathsf{sd}_i)$。3. 设置 $z_i \leftarrow x'_1 \oplus x'_2 \oplus \cdots \oplus x'_k$。

最后，压缩电路输出元组（z_d，y_1，……，y_d，sd_1，……，sd_d）的编码).

解压缩电路接收（z_d，y_1，……，y_d，sd_1，……，sd_d），并通过一个 d轮迭代算法逆向工作。在第 i次迭代中，该算法的工作方式如下：

1. 将 z_{d+1-i} 解析为 $x'_1 \circ x'_2 \circ \cdots \circ x'_k$，其中 $k \triangleq \lfloor |z_{d+1-i}|/(n-1) \rfloor$ 且 x'_1，……，$x'_k \in \{0,1\}^{n-1}$。
2. 对于每个 $j \in [k]$，计算 $x_j \triangleq D(x'_j) \oplus \mathsf{sd}_i$。3. 设置 $z_{d-i} \leftarrow x_1 \circ x_2 \circ \cdots \circ x_k \circ y_{d+1-i}$。

与引理 6.11 的证明类似，我们可以设置参数 $\ell \triangleq n^{10/\varepsilon_4}$ 和 $d \triangleq 10 \cdot n \log \ell$，使得上述压缩方案的伸展至少为 ℓ^{ε_4}。该压缩方案中随机字符串的长度为 $r \triangleq dn$。

错误概率分析。 Fix $\ell \in \mathsf{Log}$ 和 $d \in \mathsf{LogLog}$ 同上。令 $C'\colon \{0,1\}^\ell \times \{0,1\}^{dn} \to \{0,1\}^{\ell^{\varepsilon_4}}$，$D'\colon \{0,1\}^{\ell^{\varepsilon_4}} \to \{0,1\}^\ell$ 为上述压缩和解压缩算法。令$T_z\colon \{0,1\}^{dn} \to \{0,1\}$ 为电路，它将输入解析为 $\mathsf{sd} \triangleq (\mathsf{sd}_1, \ldots, \mathsf{sd}_d) \in \{0,1\}^{dn}$，并且当且仅当 $D'(C'(z,\mathsf{sd})) \neq z$ 时输出 1，也就是说，该压缩方案在输入 z 上失败。我们的目标是证明，对于每个 $\delta^{-1}, \beta^{-1} \in \mathsf{Log}$ 和 $z \in \{0,1\}^\ell$，$\mathsf{P}_\delta(T_z) \leq (\ell + dn)^{-k_4} + \delta + \beta$。

任取 $\delta^{-1}, \beta^{-1} \in \mathsf{Log}$ $z \in \{0,1\}^\ell$，并令 $\eta^{-1} \in \mathsf{Log}$ 为稍后确定的参数。令$V \triangleq \{0,1\}$。对于每个 $i \in [d]$ 和 $j \leq \lfloor \ell/n \rfloor$，我们定义 $F_{ij}(\mathsf{sd}_1, \ldots, \mathsf{sd}_d)$ 为当且仅当以下条件成立时输出 1 的电路：

- 在压缩算法的第 i 轮中，令 $k \triangleq \lfloor |z_{i-1}|/n \rfloor$，则 $j \leq k$ 和 $D(C(x_j \oplus \mathsf{sd}_i)) \neq x_j \oplus \mathsf{sd}_i$。

令 X_{ij} 为由 (V, dn, F_{ij}) 定义的随机变量。令 $F(\mathsf{sd}1, \ldots, \mathsf{sd}_d)$ 为当且仅当对于某个 $i \in [d]$ 和 $j \leq \lfloor \ell/n \rfloor$，$F_{ij}(\mathsf{sd}1, \ldots, \mathsf{sd}_d) = 1$ 时输出 1 的电路，并令 Y 为由 (V, dn, F_{ij}) 定义的随机变量。根据并集界，我们有

$$\mathsf{P}_\eta(F) \leq \mathbb{E}_\eta[Y] + 3\eta \leq \sum_{ij} \mathbb{E}_\eta[X_{ij}] + 3\eta \cdot (d\ell + 1), \tag{6.18}$$

其中第一个不等式由命题3.12得出。

显然，PV 可以证明：对于任意 $\mathsf{sd}1, \ldots, \mathsf{sd}_d \in \{0,1\}^r$，如果 $T_z(\mathsf{sd}1, \ldots, \mathsf{sd}_d) = 1$，那么就有$F(\mathsf{sd}1, \ldots, \mathsf{sd}_d) = 1$。为此，注意到如果 $F(\mathsf{sd}1, \ldots, \mathsf{sd}_d) = 0$，我们可以对 i 作归纳，证明若对输入 z 运行 i 轮迭代压缩算法，并从第 $d - i$ 轮开始运行迭代解压算法，那么它将被正确解压。这可以通过对一个 PV 项作归纳来实现，而 PV 中具备这种归纳法。随后，根据近似计数的单调性，

$$\mathsf{P}_\eta(T_z) \leq \mathsf{P}_\eta(F) + 3\eta. \tag{6.19}$$

接下来，我们证明 $\mathbb{E}_\eta[X_{ij}]$的一个上界。任取 $i \in [d]$ 和 $j \leq \lfloor \ell/n \rfloor$。令

$$\rho = (\mathsf{sd}_1, \ldots, \mathsf{sd}_{i-1}, \mathsf{sd}_{i+1}, \ldots, \mathsf{sd}_d)$$

是对 X_{ij} 的种子中除区间 sd_i 外所有位置的任意赋值。令 x_j 为压缩算法在输入 z 上使用前 $i-1$ 轮中的种子 sd_1、……、sd_{i-1} 时，第 i 轮得到的字符串。注意，给定 ρ 后，可以通过一个 PV项计算 x_j。回想一下，$T^{\oplus}_x(\mathsf{sd})$ 是一个电路，当且仅当 $D(C(x \oplus \mathsf{sd})) \neq x \oplus \mathsf{sd}$ 时输出 1。可以证明，$T^{\oplus}_{x_j}(\mathsf{sd}_i) = 1$ 当且仅当 $F_{ij}(\rho \cup \mathsf{sd}_i) = 1$，也就是说，$X_{ij}|_\rho$ 是 $T^{\oplus}_{x_j}(\mathsf{sd}) = 1$ 的指示变量。随后，

$$\mathbb{E}_\eta[X_{ij}|_\rho] \leq \mathsf{P}_\eta(T^{\oplus}_{x_j}) + 6\eta \leq n^{-k_1} + 11\eta, \tag{6.20}$$

其中，第一个不等式由命题 3.12 和全局一致性推出，第二个不等式由方程(6.17)推出。

注意，方程（6.20）对任意赋值 ρ均成立。根据期望的平均论证，我们可以进一步推出

$$\mathbb{E}_\eta[X_{ij}] \le n^{-k_1} + 11\eta + 3\eta \le n^{-k_1} + 14\eta. \tag{6.21}$$

结合上述结果，我们现在可以计算

$$\begin{aligned}
\mathsf{P}_\delta(T) &\le \mathsf{P}_\eta(T) + \delta + 2\eta && \text{(Precision Consistency Axiom)}\\
&\le \mathsf{P}_\eta(F) + \delta + 5\eta && \text{(Equation (6.19))}\\
&\le \sum_{ij} \mathbb{E}_\eta[X_{ij}] + 3\eta\cdot(d\ell+1) + \delta + 5\eta && \text{(Equation (6.18))}\\
&\le \left(n^{-k_1} + 14\eta\right)\cdot d\cdot\ell + 3\eta\cdot(d\ell+1) + \delta + 5\eta && \text{(Equation (6.21))}\\
&\le n^{-k_1}\cdot d\ell + \delta + \beta,
\end{aligned}$$

其中，最后一个不等式可通过令 $\eta \triangleq \beta/(100(d\ell+1))$ 得到。回想 $\ell = n^{10/\varepsilon_4}$和 $d = 10\cdot n\log\ell$，我们有

$$n^{-k_1}\cdot d\ell = n^{-k_1}\cdot n^{10/\varepsilon_4}\cdot\frac{100n}{\varepsilon_4}\cdot\log n \le n^{-k_4} \le (\ell+dn)^{-k_4}.$$

通过在 n 足够大时令 $k_1 \triangleq 100/\varepsilon_4 + 10k_4 + 10$。这表明 C'， D' 违反了 rrWPHP$_{m_2}$(PV)，从而完成证明。□

参考文献

[AAdRK25] Noel Arteche、Albert Atserias、Susanna F. de Rezende 和 Erfan Khaniki。证明分析问题。载于计算理论研讨会 (STOC)，2025年。[AAI+01] Manindra Agrawal、Eric Allender、Russell Impagliazzo、Toniann Pitassi 和 Steven Rudich。降低归约的复杂性。计算复杂性，10(2):117–138，2001年。[AB09] Sanjeev Arora 和 Boaz Barak。《计算复杂性——现代方法》。剑桥大学出版社，2009年。[ABM23] Albert Atserias、Sam Buss 和 Moritz M¨uller。非确定性时间电路下界的一致性。载于计算理论研讨会 (STOC)，第1257–1270页，2023年。[Agr01] Manindra Agrawal。迈向一致 AC^0-同构。载于计算复杂性会议 (CCC)，第13–20页，2001年。[AS16] Noga Alon 和 Joel H. Spencer。《概率方法》。约翰·威立父子公司，2016年。[AT25] Albert Atserias 和 Iddo Tzameret。Schwartz-Zippel引理的可行构造性证明及寻找命中集的复杂性。载于计算理论研讨会 (STOC)，第1096–1107页，2025年。[AvM11] Scott Aaronson 和 Dieter van Melkebeek。去随机化所导出的电路下界。理论计算，7(1):177–184，2011年。[AW89] Mikl´os Ajtai 和 Avi Wigderson。概率常深度电路的确定性模拟。计算机研究进展，5:199–222，1989年。[BCH+96] Mihir Bellare、Don Coppersmith、Johan H˚astad、Marcos A. Kiwi 和 Madhu Sudan。特征二上的线性测试。*IEEE* 信息论汇刊，42(6):1781–1795，1996年。

[BKKK20] Sam Buss、Valentine Kabanets、Antonina Kolokolova 和 Michal Kouck´y。VNC^{1}中的扩展图构造。《纯粹与应用逻辑年刊》，171(7):102796，2020年。[BKT14] Samuel R. Buss、Leszek A. Ko-lodziejczyk 和 Neil Thapen。近似计数的片段。《符号逻辑杂志》，79(2):496–525，2014年。[BLR93] Manuel Blum、Michael Luby 和 Ronitt Rubinfeld。自测试／自校正及其在数值问题中的应用。《计算机与系统科学杂志》，47(3):549–595，1993年。[Bus86] Samuel R. Buss。《有界算术》。Bibliopolis，1986年。[Bus94] Samuel R. Buss。关于赫布兰德定理。载于《逻辑与计算复杂性》(LCC)，《计算机科学讲义》第960卷，第195–209页。施普林格，1994年。[Bus97] Samuel R. Buss。有界算术与命题证明复杂性。载于《计算逻辑》，第67–121页。施普林格·柏林·海德堡，1997年。[CK07] Stephen A. Cook 和 Jan Kraj´ıˇcek。NP $\subseteq$P/poly 可证明性的推论。《符号逻辑杂志》，72(4):1353–1371，2007年。[CKK+25] Marco Carmosino、Valentine Kabanets、Antonina Kolokolova、Igor C. Oliveira 和 Dimitrios Tsintsilidas。电路规模层级的可证明性及其推论。载于理论计算机科学创新会议(ITCS)，第325卷，第30:1–30:22页，2025年。[CKKO21] Marco Carmosino、Valentine Kabanets、Antonina Kolokolova 和 Igor C. Oliveira。学习一致电路下界及其在有界算术中的可证明性。载于计算机科学基础研讨会（FOCS），2021年。[CL24] Yilei Chen 和 Jiatu Li。通过密码学研究受限电路的值域规避与远点问题的困难性。载于计算理论研讨会（STOC），第620–629页，2024年。[CLMP25] James Cook、Jiatu Li、Ian Mertz 和 Edward Pyne。催化空间的结构：通过压缩刻画随机性与时间。载于计算理论研讨会（STOC），第554–564页，2025年。[CLO24] Lijie Chen、Jiatu Li 和 Igor C. Oliveira。复杂性下界的逆向数学。载于计算机科学基础研讨会（FOCS），第505–527页，2024年。[CLO25] Lijie Chen、Jiatu Li 和 Igor C. Oliveira。直觉主义 S^1_2 中电路规模界的不可证性。《逻辑方法与计算机科学》，21(3)，2025年。[CN10] Stephen A. Cook 和 Phuong Nguyen。《证明复杂性的逻辑基础》。剑桥大学出版社，2010年。[Coo75] Stephen A. Cook。可行构造性证明与命题演算（初步版本）。载于计算理论研讨会（STOC），第83–97页，1975年。[CRT25] Lijie Chen、Ron D. Rothblum 和 Roei Tell。基于去随机化的明文模型 Fiat-Shamir（或者：高效算法是否相信 NP =PSPACE？）。载于计算理论研讨会（STOC），第977–985页，2025年。[CT21] Lijie Chen 和 Roei Tell。困难性与随机性：修订版——一致、非黑盒与逐实例。载于计算机科学基础研讨会（FOCS），第125–136页，2021年。[CT23] Lijie Chen 和 Roei Tell。客座专栏：研究 BPP $=$ P 猜想的新方法。《SIGACT 新闻》，54(2):44–69，2023年。

[CTW23] Lijie Chen、Roei Tell 与 Ryan Williams。去随机化与反驳：刻画去随机化的统一框架。载于计算机科学基础研讨会（FOCS），第1008–1047页，2023年。[For01] Lance Fortnow。比较完全去随机化的各种概念。载于计算复杂性会议（CCC），第28–34页，2001年。[FSS84] Merrick L. Furst、James B. Saxe 与 Michael Sipser。奇偶性、电路与多项式时间层次。Math. Syst. Theory，17(1):13–27，1984年。[Gay24] Azza Gaysin。CSP 二分定理证明中泛代数的证明复杂性，2024年。[GC25] Stefan Grosser 与 Marco Carmosino。学生-教师构造性分离与有界算术中的（不）可证明性：见证这一差距。载于计算理论研讨会（STOC），第1341–1347页，2025年。[Gol11] Oded Goldreich。在一个 p=bpp 的世界中。载于 Oded Goldreich 编，《复杂性与密码学研究》，《计算机科学讲义》第6650卷，第191–232页。施普林格，2011年。[Har04] Prahladh Harsha。稳健的邻近性 PCP 与更短的 PCP。博士论文，麻省理工学院，2004年。[HP93] Petr H´ajek 与 Pavel Pudl´ak。一阶算术的元数学。施普林格出版社，1993年。[IK06] Russell Impagliazzo 与 Bruce M. Kapron。关于密码学构造推理的逻辑。J. Comput. Syst. Sci.，72(2):286–320，2006年。[IKW02] Russell Impagliazzo、Valentine Kabanets 与 Avi Wigderson。寻找容易的见证：指数时间与概率多项式时间。J. Comput. Syst. Sci.，65(4):672–694，2002年。[ILW23] Rahul Ilango、Jiatu Li 与 Ryan Williams。不可区分混淆、值域规避与有界算术。载于计算理论研讨会（STOC），第1076–1089页。ACM，2023年。[IW97] Russell Impagliazzo 与 Avi Wigderson。若 E复杂度类需要指数电路，则 P = BPP：异或引理的去随机化。载于计算理论研讨会（STOC），第220–229页，1997年。[Jeˇr04] Emil Jeˇr´abek。对偶弱鸽巢原理、布尔复杂性与去随机化。《纯粹与应用逻辑年刊》，129(1-3):1–37，2004年。[Jeˇr05] Emil Jeˇr´abek。弱鸽巢原理与随机计算。博士论文，布拉格查理大学，2005年。[Jeˇr06] Emil Jeˇr´abek。尖锐有界归纳的强度。Mathematical Logic Quarterly，52(6):613–624，2006年。[Jeˇr07a]Emil Jeˇr´abek。有界算术中的近似计数。《符号逻辑杂志》，72(3):959–993，2007年。[Jeˇr07b] Emil Jeˇr´abek。论弱鸽巢原理变体的独立性。J. Log. Comput.，17(3):587–604，2007年。[Jeˇr09] Emil Jeˇr´abek。有界算术中基于哈希的近似计数。《符号逻辑杂志》，74(3):829–860，2009年。

[Jeˇr23] Emil Jeˇr´abek。VTC^{0}中的初等解析函数。《纯粹与应用逻辑年刊》，174(6)，2023年。文章编号103269，共50页。[JJ22] Abhishek Jain 与 Zhengzhong Jin。经由等价性的数学证明实现不可区分混淆。载于计算机科学基础研讨会（FOCS），第1023–1034页，2022年。[JJMP25] Abhishek Jain、Zhengzhong Jin、Surya Mathialagan 与 Omer Paneth。论经由命题证明的简洁混淆。载于计算机科学基础研讨会（FOCS），2025年。[JKLM25]Zhengzhong Jin、Yael Tauman Kalai、Alex Lombardi 与 Surya Mathialagan。由正确性证明得到的面向 NP 的通用简洁非交互论证。载于计算理论研讨会（STOC），2025年。[JKLV24] Zhengzhong Jin、Yael Kalai、Alex Lombardi 与 Vinod Vaikuntanathan。经由命题证明、在带误差学习假设下的简洁非交互论证。载于计算理论研讨会（STOC），第1750–1757页，2024年。[Kha24] Erfan Khaniki。跳跃算子、交互式证明与证明复杂性生成器。载于计算机科学基础研讨会（FOCS），第573–593页，2024年。[KKMP21] Robert Kleinberg、Oliver Korten、Daniel Mitropolsky 与 Christos H. Papadimitriou。多项式层次中的全函数。载于理论计算机科学创新会议（ITCS），第44:1–44:18页，2021年。[Kor21] Oliver Korten。最难的显式构造。载于计算机科学基础研讨会（FOCS），第433–444页，2021年。[Kor22] Oliver Korten。由时空权衡得到的去随机化。载于计算复杂性会议（CCC），第37:1–37:26页，2022年。[Kor25] Oliver Korten。值域规避与显式构造的复杂性。EATCS通报，145，2025年。[KPT91] Jan Krajˇıcek、Pavel Pudl´ak 与 Gaisi Takeuti。有界算术与多项式层次。《纯粹与应用逻辑年刊》，52(1-2):143–153，1991年。[Kra95] Jan Krajˇıcek。《有界算术、命题逻辑与复杂性理论》。数学及其应用百科全书。剑桥大学出版社，1995年。[Kra19] Jan Krajˇıcek。《证明复杂性》。数学及其应用百科全书。剑桥大学出版社，2019年。[Kra25] Jan Krajˇıcek。《证明复杂性生成器》。剑桥大学出版社，2025年。[LC11] Dai Tri Man Le 与 Stephen A. Cook。随机匹配算法的形式化。《逻辑方法与计算机科学》，8(3)，2011年。[Li25] Jiatu Li。面向计算机科学家的可行数学与有界算术导论。Electron. Colloquium Comput. Complex.，TR25-086，2025年。[LLR24] Jiawei Li、Yuhao Li 与 Hanlin Ren。归结下界的元数学：一种 TFNP 视角。预印本，2024年。[LO23] Jiatu Li 与 Igor C. Oliveira。有界算术中强复杂性下界的不可证性。载于计算理论研讨会（STOC），第1051–1057页，2023年。

[LP22]Yanyi Liu 和 Rafael Pass。通过 Levin-Kolmogorov 复杂性的困难性刻画去随机化。载于计算复杂性会议（CCC），第234卷，页码35:1–35:17，2022年。[LPT24] Jiatu Li、Edward Pyne 和 Roei Tell。区分、预测与认证：论部分伪随机性概念的深远影响。载于计算机科学基础研讨会（FOCS），页码1–13，2024年。[Lˆe14] Dai Tri Man Lˆe。有界算术与概率证明的形式化。博士论文，加拿大多伦多大学，2014年。[MDS25] Yaohua Ma、Chenxin Dai 和 Elaine Shi。通过等价性的数学证明实现准线性不可区分混淆及其应用。载于国际密码学理论与应用会议（EUROCRYPT），页码157–186，2025年。[MP20] Moritz M¨uller 和 J´an Pich。可行构造性证明：简洁弱电路下界。《纯粹与应用逻辑年刊》，171(2)，2020年。[Mul18] Wolfgang Mulzer。Chernoff界的五种证明及其应用。EATCS通报，124，2018年。[Nis92] Noam Nisan。空间受限计算的伪随机生成器。《组合学》，12(4):449–461，1992年。[NW94] Noam Nisan 和 Avi Wigderson。困难性与随机性。《计算机与系统科学杂志》，49(2):149–167，1994年。[Oja04] Kerry Ojakian。有界算术中的组合学。博士论文，卡内基梅隆大学，2004年。[Oli25]Igor C. Oliveira。计算复杂性理论的元数学。《SIGACT 新闻》，56(1):41–68，2025年。[Pic14] J´an Pich。可行数学中的复杂性理论。博士论文，布拉格查理大学，2014年。[Pic15a] J´an Pich。有界算术中的电路下界。《纯粹与应用逻辑年刊》，166(1):29–45，2015年。[Pic15b] J´an Pich。复杂性理论的逻辑强度及有界算术中 PCP 定理的形式化。《计算机科学逻辑方法》，11(2)，2015年。[PS21] J´an Pich 和 Rahul Santhanam。NP 的强共非确定性下界无法得到可行证明。载于计算理论研讨会（STOC），页码223–233，2021年。[Pud90] Pavel Pudl´ak。有界算术中的 Ramsey 定理。载于计算机科学逻辑（CSL），《计算机科学讲义》第533卷，页码308–317，1990年。[PWW88] Jeff B. Paris、A. J. Wilkie 和 Alan R. Woods。鸽巢原理的可证明性与无限多个素数的存在。《符号逻辑杂志》，53(4):1235–1244，1988年。[Raz95] Alexander A. Razborov。有界算术与布尔复杂性中的下界。载于《可行数学II》，页码344–386。Birkh¨auser，1995年。[Rii93] Søren M. Riis。在二阶有界算术模型中使无限结构有限化。载于 P. Clote 和 J. Kraj´ıˇcek（编），《算术、证明论与计算复杂性》，牛津逻辑指南第23卷，页码289–319。牛津大学出版社，牛津，1993年。

[RSW22] Hanlin Ren、Rahul Santhanam 和 Zhikun Wang。关于电路的范围规避问题。载于计算机科学基础研讨会 (FOCS)，2022年。[Tel19] Roei Tell。证明 prBPP=prP 与证明“几乎NP”不包含于 P/poly 一样困难。《信息处理快报》，152，2019年。[Tha02] Neil Thapen。有界算术模型中的弱鸽巢原理。博士论文，牛津大学，2002年。[Tha24] Neil Thapen。如何将大型复杂性类纳入 TFNP。《CoRR》，abs/2412.09984，2024年。[Tha25] Neil Thapen。关于 NEXP 更强下界的一致性。《CoRR》，abs/2504.03320，2025年。[Vad12] Salil P. Vadhan。伪随机性。《理论计算机科学基础与趋势》，7(1-3):1–336，2012年。[Wil14] Ryan Williams。非一致ACC电路下界。《ACM杂志》，61(1):2:1–2:32，2014年。[Yao82] 姚期智。陷门函数理论及其应用（扩展摘要）。载于计算机科学基础研讨会 (FOCS)，页码80–91，1982年。