arXiv:2302.04322v1 [quant-ph] 8 Feb 2023

量子自由博弈

AnandNatarajan* Tina Zhang†麻省理工学
院 麻省理工学院

2023年2月10日

摘要

两个或更多经典玩家参与的自由博弈的复杂性，基本上已由 Aaron- son、Impagliazzo 和 Moshkovitz [AIM14] 确定。在量子世界中，有两个复杂性类可视为经典自由博弈的量子类比：(1) AM*，对应于有纠缠 玩家的自由博弈的多证明者交互证明类；以及稍不明显的 (2) BellQMA(2)，即具有两个无纠缠 Merlin 的量子 Merlin–Arthur 证明系统类，其证明状态由 Arthur分别 测量。在这项工作中，我们在对这两个类进行紧确刻画方面取得了重大进展。

1. 我们展示了一个针对含 n 个变量的 3SAT 的 BellQMA(2) 协议，其通信总量为 $\tilde{O}(\sqrt{n})$。这回答了 Chen 和 Drucker [CD10] 提出的一个未解决问题，同时也表明，在指数时间假设成立的条件下，Brandao、Christandl 和 Yard [BCY10] 用于在可分态上进行优化的算法，除对数因子外是紧的。2. 我们证明 $AM^*[n_{provers} = 2, q = O(1), a = \text{poly}\log(n)] = RE$，即具有常数大小问题的自由纠缠游戏与一般纠缠博弈同样强大。（相比之下， [AIM14]表明，经典自由博弈比一般经典博弈弱得多。）我们使用一个问题“超压缩”定理证明了这一点，该定理迭代应用 Ji 等人 [JNV+20]的内省技术。我们的结果显著改进了 Ji 等人的主要结果；后者针对停机问题的多证明者交互式证明协议具有 poly(n) 大小的问题和答案。3. 通过相同的技术，我们为一个递归枚举语言获得了一个零间隙 AM* 协议，该协议具有常数大小的问题和近似对数大小的答案（$O(\log n \ \log^* n)$），改进了 Mousavi、Nezhadi 和 Yuen [MNY21]的主要结果。4. 利用停机问题的非一致复杂度之间的联系，我们证明任何针对递归枚举语言的多证明者交互式证明协议都需要 $\Omega(\log n)$ 个通信比特。因此，我们第 3 项中的结果除 $O(\log^* n)$ 因子外是最优的，并且 [MNY21] 的无间隙压缩定理在渐近意义下是最优的。我们猜想，在有间隙情形下这些界也可以达到。

*anandn@mit.edu
†tinaz@mit.edu

目录

1 引言 31.1 BellQMA(2) ..... 4 1.1.1 背景与先前工作..... 4 1.1.2 我们关于 BellQMA(2) 的结果..... 6 1.2 AM*(2) ..... 8 1.2.1 背景与先前工作..... 8 1.2.2 我们关于 AM*(2) 的结果..... 8 1.3 基于柯尔莫哥洛夫复杂度的多证明者交互式证明* 协议下界..... 10 1.4 相关工作..... 11 1.5 未解决问题..... 11

2 预备知识 **13**

2.1 概率基础.13 2.2 量子信息基础.13 2.3 柯尔莫哥洛夫复杂度.13 2.4 非局域博弈与多证明者交互式证明* 协议.13 2.4.1 非局域博弈.13 2.4.2 无间隙博弈族与 $AM_0^*(2)$ 协议.14 2.4.3 有间隙的游戏族与多证明者交互式证明*(2) 协议.16 2.4.4 无间隙与有间隙定义之间的关系.18 2.5 QMA(2) 及相关复杂性类.18

3 用于 3SAT 的 BellQMA（2）**协议 18**

3.1 协议.18 3.2 均匀性测试的可靠性.19 3.3 一致性测试的可靠性及主协议的可靠性.23 3.4 基于指数时间假设的h^{Sep} 下界.26

4 免费纠缠游戏：无间隙情形 26

4.1 游戏的细粒度压缩定理.27 4.1.1 无间隙问题归约.27 4.1.2 无间隙答案归约.28 4.1.3 无间隙压缩.30 4.2 无间隙超压缩.30

5 自由纠缠游戏：有间隙情形 34

5.1 粒度化有间隙压缩定理.34 5.1.1 有间隙问题约简.34 5.1.2 有间隙答案约简.37 5.1.3 有间隙压缩.41 5.2 有间隙超压缩.43

6 柯尔莫哥洛夫复杂度界 45

7 致谢 49

1 引言

Babai、Fortnow 和 Lund 于 1991 年的研究表明，MIP = NEXP [BFL91] 至今仍是复杂性理论领域最重要的成果之一。证明中使用的技术为其他几项重要成果铺平了道路，其中包括 PCP = NP[AS98、ALM+98] 的证明，以及较近的 MIP* = RE [JNV+20]。简而言之，历史表明，对多人游戏的研究——在这类游戏中，一位诚实的多项式时间验证者担任裁判，主持一场由两名或更多可能不诚实且能力无界的证明者参与的博弈——为复杂性理论领域带来了最富成果的研究方向之一。

在多人博弈中，验证者受计算能力限制，天然处于劣势，因此必须巧妙地迫使与之交互的无界证明者代为执行计算，尽管验证者未必能亲自重复这些计算，以检查其是否准确完成。验证者可运用的最有力手段之一，就是向证明者提出相关问题。例如，多证明者证明设计中一种常见的范式是一致性测试：验证者要求一位证明者（“Alice”）给出其试图判定的整体问题中的某个小型子问题的答案，同时要求另一位证明者（“Bob”）给出同一子问题答案的一部分。这种范式的一个例子是子句-变量博弈。在该博弈中，验证者试图判断某个约束满足问题（CSP）实例（例如3SAT或图着色问题）是否可满足；它要求Alice给出该CSP中某个单独约束的满足赋值，并要求Bob只给出该约束所涉及的某一个变量的赋值。例如，若验证者试图判定一个3SAT实例，它可以要求Alice给出3SAT公式中某个单独子句的满足赋值，并要求Bob给出该子句中某个变量的赋值。随后，验证者会检查Alice提供的赋值确实满足该子句，并进一步检查Bob的答案是否与Alice的赋值一致。注意，即使整个公式不可满足，3SAT公式中的单个子句也总是有满足赋值。阻止Alice和Bob利用这一点说服验证者相信不可满足的公式可满足的关键在于，他们无法彼此沟通。因此，Alice要想与Bob保持一致，唯一的办法就是事先商定好一份与3SAT公式的全局满足赋值一致的答案。否则，如果Alice报告的赋值取决于验证者给她的子句，她就无法与Bob保持一致，因为Bob并不知道她拿到的是哪个子句。

与单证明者 NP 风格验证相比，一致性测试范式具有一个至关重要的优势：在单证明者 NP 风格验证中，验证者只需要求提供一个满足 3SAT 实例中所有子句的赋值，并检查该赋值确实满足所有子句；而一致性测试则允许验证者高效地检查约束满足问题的可满足性，即使其中的子句数量远远超过验证者逐一读取它们所能高效处理的数量。具体而言，一致性测试范式使多项式有界的验证者能够仅用多项式时间检查一个指数级长度的约束满足问题是否可满足，或是否远未达到可满足状态，因为验证者只需向 Alice 和 Bob 发送长度为多项式的问题，即可指定它想要了解指数级长度的约束满足问题中的哪个约束和哪个变量。这是 MIP = NEXP 等结果背后的核心且必不可少的验证框架。

于是我们可以提出这样的问题：如果我们剥夺验证者这一能力——它对于设计许多多证明者交互式证明系统至关重要，并允许验证者向证明者提出相关问题（从而执行一致性测试之类的测试）——会怎样？如果我们要求验证者向证明者提出的问题必须独立采样，多人游戏模型的计算能力会发生怎样的变化？在这一模型中，一个计算高效的验证者负责裁判一场涉及两个或更多可能不诚实且无界的证明者的博弈，并且验证者向证明者提出的问题必须由独立采样且均匀随机的比特组成；该模型被称为自由游戏模型。本文将主要讨论自由游戏模型。

Aaronson、Impagliazzo 和 Moshkovitz 于 2014年 研究了经典自由博弈的能力[AIM14]。他们定义了复杂性类 AM(k)，它恰好包含这样一类问题：这些问题可由一个计算高效的验证者通过与k 个可能不诚实且无界的证明者交互来判定，但须满足验证者向证明者提出的问题由独立抽取的均匀随机比特组成这一限制。Aaronson、Impagliazzo 和 Moshkovitz 还证明，对于任意$k = \text{poly}(n)$，其中n 是验证者输入的长度，AM(k) = AM。

这说明，相较于经典多人游戏的全部能力，经典自由博弈非常弱。Babai、Fortnow 和 Lund [BFL91] 证明了，多证明者交互式证明(2) 包含 NEXP，其中多证明者交互式证明(2)

对应于“不受限制”的双玩家多人博弈模型；另一方面，Aaronson、Impagliazzo 和 Moshkovitz 证明了，当我们强制验证者提出独立抽样的问题时，它只能判定 AM 中的问题——在合理的复杂性理论假设下，该类等于非确定性多项式时间 [MV05]。也就是说，在经典世界中，对验证者施加自由游戏限制，似乎会导致其判定能力呈指数级下降！

直观地说，我们可以如下理解这种关系。将 MIP(2) 协议转化为 AM(2) 协议的已知最佳范式，就是我们所说的生日重复。假设存在一个单轮 MIP(2) 协议 P，其完备性-可靠性差距为常数，该协议允许验证者判定某个我们感兴趣的语言 L，并且验证者会从集合 $\mathcal{X} \times \mathcal{Y}$ 中为两个证明者采样相关问题 (x, y)。为简单起见，假设验证者从集合 $\mathcal{S} \subseteq \mathcal{X} \times \mathcal{Y}$ 中均匀随机地采样 (x, y)。（例如，我们先前讨论的子句-变量例子就符合这一情况。）我们只需让自由验证者独立随机地从 $\mathcal{X}$ 中采样 k 个问题 $(x_1, \ldots, x_k)$，并从 $\mathcal{Y}$ 中采样 ℓ 个问题 $(y_1, \ldots, y_\ell)$，就能得到该协议的自由版本 P^{free}。随后，验证者检查是否存在 (x_i, y_j)，使得对于 $i \in [k], j \in [\ell]$，有 $(x_i, y_j) \in \mathcal{S}$。如果存在这样一对 (x_i, y_j)，自由验证者就按照 MIP 验证者的做法行事；否则，它会自动接受。

我们可以将集合 $\mathcal{X} \times \mathcal{Y}$ 表示为一个二部图 $\mathcal{G}$：左侧的每个 $x \in \mathcal{X}$ 对应一个顶点，右侧的每个 $y \in \mathcal{Y}$ 也对应一个顶点。我们还可以设想，当且仅当 $(x, y) \in \mathcal{S}$ 时，x 和 y 之间有一条边。假设 $\mathcal{G}$ 中的每个顶点至少参与一条边（也就是说，Alice 的每个问题 $x \in \mathcal{X}$ 都有非零概率被问到，Bob 的每个问题也同样如此），那么从 $\mathcal{X}$ 中均匀随机选取 x，并从 $\mathcal{Y}$ 中独立且均匀随机选取 y 时，$(x, y) \in \mathcal{S}$ 的概率至少为 $\Omega\left(\frac{|\mathcal{X}|+|\mathcal{Y}|}{|\mathcal{X}||\mathcal{Y}|}\right)$。当 $|\mathcal{X}| \approx |\mathcal{Y}| := N$ 时，该概率为 $\Omega(1/N)$。因此，根据生日悖论，为了确保 P^{free}（即多证明者交互式证明协议 P 的自由版本）仍具有常数可靠性，我们预计需要令 $k \approx \ell \approx O(\sqrt{N})$。（我们称这种将非自由游戏转化为自由博弈的过程为生日重复，因为它与生日悖论有关。）

对于强大到足以涵盖所有 NEXP 的多证明者交互式证明协议，正如我们先前提到的，$|\mathcal{X}|$ 和 $|\mathcal{Y}|$ 通常都随输入长度呈指数级增长。换句话说，要通过生日重复将一个 MIP(2)-完全协议转换为 AM(2) 协议，验证者就需要向证明者发送长度为 2^{cn} 的问题，其中 c 是某个常数，n 是输入的长度。这显然在计算上不可行。只有当问题集 $\mathcal{X}$ 和 $\mathcal{Y}$ 的规模为多项式级时，生日重复在计算上才可行；换句话说，只有当验证者要判定的约束满足问题长度仅为多项式级时才可行。这样我们就回到了非确定性多项式时间的情形。

然而，在先前一系列工作的基础上 [BT09、ABD+09]，Aaronson、Impagliazzo 和 Moshkovitz 还指出，自由验证者与两个不通信证明者交互时能够做到一件事，而任何与单个证明者交互的多项式有界验证者都做不到：前者能够~~仅~~使用 O（$\sqrt{N} \cdot \text{polylog}\, N$）比特与证明者通信来判定 3SAT，其中 N 是 3SAT 实例中的子句数。假设指数时间假设（ETH）成立，即 3SAT 无法在 $2^{o(N)}$ 时间内求解，那么与单个证明者交互的多项式有界验证者就无法如此高效地验证 3SAT：任何能够做到这一点的此类验证者，都会导出一个求解 3SAT 的亚指数时间算法。因此，尽管 AM(2) = NP 可能确实成立，但负责裁决双人自由博弈的验证者仍可能具备与单个证明者交互的多项式有界验证者所不具备的能力。

1.1 BellQMA(2)

1.1.1 背景与先前工作

Aaronson、Impagliazzo 和 Moshkovitz 最初研究经典自由博弈的动机 [AIM14，第 4] 节，是后者在次线性通信中判定 3SAT 的应用；其中的核心思想最初并非源自经典文献，而是来自对一个称为 QMA(2) 的量子复杂性类的研究。粗略地说，如果非确定性多项式时间是指这样一类问题：经典验证者在获得经典见证后可以高效地判定这些问题；而 QMA 是指这样一类问题：量子验证者在获得量子见证后可以高效地判定这些问题，那么 QMA(2) 就是指这样一类问题：量子验证者在获得

[1]实际上，$2^{o(n)}$ 这是 所 3SAT 实例中的变量数量，但对于困难实例而言，这与 N 呈线性关系。

量子见证后可以高效地判定这些问题。对于非确定性多项式时间，区分一个见证和两个见证显然毫无意义：任意两个经典见证都可以串接成一个见证，而任意一个经典见证也可以随意拆成两个。在 QMA(2) 中，一个见证和两个见证之间的区别却有了明确含义，因为要求这“两个”见证态必须是无纠缠的 （或者等价地，它们来自两个无法通信、不能共享纠缠的证明者）。如果高效量子验证者能够自行检验无纠缠性，那么任何 QMA(2) 协议都可以转换成 QMA 协议；然而，目前尚未 证明这一点，而且 QMA(2) $=$ QMA 是否成立仍然未知。当然，我们也可以对 $k \geq 2$ 定义 QMA(k)，其中量子验证者从k 个彼此独立的证明者那里接收k 个无纠缠见证。

我们认为，QMA(2) 设置最有说服力的应用实例，是以次线性通信解决非确定性多项式时间问题。（在指数时间假设成立的条件下，这一问题无法在 QMA 设置中实现。）也就是说，我们知道一种 QMA(2) 协议，其中两位证明者各自只向量子验证者发送 $O(\sqrt{N} \cdot \log N)$ 个量子比特；其中N 是 3SAT公式 ϕ中的子句数，而该验证者随后能够以常数错误概率判定 ϕ。（请注意，在 QMA(2) 模型中，量子验证者不会向两位证明者发送任何挑战，这与 AM(k) 模型不同——QMA(2) 协议中的所有通信都通过证明者发给验证者的一条量子消息完成。）最初，有人针对 QMA($\sqrt{N}$ poly log N) 设置提出了一种以次线性通信判定 3SAT 的协议 [ABD$^+$09]；在该协议中，量子验证者与 $\sqrt{N}$ poly log N位独立的证明者交互。随后， [HM13] 证明存在一种 QMA(2) （双证明者）协议，能够以相近的总通信长度实现同样的目的。

普遍出现的 $\sqrt{N}$ 也出现在出于同一目的而设计的 [AIM14] AM(2)协议的通信复杂度中，这并非巧合——事实上，用次线性通信判定 3SAT 的 [AIM14] AM(2) 协议深受最初为 QMA(2)设计的协议启发。$\sqrt{N}$ 这一因子确有一定依据：它源于对生日悖论 [ABD$^+$09] 的巧妙应用。迄今为止，还没有人想到其他可能取得更好结果的技术。因此，人们自然会想知道，是否无法避免使用 $\sqrt{N}$ 个量子比特进行通信。是否任何用于 3SAT 的 QMA(2)协议都必须至少使用$O(\sqrt{N})$ 个量子比特进行通信?

遗憾的是，在这种情况下，我们能够证明的通信下界与上界并不完全吻合。目前已知的、关于判定 3SAT 的 QMA(2) 协议通信复杂度的最佳下界源自 [BCY10]，，其证明表明：如果存在任何特定受限形式的QMA(2) 协议，能够以常数错误概率判定 3SAT，那么该协议至少必须使用$O(\sqrt{N})$ 个量子比特进行通信。 [BCY10] 证明，任何通信复杂度更低的此类协议都会推出一个用于 3SAT 的亚指数时间算法，因而与指数时间假设相矛盾。

在 [BCY10] 的下界证明中所考虑的受限模型是这样的：量子 QMA(2) 验证者的行为仿佛由两个独立的参与者组成——称他们为 Arthur 和 Lancelot——两人分别接收全能证明者提供的两个无纠缠见证之一。随后，Arthur 和 Lancelot 可以分别对各自的见证态进行测量，并进行经典通信。在彼此经典地传达测量结果后，他们可以继续进行更多测量，然后再次进行经典通信，直到无穷；但是，他们不能执行跨越两个见证态的任何纠缠测量。经过多轮独立测量和经典通信后，Arthur 和 Lancelot 最终输出一个联合判定。该模型称为局部操作与经典通信（LOCC）模型，而验证者被限制为按这种方式行动的 QMA(2) 版本称为 LOCC-QMA(2)。[BCY10] 证明，对于 3SAT，任何 LOCC-QMA(2) 协议都必须使用至少$O(\sqrt{N})$ 个量子比特与证明者和验证者进行通信。

关于在 LOCC-QMA（2）模型中求解 3SAT 所需通信量的上界，我们知道些什么？即使无法为 NP 的一般 QMA（2）协议刻画其类别，至少能否得到一个紧确刻画？当然，LOCC-QMA 模型包含这样一种模型：Arthur 和 Lancelot 各自对自己的见证恰好进行一次测量，然后对测量结果进行联合的经典计算，以确定判定结果。后一种模型称为 BellQMA 模型。2010年，在 Blier 和 Tapp 的工作基础上， [BT09], Chen 和 Drucker [CD10] 提出了一个极为简洁的 BellQMA 版本，用于实现最初的 [ABD$^+$09] QMA（$\sqrt{N}$ poly log N） 3SAT 协议。在

Chen-Drucker 协议中，每个独立的量子见证都要分别测量，验证者随后对这些测量得到的经典测量结果进行经典后处理，以确定最终判定。Chen-Drucker 协议的总通信复杂度为$O(\sqrt{N}\cdot \log N)$量子比特。因此，Chen-Drucker 协议看起来似乎满足了我们的期望：为 NP 提供一种 LOCC-QMA 协议，其通信复杂度与 Brand˜ao、Chri- standl 和 Yard 证明的 LOCC-QMA 协议通信复杂度下界相匹配（相差至多 $\log N$ 因子）。遗憾的是，Chen-Drucker 协议需要 $\sqrt{N}$ 个无纠缠证明者，而不只是两个，因此它无法证明 [BCY10] 算法给出的通信下界是最优的。[2]

尽管如此，针对非确定性多项式时间的 Chen-Drucker 协议揭示了 BellQMA(k) 与 AM(k)之间密切的联系，这种联系乍看之下或许并不明显。Chen-Drucker 协议的关键要素是一种称为均匀性测试的量子测试。大体而言，该测试涉及在傅里叶基下测量证明者提供的见证态中的某些寄存器，并要求测量结果为零。零傅里叶态是标准基下的均匀叠加态。因此，从某种意义上说，均匀性测试可以取代 AM(k) 模型中由验证者生成的均匀随机挑战，因为均匀性测试在某种意义上迫使证明者自行生成均匀抽样的挑战。具体而言，如果证明者向我们（验证者）提供如下形式的状态

$$|\psi\rangle = \sum_{q\in\mathcal{Q}} \alpha_q |q\rangle_Q |a(q)\rangle_A \tag{1}$$

其中 $\mathcal{Q}$ 是一组问题，而$a(q)$ 表示对给定问题q的答案；如果我们能够以某种方式证明这些 α_q彼此相等（也就是说，如果我们能够以某种方式将问题寄存器Q与答案寄存器A“解纠缠”之后，证明该问题寄存器处于均匀叠加态），那么在标准基下测量该状态 $|\psi\rangle$，就等同于抽取一个均匀随机的问题$q \in \mathcal{Q}$, 将其发送给证明者，并接收证明者给出的答案$a(q)$。因此，利用均匀性测试替代均匀生成的挑战，我们便可以——暂且把不可避免的种种保留意见都抛诸脑后——在 BellQMA(k) 中模拟 AM(k)协议。

当然，现实并没有这么简单：要在 BellQMA(k) 中模拟 AM(k) 的这种方法，并不像我们刚才含糊地描述的那样具有普适性。特别是，要使均匀性测试技术奏效（也就是存在一种能通过均匀性测试的诚实的策略），答案 $a(q)$ 必须很短——长度为常数，或至多为对数级。原因在于，为了真正使问题寄存器 Q 处于我们定义为 $|0\rangle_{\mathcal{F}} = \sum_{q\in\mathcal{Q}} \frac{1}{\sqrt{|\mathcal{Q}|}}|q\rangle$ 的零傅里叶态，

我们需要先将它与答案寄存器“解纠缠”，而这项操作涉及测量答案寄存器，并对某个测量结果进行后选择；如果答案很长，该结果出现的概率会小到可以忽略。

然而，如果问题 q 表示约束满足问题中的约束，而答案 $a(q)$表示对这些约束所涉及变量的赋值，那么一切就迎刃而解了。在几乎所有经过深入研究的约束满足问题中，例如 3SAT 和图着色，任意一个约束以及对该约束中任意单个变量的赋值，都可以用常数个比特来描述！因此，采用子句-变量范式的 3SAT AM(k) 协议，至少在概念上，确实可以通过这种方式“编译”为 BellQMA(k)协议——这正是 Chen-Drucker 协议的出发点。

1.1.2 我们关于BellQMA(2)的结果

在这项工作中，我们通过展示一种 BellQMA(2)（双证明者）协议，解决了一个问题： [BCY10] 证明的 LOCC-QMA(2) 下界是否紧致。该协议的通信复杂度为$O(\sqrt{N}\cdot\log N)$，并以常数错误概率判定 3-SAT 实例。Chen 和 Drucker 在发表他们的协议后，于 2010 [CD10] 中提出了这个问题；此后其他人也曾多次提出或提及该问题 [CF11, Question 1] [BH13] [AIM14], ，但尽管如此，这个问题仍悬而未决，已逾十年。为解决这一问题，我们给出了对 Chen-Drucker 均匀性测试（可以说是）更简单的分析，并对一个用于 3SAT 的 QMA(2) 协议进行了更具模块化的分析

[2]我们指出，原始的 [ABD+09] 协议也要求 $\Omega(\sqrt{N})$ 无纠缠证明者；之后，[HM13]通过“编译”将其转化为双证明者协议。不过，这种“编译”技术需要对多个见证态进行纠缠测量。我们还指出，在多方场景中，Brand˜ao 和 Harrow [BH13]证明了 Chen-Drucker 协议的最优性。

其通信量比我们所知的任何其他协议都更低，呈次线性增长；我们希望这在概念上也能有所助益。

因此，我们证明，在指数时间假设成立的前提下， [BCY10] 算法（用于将 LOCC-QMA(2) 协议的博弈值近似到常数加性误差）的运行时间在对数因子范围内是最优的。这是因为，任何对其算法的改进，若与我们的协议结合起来，就会得到一个用于 3SAT 的亚指数时间算法，这将与指数时间假设相矛盾。

我们的协议与 Chen-Drucker 协议非常相似。我们所做的主要改动在于分析，而这些改动基于这样一个观察：均匀性测试的可靠性实际上并不需要无纠缠性。Chen 和 Drucker 假设，其协议中的$k = O(\sqrt{N})$ 诚实证明者向验证者提供$k = O(\sqrt{N})$ 个无纠缠副本，其状态具有公式 (1) 中的形式；并定义了一个k态均匀性测试（当然，可以通过对各个状态分别进行测量来实现），该测试具有以下性质：

1. 完备性：诚实的证明者提供k 份形如公式 (1) 的状态，其中 $\alpha_q = \alpha^*$，对于某个常数 α^*，对所有q 均成立，则通过k态均匀性测试的概率为 $1 - 2^{-\Omega(k)}$。2. 可靠性：任何k 个无纠缠状态若以高概率通过k态均匀性测试，则其中足够多的状态都具有公式 (1) 中的形式，其中 $\alpha_q \approx \alpha^*$，对于某个常数 α^*，对所有q均成立。

我们的核心观察如下：对于某种我们即将定义的可靠性形式，k态均匀性测试的输入态不必处于k 个无纠缠寄存器中。我们证明的可靠性保证可非正式地表述如下：

引理1 (引理 26 的非正式版本)**.** 设 $|\psi\rangle$ 是以高概率通过 *Chen-Drucker k* 态均匀性测试的任意状态。$|\psi\rangle$ 不失一般性地分为 k 个“问题寄存器”和 k 个“答案寄存器”，`如公式(1)所示，这些寄存器可能相互纠缠。 $|\psi\rangle$ 满足：在标准基中测量所有问题寄存器后，在足够多的寄存器上（近似地）得到均匀随机字符串，其余位置则为无关内容。

引理 1 是我们这部分工作的主要技术引理。现在我们将说明，引理 1 如何给出一个用于 3SAT 的双证明者 BellQMA 协议，其通信量为 $O(\sqrt{N} \cdot \log N)$。

[AIM14] 给出了一个 AM(2) （经典双验证者自由博弈）协议，其通信复杂度为 $\widetilde{O}(\sqrt{N} \cdot \log N)$，能够以常数错误概率判定 3-SAT 实例。该协议（由于其受 Chen-Drucker 协议启发）恰好是一个子句-变量博弈，可按照我们在第 1.1.1 节末尾所述的方式由 BellQMA 协议“模拟”。具体来说，验证者 Arthur 向第一位证明者 Alice 提出的问题包含约束满足问题中的 k 个约束；对于每个约束，Arthur 期望收到一个答案，其中包含对该约束涉及的变量所作的常数大小赋值。与此同时，Arthur 向第二位证明者 Bob 提出的问题包含同一约束满足问题中的 k 个变量；对于发送给 Bob 的每个变量，Arthur 都期望收到对该变量的常数大小赋值。因此，借助我们在第 1.1.1 节末尾所述的直觉，我们可以将 [AIM14]AM(2) 协议“编译”为 BellQMA(2) 协议：对于任一证明者，诚实策略都是提供 k 份形如公式 (1) 的状态副本，其中 $\alpha_q = \alpha^*$ 对于某个常数α^* 对所有 q 均成立。接着，我们可以使用 Chen-Drucker k 状态均匀性测试，确保问题是均匀采样的。完备性成立，因为对任何给定问题的答案大小都是常数；而我们在引理 1 中证明的可靠性形式，足以推出[AIM14]的可靠性保证。

引出引理 1 证明的主要技术观察如下。粗略地说，Chen-Drucker k 态均匀性测试的结构如下：

1. 给定一个作用于k 个问题寄存器和k 个对应答案寄存器上的输入态 $|\psi\rangle$：在傅里叶基下测量所有答案寄存器。如果所得测量结果中有“足够多”的零，我们就继续；否则就拒绝。（这里不具体说明“足够多”是什么意思。详情见图 2。）

2. 对于每个 $i \in [k]$: 如果在步骤1中测量第i个答案寄存器得到零，则也在傅里叶基下测量第i个问题寄存器。如果对于任何这样的i，答案都不为零，则拒绝；否则，如果对于所有满足以下条件的i，即在步骤1中测量第i个答案寄存器得到零，答案都为零，则接受。

直观地说，该测试试图利用我们在第 1.1.1 节末尾所解释的直觉，以保证尽可能多的问题寄存器处于均匀叠加态。步骤1是必要的，因为我们必须先将答案寄存器与问题寄存器“解纠缠”。我们不会详细解释该测试的完备性，因为相关分析见 [CD10，第 3 节1]。相反，我们将概述如何证明引理 1。

假设我们有某个状态 $|\psi\rangle$，它以概率 1 通过了这项测试。那么，步骤1中的测量将得到一组「较大」的索引 $\mathcal{S} \subseteq [k]$，使得对于所有 $i \in \mathcal{S}$，第 i 个答案寄存器在傅里叶基下测得为零。将步骤1中的测量完成后的测量后状态记为 ρ_1。由于 $|\psi\rangle$ 以概率 1 通过了 k-状态均匀性测试，我们知道 ρ_1 必然有「大量」问题寄存器处于零傅里叶态（也就是说，ρ_1 中由 $i \in \mathcal{S}$ 索引的所有问题寄存器都必须处于零傅里叶态——否则步骤2就会拒绝）。因此，如果我们假设在标准基下测量 ρ_1 的问题寄存器，那么大量问题寄存器会得到均匀随机的结果，其余位置则会得到无关结果。

关键观察在于，后面这个假设的、对问题寄存器进行的标准基测量，与我们在步骤1中对答案寄存器进行的傅里叶基测量彼此可交换——因为它们作用于不同的寄存器。因此，即使我们不先按照测试的要求测量 $|\psi\rangle$ 的答案寄存器，而是直接在标准基下测量 $|\psi\rangle$ 的问题寄存器，也会在“数量很多”的问题寄存器上得到均匀随机的结果，而在其余寄存器上得到无用结果，就像我们测量了 ρ_1 的问题寄存器一样。引理 1 得证。

1.2 $\mathsf{AM}^*(2)$

1.2.1 背景与先前工作

我们在第 1.1.1 节末尾解释的 BellQMA(2) 与 AM(2) 之间的紧密联系表明，应当将 BellQMA(2) 视为 AM(2)的一个“量子类比”。然而，另一个量子复杂性类同样有充分理由获得这一称号。这个复杂性类包含这样一类问题：由一位经典 验证者主持一场自由博弈，两位无界证明者可以共享纠缠，而该类中的问题均可由此判定。遵循 [AIM14]，，我们将这个复杂性类记为 $\mathsf{AM}^*(2)$。据我们所知，Aaronson、Impagliazzo 和 Moshkovitz 是最早定义这一复杂性类的人 [AIM14, 第 8]，节；他们将其相对于 AM(2) 的能力刻画留作一个开放问题。

研究经典多证明者类的“纠缠版本”的能力，有着悠久而富有成果的历史 [CHTW04, IV12, R UV13, FNT14, Ji17]，，最近还取得了一些令人惊讶且深刻的结果 [JNV+20]，并与纯数学建立了联系。目前尚不先验地清楚，允许双证明者之间存在纠缠，究竟会增强还是削弱验证者的判定能力。一方面，纠缠可能使证明者能够更有效地帮助验证者；但另一方面，也可能使他们能够更有效地作弊。这是一个熟悉的故事：在 $\mathsf{MIP}^*(2)$（MIP 的纠缠版本）及其变体的发展史中，我们已经多次遇到并解决了纠缠究竟有利还是有害这一问题。Ji、Natarajan、Vidick、Wright 和 Yuen 最近证明了 $\mathsf{MIP}^*(2) = \mathsf{RE}$ [JNV+20]，这清楚地表明，在普通的多参与者博弈模型中，允许纠缠会增强验证者的判定能力（从 NEXP 提升到 RE！）。另一方面，允许纠缠使任意给定的多证明者证明系统更强大，远非理所当然。例如，已知 MIP 的纠缠版本属于 EXP；MIP 是这样一种 MIP 版本：验证者的判定仅仅是两个证明者各自给出的一个比特答案的异或。尽管如此，$\oplus$MIP 本身等于 NEXP [Weh06]。我们只能从这些例子中得出结论：目前尚不先验地清楚 $\mathsf{AM}^*(2)$ 应当如何与 AM(2)建立关系。

1.2.2 我们关于 $\mathsf{AM}^*(2)$ 的结果

在这项工作中，我们解决了 Aaronson、Impagliazzo 和 Moshkovitz 提出的关于 $\mathsf{AM}^*(2)$ 能力的开放问题，证明了实际上，$\mathsf{AM}^*(2) = \mathsf{MIP}^*(2) = \mathsf{RE}$。换言之，量子自由博弈与一般量子多人游戏同样强大，尽管在经典世界中，自由游戏限制会显著降低验证者的判定能力！

我们注意到，在我们的工作之前，Brand˜ao 和 Harrow[BH13 所得到的 $\mathsf{AM}^*(k)$ 的最佳下界是 $\mathsf{NP} \subseteq \mathsf{AM}^*(\sqrt{N})$。具体而言，Brand˜ao 和 Harrow 证明存在一种

$\mathrm{AM}^*(\sqrt{N})$ 协议（类似于 [AIM14] $\mathrm{AM}(2)$ 协议），它有 $\sqrt{N}$ 个证明者，通信总量为 $O(\sqrt{N}\cdot\log N)$，并能以常数错误概率判定含有 N 个子句的 3SAT。我们的结果涵盖了这一结果：具体来说，我们证明存在一种 $\mathrm{MIP}^*(2)$ 协议，其问题大小为*constant*，答案长度以 $\mathrm{poly}\log(n)$ 的速度增长，并且能够以常数错误概率判定所有 RE，其中 n 是待判定问题实例的大小。由于常数大小问题的自由博弈等价于常数大小问题的一般博弈，我们由此得到一种通信效率极高的 $\mathrm{AM}^*(2)$ 协议来判定 RE。我们利用 Ji、Natarajan、Vidick、Wright 和 Yuen 开发的强大工具证明这一结果；2013 年 Brand˜ao 和 Harrow 尚无法使用这些工具。

量子自由博弈与经典自由博弈的关键区别在于，允许证明者共享纠缠后，便能运用自检文献中的工具；这使得 $\mathrm{AM}^*(2) = \mathrm{MIP}^*(2)$成为可能，尽管 $\mathrm{AM}(2)$ 与 MIP 的能力差异显著。借助这些工具，我们能够绕过本引言第一节中指出的“生日重复障碍”。具体而言，自检让我们只需较少的通信，就能迫使双证明者在进行纠缠博弈时进行内省，也就是自行生成（很长的）问题，因此无需发送非常长的问题，也能达到常数概率的自由碰撞。内省机制由 [NW19] 引入，用以证明 $\mathrm{MIP}^* \supseteq \mathrm{NEEXP}$；它也是压缩定理的核心，而这些定理最终导出了 $\mathrm{MIP}^* = \mathrm{RE}$。压缩定理是一种变换：它以某个问题和答案都很长、验证者复杂度也很高的多人博弈作为输入，输出一个问题和答案都更短（通常短了指数倍）、验证者复杂度也更低的新多人博弈，其博弈值与原始博弈大致相同；特别是，原始博弈的博弈值究竟是 $= 1$ 还是 $\leq 1/2$ 这一事实应当得到保留。纠缠博弈竟然也存在压缩定理，足以证明自检定理具有非凡的力量。具体而言，$\mathrm{MIP}^* = \mathrm{RE}$ 的证明是通过（某种意义上的）递归应用压缩定理得到的。

在这项工作中，我们将用于证明 $\mathrm{MIP}^* = \mathrm{RE}$ 的压缩定理“引导提升”，以证明 MIP^* 等于问题大小为常数的 MIP^*。具体而言，我们证明了一个称为超压缩定理（定理 54）的结果。该结果同样通过递归应用压缩定理得到，但方式与 $\mathrm{MIP}^* = \mathrm{RE}$ 证明中采用的方式略有不同。我们的超压缩定理以任意一个问题和答案长度均为多项式的 MIP^* 协议为起点，先应用一次一般压缩定理，将其转化为问题和答案长度均为多对数的协议；随后递归应用问题约简定理，在大致保持答案大小不变的同时，将问题大小降至常数。（这种递归应用过程的有效性取决于问题约简定理的结构——尤其是，我们无法以大致相同的方式缩减答案大小；原因在于，答案约简的有效性取决于原始博弈中验证者的运行时间，而问题约简则不然。）我们采用的问题约简过程与 [JNV$^+$20]中的方法相似，不过我们认为，若能结合 de la Salle [dlS22], 对问题约简分析所作的近期改进，便有望证明一个更好的问题约简定理，并以此作为迈向以下目标的垫脚石：构造一个面向递归可枚举语言（RE）的 MIP^* 协议，其问题大小为常数，答案大小为对数级（严格来说，或允许相差一个$O(\log^* n)$因子）。由于时间有限，我们将这一改进留待论文的未来版本再作探讨。我们将在第1.5节中更详细地讨论这一可能性。

为方便感兴趣的读者，关于这一结果有两点值得说明。

- 我们还证明了这一结果的无间隙版本（定理 47），即零间隙 MIP^* 等于具有常数规模问题和 $O(\log n\cdot\log^* n)$ 规模答案的零间隙 MIP^*。零间隙 MIP^* 与普通 MIP 相同，只不过对于否定实例，验证者的接受概率只要求严格小于 1，而不是 $\leq \frac{1}{2}$。为了得到 [JNV$^+$20] 的问题约简和答案约简定理的无间隙对应版本，我们参考了 [MNY20], ，该文证明了零间隙 MIP^* 等于 Π_2。

- 我们的无间隙超压缩定理的一个自然推论是，存在一种针对n 对 EPR 对的（非鲁棒）双验证者测试，只使用常数 大小的问题（以及$O(n)$ 大小的答案）。这一结果（定理 48）源于将无间隙超压缩定理应用于 [MNY20], 的“问题采样博弈”；该博弈可对n 对 EPR 对进行自检，因为超压缩也能保留纠缠界。（我们认为，在应用超压缩之前，先对问题采样博弈进行一轮无间隙答案约简，或许可以将$O(n)$大小的

答案缩减至 polylog(n)。）据我们所知，这是文献中首个能针对不断增长数量的 EPR 对实现自检、且问题大小为常数的非局域游戏[3]（见 [˜SB20，表 1]）。我们将获得有间隙情形下的类似结果留作一个开放问题；该结果将带来一种针对n 对 EPR 对、问题大小为常数的鲁棒 双验证者测试。更多讨论见第1.5节。

1.3 基于柯尔莫哥洛夫复杂度的 多证明者交互式证明* 协议下界

我们之前的结果表明，具有常数问题复杂度和多对数答案复杂度的多证明者交互式证明*，等于一般的多证明者交互式证明*（具有多项式问题、答案和判定复杂度）。（我们还证明，具有常数问题复杂度和近似对数答案复杂度的零间隙多证明者交互式证明*，等于一般的零间隙多证明者交互式证明*。）自然会问，我们沿这个方向还能推进多远。例如，具有常数大小问题和（真正的）$O(\log n)$ 大小答案的多证明者交互式证明*，是否等于一般的多证明者交互式证明*? 那么，具有常数大小问题以及例如 $O(\log\log n)$ 大小答案的多证明者交互式证明* 呢?

我们最后一组结果表明，通过使用超压缩（见本引言的上一节）所能达到的参数实际上几乎是紧确的。具体而言，我们证明（定理 64），任何能够判定所有递归可枚举语言的多证明者交互式证明* 协议——事实上，任何能够判定所有 EEXP 的多证明者交互式证明* 协议——都必须满足 $q(n) + a(n) \geq \frac{1}{2}\log n$，其中 n 是实例规模，而 q(n) 和 a(n) 分别是该协议中（针对单个证明者）的问题大小和答案大小。对于能够判定所有 EEXP 的无间隙多证明者交互式证明* 协议，问题大小和答案大小也满足相同的下界。特别地，后者表明，就问题复杂度和答案复杂度而言，我们实际上已经对零间隙多证明者交互式证明* 实现了紧确刻画： [MNY20] 展示了一个针对 Π_2 的零间隙多证明者交互式证明* 协议，其问题复杂度为 O(log n)、答案复杂度为 O(1)；而我们展示了一个针对 Π_2 的零间隙多证明者交互式证明* 协议，其问题复杂度为 O(1)、答案复杂度为 $O(\log n \cdot \log^* n)$；前者与下界仅相差常数因子，后者与下界仅相差 $O(\log^* n)$ 因子。在有间隙情形下，上界与下界之间仍存在一定的余地——特别是，下界满足 $q(n) + a(n) \geq \frac{1}{2}\log n$，但我们认为现有技术所能证明的最佳上界仅满足 $q(n) + a(n) = \text{poly}\log(n)$。我们认为可以收紧的是上界，并将弥合这一差距留作一个有趣的开放问题；解决该问题可能还会带来其他重要影响。（关于这一点的更多讨论，见我们的开放问题部分，即第1.5节。）

我们通过观察如下联系来证明这个下界：判定某个计算问题的多证明者交互式证明* 协议中问题和答案的大小，与确定性图灵机解决同一问题所需的辅助信息大小（或者等价地，解决同一问题的图灵机描述的大小）之间的联系。更具体地说，我们展示了一种转换方法：将任何判定语言L 的多证明者交互式证明*协议——其问题大小为$q(n)$、答案大小为$a(n)$，验证者的时间复杂度为$t(n)$ ——转换为一台运行时间大约为 $2^{t(n)}$ 、所需辅助信息长度大约为 $2^{2^{2(q(n)+a(n))}}$ 的确定性图灵机，该机器同样判定L。接着，我们指出，可以运用有时间限制的柯尔莫哥洛夫复杂度理论中的技巧，证明 EEXP 不能由任何运行时间为 $2^{\text{poly}(n)}$ 且使用 $\varepsilon 2^{cn}$ 辅助信息的图灵机判定，其中任意 $\varepsilon + c < 1$。[4] 结合这两个结论即可证明

[3]存在一些非局域关联，其问题大小为常数 [CGS17]，；事实上，也存在问题和答案大小均为常数的情形 [Fu22]，能够对任意高维的最大纠缠态进行自检。不过，这是一种不同的自检概念：它要求的不只是获胜概率接近最优，还要求给定问题时答案的整个分布接近目标分布。[4]有人可能会问，我们为什么必须证明这一点，也就是说，为什么不使用已知的大时间复杂度类的电路下界。答案是，我们从“转换”多证明者交互式证明* 协议中得到的图灵机，其辅助信息复杂度比同一图灵机的运行时间对 $q(n)+a(n)$ 更敏感，因此我们希望得到一个将运行时间与辅助信息分开处理的下界。具体而言，t(n)（多证明者交互式证明* 协议中验证者的时间复杂度）可以是 n 的任意多项式，例如 n^{100}，，而且可能并不显式依赖于 $q(n) + a(n)$（这里它可以是次对数的）。由于任何语言都可由大小为 2^n 的电路判定，而从我们的“转换”过程中得到的图灵机 M 的运行时间为$2^{t(n)}$，如果 t(n) 恰好是 n^{100}，，那么即使我们只计算那些用于编码 M 执行过程的图灵机配置表的门，M 的电路版本的复杂度也已经足够大，足以判定任何语言。因此，通过将 M 的电路版本与已知电路下界进行比较，我们无法对 $q(n)+a(n)$ 得出任何实质性结论。另一方面，由于图灵机 M 的辅助信息复杂度强烈依赖于 $q(n)+a(n)$，一个对辅助信息的依赖精确、而对时间复杂度的依赖较宽松的 RE（或 EEXP $\subseteq$ RE）下界，正好符合我们的需要。

我们所声称的下界，因为如果存在一个问题和答案都非常短、用于判定 RE 的多证明者交互式证明* 协议，就会得到一台判定 RE 的图灵机，而且它所需的辅助信息相对较少，这将与 EEXP 的下界相矛盾。

1.4 相关工作

我们已在第 1.1.1 节和第 1.2.1 节中讨论了与我们工作相关的大部分文献；本节我们将简要介绍一些尚未讨论的其他相关工作。

- Chiesa 和 Forbes [CF11] 讨论了若干与是否存在一种针对 NP、具有次线性通信的 BellQMA（2） 协议相关的问题，尤其还对 Chen-Drucker 协议 [CD10]进行了更精细的分析。最初对 Chen-Drucker 协议的分析仅得出了常数可靠性和 $1-\exp(-\sqrt{N})$ 完备性，适用于 $O(\sqrt{N})$ 个证明者的设置。Chiesa 和 Forbes 在证明者数量与完备性-可靠性间隙之间得到了平滑的权衡：具体而言，他们证明，使用 κ 个证明者执行 Chen-Drucker 协议时（每个证明者向验证者发送一个见证态，其长度为$O(\log N)$ 量子比特），其完备性

  只要 $\kappa=\Omega(\log N)$， $\Omega(\kappa^2 N^{-1})$ 的可靠性间隙便可达到。然而，Chiesa 和 Forbes 似乎没有考虑过类似我们这种协议：其中常数个（在我们的例子中为 2 个）证明者各自向验证者提供 $O(\sqrt{N})$ 个量子比特；并且两个见证态中的每一个（在诚实证明者的情况下），实际上都是该证明者在原始 Chen-Drucker 协议中会发送的状态的许多份拷贝，只不过这些拷贝被“打包”在一起，由单个证明者发送。

- Brand˜ao 和 Harrow [BH13] 还证明了许多其他结果，其中包括：在 $O(\sqrt{N})$ 个对称 BellQMA 证明者的设置下，Chen-Drucker 协议本质上是最优的。也就是说，他们证明，任何具有常数可靠性且通信量为 $O(n^{1/2-\varepsilon})$ 的 BellSymQMA($\sqrt{N}$) 协议（对任意 $\varepsilon>0$）都会与指数时间假设相矛盾；其中 BellSymQMA 是对 BellQMA 的进一步限制，要求每个证明者都必须向验证者发送相同的状态。他们的结果可以看作是 BellSymQMA($\sqrt{N}$) 设置下 [BCY10] 下界的类比。BellSymQMA($\sqrt{N}$)（通信量为 $O(\sqrt{N}\cdot\log N)$）能否通过 $O(\sqrt{N}\cdot\log N)$ 的通信量在 BellQMA(2) 中模拟，事先并不显然，因为更强的非纠缠保证或许对验证者有用；然而，反过来同样不明朗，因为原则上，BellQMA(2) 协议可能要求 Arthur 和 Lancelot 对各自独立的两个见证态进行任意测量，而这些测量可能跨越任何试图将这两个见证态划分为 $O(\sqrt{N})$ 个独立见证态的一系列切分产生纠缠。因此，BellQMA(2) 相对于 BellSymQMA($\sqrt{N}$) 的能力仍未得到理解。

  碰巧的是，我们针对 3SAT 的 BellQMA(2) 协议可以在 BellSymQMA($\sqrt{N}$)中模拟，因为要满足完备性，我们并不需要 Arthur 和 Lancelot 执行任何高度纠缠的测量。与此同时，从另一个角度来看，我们的结果也可以理解为一项证明：Chen-Drucker 协议中额外的不纠缠实际上并未赋予它多少额外能力。我们认为，这揭示了一种可能颇有趣的联系，因为我们的结果表明，要么 BellQMA(2) 与 BellQMA($\sqrt{N}$) 之间的不纠缠差异实际上并没有太大影响，要么我们尚未充分发挥其力量。

1.5 未解问题

1. **将 MA 或 AM 纳入 QMA(k) 并实现较低的通信复杂度**。目前，已有大量关于 NP 的 QMA(2) 协议研究，其通信复杂度为次线性。因此，一个自然的问题是：是否存在通信复杂度为次线性的 QMA(k) 协议（或 AM(k) 协议），用于处理 AM（或 MA）？这里的主要障碍在于，我们没有针对 MA 或 AM 的“PCP 定理”（如同我们对 NP 所拥有的那样），除非 MA NP（分别地，AM NP）；不过，将 NP 纳入 QMA**(2)** 且实现次线性通信复杂度的生日悖论技巧，核心依赖于拥有一个非常短的（就证明长度而言）针对 NP 的 PCP。

我们指出，关于 RE 的另一个下界对辅助信息有精确的依赖关系，但对时间复杂度的依赖关系较宽松：该下界指出，没有任何有限时间图灵机能够在使用少于 $\approx n$ 比特辅助信息的情况下解决停机问题。不过，这个下界“在另一个方向上又过于宽松”，也就是说，对辅助信息的下界非常弱，因为运行时间可以是任意有限值，因此可能远大于 $2^{\mathrm{poly}(n)}$。我们希望得到一个能够刻画运行时间与辅助信息之间权衡关系的下界，从而推导出 $q(n)+a(n)$ 的对数下界，因此我们证明了正文中陈述的下界。

不过，将 NP 纳入 QMA(2) 且实现次线性通信复杂度的生日悖论技巧，核心依赖于拥有一个非常短的（就证明长度而言）针对 NP 的 PCP。或者，我们能否证明：如果 MA（或 AM）属于通信复杂度为次线性的 QMA(k)，那么 MA $=$ NP（或 AM $=$ NP)?

2. **紧的有间隙**多证明者交互式证明* **协议，用于** RE。 正如我们在第1.3节中提到的，对于 EEXP 的任意多证明者交互式证明* 协议，其通信复杂度下界与我们相信通过将超压缩应用于用于 RE 的 [JNV+20]多证明者交互式证明* 协议所能达到的上界之间存在一定的余地。一种证明紧上界的方法，是证明存在对 NP具有纠缠可靠性的 *PCPP*——也就是说，证明 [NV18] 声称证明的那个结果，但其证明后来被发现存在漏洞。这样的结果将导出一个有间隙答案归约定理，其参数与我们在第4节中使用的无间隙答案归约定理（定理43）相近。我们认为，为了获得一个参数与我们在第4节中使用的无间隙问题归约定理（定理 42）相近的有间隙问题 归约定理，可以应用 de la Salle[dlS22]近期的结果。由于我们的超压缩定理能够利用 [MNY20] 的无间隙问题和答案归约定理，构造一个具有$O(1)$ 个问题和$O(\log n \cdot \log^* n)$ 个答案的零间隙多证明者交互式证明* 协议（用于 Π_2），因此我们相信，如果我们拥有同样强大的有间隙问题和答案归约定理，就能够在有间隙设置下构造一个具有相近参数的协议。

3. **一个**刚性**自检，用于**n **个EPR 对，且问题大小为常数**。本文中的技术只能给出一个界，限制任何一对通过我们所谓的“常数大小问题的 n 个 EPR 对自检”的证明者共享的希尔伯特空间的维度。是否存在一种针对 n 个 EPR 对的自检，其问题大小为常数（答案大小例如为多项式(n)），并能保证任何通过自检的双证明者所使用的策略，在局部等距变换意义下都等同于某个特定策略？这是文献中大多数 EPR 对自检都具有的一项非常强大且实用的性质，称为刚性。

4. **一个**稳健的**施密特秩测试**n**，问题大小为常数**。在本文中，我们能得到的纠缠界仅适用于无间隙情形（即针对完美策略）。我们能否证明，存在一个问题大小为常数的博弈，使得任何博弈值达到 $\geq 1/2$ 的策略，其施密特秩都至少为n？（施密特秩是非零施密特系数的数量，是一种相对宽松的纠缠刻画。） [JNV+20] 在其压缩定理中得到了这样的界，但由于一个有趣的技术原因，我们无法使用它：在本文中，为了对答案大小较大的游戏进行平行重复，我们必须采用 [DSV15], 的分析，而不是 [BVY17] 的分析。然而，这种分析无法保留纠缠界，因为将平行重复后的策略归约为单轮策略时，需要添加大量纠缠。关于这一点的更多细节，请参阅 [JNV+20 的讨论，11] 节。

5. **对** n **个 EPR 对的自检的通信下界**。 我们为 RE 的多证明者交互式证明* 协议得到的通信复杂度下界，几乎与我们通过超压缩达到的上界相匹配。正如我们在第 1.2.2 节中提到的，（无间隙）超压缩的另一个推论是：对n 个 EPR 对进行自检，问题规模为$O(1)$，答案规模为 polylog(n)（可能需要用到答案约简），但该自检并不具备鲁棒性。能否像我们为 RE 的多证明者交互式证明* 协议的通信复杂度所做的那样，利用计算论证给出对 n 个 EPR 对自检的通信复杂度下界？这并非显而易见，因为这种自检并不能直接解决任何我们熟知的计算问题。

6. **双证明者的无限随机性扩展**。超压缩为n 对 EPR 对提供了自检，所需问题的大小为常数。于是很自然会问：能否利用这一自检，仅用 2 个证明者实现无限随机性扩展 [CY13]？朴素的方法行不通，因为在 [MNY21] 的“问题采样博弈”和 [JNV+20] 的“内省博弈”中，每应用一次问题约简，证明者被问到会促使他们生成随机数的“内省”问题的概率（相对于那些用于检验他们彼此一致性的问题）就会减少一个常数因子，而我们需要应用

问题约简约 $\log^*(n)$ 次，才能使问题的大小为常数。能否克服这一障碍?

2 预备知识

2.1 概率基础

我们可以将有限样本空间 Ω 上的概率分布 $\mu\colon \Omega \to [0,1]$ 表示为长度为 $|\Omega|$ 的向量 $\vec{\mu}$，使得该向量的第 i个分量 $\vec{\mu}$ 恰好为 $\mu(i)$。对于样本空间 Ω 和 Ω'上的两个概率分布 μ、ν，我们用 $\mu \otimes \nu$ 表示样本空间 $\Omega \times \Omega'$ 上的概率分布，其向量表示为向量 $\vec{\mu} \otimes \vec{v}$。

2.2 量子信息基础

定义 2. 对于 $K \in \mathbb{N}$，量子傅里叶变换 $\mathcal{F}_K$ 是定义在 $\mathbb{C}^K$ 上的酉映射，其定义为

$$\mathcal{F}_K|s\rangle = \frac{1}{\sqrt{K}} \sum_{t=0}^{K-1} \omega_K^{s\cdot t}|t\rangle, \tag{2}$$

其中 ω_K = 指数$(2\pi i/K)$。该映射定义了由状态 $|\bar{s}\rangle = \mathcal{F}_K|s\rangle$ 组成的傅里叶基，其中 $s \in\{0,\ldots,K-1\}$。特别地，

$$|\bar{0}\rangle = \frac{1}{\sqrt{K}} \sum_t |t\rangle. \tag{3}$$

定义 3. 贝尔测量是在双部希尔伯特空间$\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$ 上的一种双结果测量 $\{M, \mathbf{1}-M\}$，它可以通过分别对 A 和 B 寄存器进行正算子值测度测量，然后对测量结果应用一个经典布尔函数来实现。换言之，存在作用于 $\mathcal{H}_A$ 上的正算子值测度 $\{A_a\}$，以及作用于 $\mathcal{H}_B$上的正算子值测度 $\{B_b\}$，还有一个布尔函数f，使得

$$M = \sum_{a,b:f(a,b)=1} A_a \otimes B_b.$$

2.3 柯尔莫哥洛夫复杂度

定义 4. 以下定义基于 *[HM95]* 中的定义 *2*。

固定一个通用模拟器 T（一个图灵机）。令 $K[f,g]$ 为 T 在长度为 f、运行时间为 g 的字符串上运行时能够生成的字符串集合。更正式地说，

$$K[f,g] = \{u\colon \exists w \ s.t.\ |w| \le f(|u|), T(w) = u，且此结果由\ T\ 在至多\ g(|u|)\ 步内得到\} \quad .$$

[HM95] 中的引理 *2.1*[表明，如果将 T 换成另一个通用模拟器，$K[f、g]$ 的博弈值变化不大，从而证明了使用固定通用模拟器是合理的。

2.4 非局域博弈与多证明者交互式证明* 协议

本节定义关于非局域游戏、策略和协议的基本概念。有关更详细的论述，请参阅 [MNY21] 和 [JNV+20]。

2.4.1 非局域博弈

以下定义摘自 [JNV+20]。

定义 5（双人单轮博弈）。一个双人单轮博弈 G 由一个元组（$\mathcal{X}$，$\mathcal{Y}$，$\mathcal{A}$，$\mathcal{B}$，μ，D）指定，其中

1. $\mathcal{X}$ 和 $\mathcal{Y}$ 是有限集（称为问题字母表），
2. $\mathcal{A}$ 和 $\mathcal{B}$ 是有限集（称为答案字母表），

3. μ 是关于 $\mathcal{X}\times\mathcal{Y}$ 的概率分布（称为问题分布），并且

4. D: $\mathcal{X}\times\mathcal{Y}\times\mathcal{A}\times\mathcal{B}\to\{0,1\}$ 是一个函数（称为判定谓词）。

定义 6（张量积策略）。对于博弈 $G=$（$\mathcal{X}$、$\mathcal{Y}$、$\mathcal{A}$、$\mathcal{B}$、μ、D），一个张量积策略 $\mathscr{S}$是一个元组（$|\psi\rangle$、A、B），其中

- $|\psi\rangle$ 是一个纯量子态，即有限维复希尔伯特空间$\mathcal{H}A$、 $\mathcal{H}B$中 $\mathcal{H}A\otimes\mathcal{H}B$ 的一个单位向量，

- A 是一个集合 $\{Ax\}$，使得对于每个 $x\in\mathcal{X}$，$Ax=\{Axa\}_{a\in\mathcal{A}}$是 $\mathcal{H}A$ 上的一个正算子值测度，并且

- B 是一个集合 $\{By\}$，使得对于每个 $y\in\mathcal{Y}$，$By=\{By\,b\}_{b\in\mathcal{B}}$ 是 $\mathcal{H}B$ 上的一个正算子值测度。

定义 7（张量积值）。关于博弈 $G=$（$\mathcal{X}$、$\mathcal{Y}$、$\mathcal{A}$、$\mathcal{B}$、μ、D），张量积策略 $\mathscr{S}=$（$|\psi\rangle$、A、B）的张量积值 定义为

$$\mathrm{val}^*(G,\mathscr{S})=\sum_{x,y,a,b}\mu(x,y)\,D(x,y,a,b)\,\langle\psi|A_a^x\otimes B_b^y\,|\psi\rangle\ .$$

对于 $\in[0,1]$，我们称策略 $\mathscr{S}$以概率 v 通过（或赢得）博弈G，当且仅当 $\mathrm{val}^*(G,\mathscr{S})\geq v$。$G$ 的张量积值定义为

$$\mathrm{val}^*(G)=\sup_{\mathscr{S}}\mathrm{val}^*(G,\mathscr{S})\ ,$$

其中，上确界取遍 G 的所有张量积策略 $\mathscr{S}$。

注 8。除非另有说明，本文中考虑的所有策略均为张量积策略，我们简称为策略。类似地，我们将$\mathrm{val}^*(G)$ 称为博弈 G 的博弈值或量子值。

定义 9。若博弈 $G=(\mathcal{X},\mathcal{Y},\mathcal{A},\mathcal{B},\mu,D)$ 满足以下条件，则称其为对称博弈：两个玩家的问题与答案字母表相同（即 $\mathcal{X}=\mathcal{Y}$和 $\mathcal{A}=\mathcal{B}$）；分布 μ 是对称的（即 $\mu(x,y)=\mu(y,x)$）；且判定谓词 D 对两个玩家一视同仁（即对所有 x,y,a,b，$D(x,y,a,b)=D(y,x,b,a)$）。

如果 $|\psi\rangle$ 是某个希尔伯特空间 $\mathcal{H}\otimes\mathcal{H}$中的一个（纯）状态，其中$\mathcal{H}$在两个因子的置换下保持不变，且两位玩家的测量算子相同，则称策略 $\mathscr{S}=(|\psi\rangle,A,B)$ 为对称策略。

我们常用一种紧凑的记号来表示对称博弈G 和对称策略 $\mathscr{S}$：记作$G=(\mathcal{X},\mathcal{A},\mu,D)$ 和 $\mathscr{S}=(|\psi\rangle,M)$，其中$M$ 表示两位玩家的测量算子集合。

定义 10. 如果对所有的 $x\in\mathcal{X}$以及满足 $a,b\in\mathcal{A}$且 $a\neq b$ 的情形，都有 $D(x,x,a,b)=0$，则称博弈 $G=(\mathcal{X},\mathcal{A},\mu,D)$ 为同步博弈。如果两位玩家共享一个最大纠缠态，且对于每个问题 x 和结果 a，*Alice* 和 *Bob* 的测量算子 A_a^x,B_a^x都是投影的，并满足 $B_a^x=(A_a^x)^T$，则称策略为有限维同步策略。

定义 11。对于具有值为1 的有限维策略的同步非局域博弈 G，纠缠界 $\mathcal{E}(G)$ 是实现值为1的同步策略的最小维度。

2.4.2 无间隙博弈族与$\mathsf{AM}_0^*(2)$ 协议

对于我们的无间隙结果，按照 [MNY21]，我们只给出同步值的界。我们并不认为这是一个重大限制，因为对于同步博弈而言，同步值保留了纠缠值的所有定性特征，同时在技术上更易于处理。众所周知，在有间隙情形下，对于同步博弈，同步值接近量子值 [Vid22]。

粗略地说，如果对于语言中的每个实例 x，对应博弈的纠缠值为 1，而对于任何不属于该语言的实例，对应博弈的博弈值小于 1，那么该语言就具有零间隙多证明者交互式证明*。对于任意具有问题分布 μ 的非局域游戏 G，只要将问题分布改为任何与 μ 具有相同支撑集的分布 μ'，博弈值为 1 这一性质就会保持不变。

因此，遵循 [MNY21]，，我们用两台图灵机来定义零间隙协议：一个判定器 D，给定一对问题和答案，判定是否赢得了博弈；以及一个检查器 C，给定一对问题，判定它们是否属于分布 μ 的支撑集。为了强调问题分布在此处无关紧要，并与有间隙情形建立联系，我们将这一类称为 AM_0^*（2）。为定义它，我们先用判定器和检查器来形式化游戏规格。

定义 *12.* 给定一个自然数 q 以及一对图灵机 D、C，其中 D 接受输入 x、y、a、b，C 接受输入 x、y。假设对于任意 x、y，D 和 C 总能停机，并且对于某个有限的 m，当输入 x、y 时，D 读取的 a、b 不超过 m 个比特。那么，与之关联的非局域游戏，即由 q 和 (D, C) 给出的博弈，定义为 $(\mathcal{X} = \{0,1\}^q, \mathcal{A} = \{0,1\}^m, \mu, D')$，其中 μ 是 $\mathcal{X} \times \mathcal{X}$ 上的均匀分布；对于输入 x、y、a、b，D'：*(1)* 首先运行检查器 $C(x, y)$，如果检查器拒绝，则自动接受（即声明 x、y 不是有效问题对）；*(2)* 然后运行 $D(x, y, a, b)$，如果其接受则接受，否则拒绝。

对于本文讨论的所有对 D,C，m 的存在性都是显而易见的，因此我们不证明m 存在。

为了讨论压缩定理，定义由自然数n索引的非局域游戏族很有用。

定义 *13.* 零间隙游戏族由图灵机三元组 (D, C, Q) 指定，其中 D 的输入为 (n, x, y, a, b)，C 的输入为 (n, x, y)，Q 的输入为 n。输入 n 称为索引。对于索引 n，相应的博弈由 $Q(n)$ 和 $(D(n, \cdot, \cdot, \cdot, \cdot), C(n, \cdot, \cdot))$ 指定。如果 Q 在输入 n 上的输出长度不超过 $q(n)$，则称该游戏族的问题长度为 $q(n)$；如果 D 在输入 n 时读取的答案 a、b 的比特数不超过 $a(n)$，则称答案长度为 $a(n)$；如果 D 和 C 在输入 n 上分别于相应的运行时间内运行，则称判定器运行时间为 $t_d(n)$，检查器运行时间为 $t_c(n)$。

定义 14. 一个$\mathrm{AM}_0^*(2)$ 协议是一个由图灵机组成的三元组(D,C,Q)，满足

- D 接收输入 z,x,y,a,b，并在关于 $|z|$ 的多项式时间内运行 .
- C 接收输入 z,x,y，并在关于 $|z|$ 的多项式时间内运行。
- Q 接收输入 z，并在关于 $|z|$ 的多项式时间内运行。

如果对于任意 z，协议(D,C,Q) 所指定的语言 L 都能被判定，则称该协议判定语言 L：

- 完备性： 如果 $z \in L$，那么由 $Q(z)$ 给出的非局域游戏 Gz，以及$(D(z,\cdot,\cdot,\cdot,\cdot),C(z,\cdot,\cdot))$ 的博弈值为ω $q(Gz) = 1$。
- 可靠性： 如果 $z \notin L$，则由 $Q(z)$ 和 $(D(z,\cdot,\cdot,\cdot,\cdot),C(z,\cdot,\cdot))$ 给出的非局域游戏 Gz 的博弈值为ω $q(Gz) < 1$。

定义 13 和 14 并不完全兼容，因为前者中的图灵机将索引n 作为输入，而后者中的图灵机将任意字符串z作为输入。我们通过定义n-索引的 $\mathrm{AM}_0^*(2)$ 协议来弥合这一差距。事实证明，我们构造的所有$\mathrm{AM}_0^*(2)$协议都将是n-索引协议。

定义 15。 一个 n-索引的$\mathrm{AM}_0^*(2)[q(\cdot),\ a(\cdot),\ t_d(\cdot),\ t_c(\cdot)]$ 协议是一对图灵机 $GenG$，N，使得

- $GenG$ 以 z 作为输入，并在多项式时间内输出一个由三元组 Dz，Cz、Qz 指定的非局域博弈族的描述。它们分别期望接收以下形式的输入：n，x，y，a，b，以及 n，x，y。
- N 以 z 为输入，并在多项式时间内输出一个自然数 n，满足 $n = \mathrm{poly}(|z|)$。
- $Dz(N(z),x,y,a,b)$ 读取 x,y 中至多 $q(|z|)$ 比特，以及 a,b 中至多 $a(|z|)$ 比特，并且运行时间至多为 $td(|z|)$。
- $Cz(N(z),x,y)$ 读取 x,y 中至多 $q(|z|)$ 比特，并且运行时间至多为 $tc(|z|)$。
- $Qz(N(z))$的输出最多为 $q(|z|)$，运行时间最多为多项式$(|z|)$。

默认情况下，如果提及$\mathsf{AM}_0^*(2)$而未指定 q, a, t_d, t_c，我们便假设它们是多项式函数。若对于任意 z，D, C 指定的协议都能判定语言 L，则称该协议判定语言 L。

- 完备性：若 $z \in L$，则由 $Qz(N(z))$ 和 $(Dz(N(z), \cdot, \cdot, \cdot, \cdot), Cz(N(z), \cdot, \cdot))$定义的非局域游戏 G 的博弈值为 $\omega sq(Gz) = 1$。
- 可靠性：若 $z \notin L$，则由 $Qz(N(z))$和 $(Dz(N(z), \cdot, \cdot, \cdot, \cdot), Cz(N(z), \cdot, \cdot))$给出的非局域游戏 G 的博弈值为 $\omega sq(Gz) < 1$。

我们注意到，如果存在一个n-索引 $\mathsf{AM}_0^*(2)$ 协议来判定语言L，那么也存在一个$\mathsf{AM}_0^*(2)$ 协议来判定L。

2.4.3 有间隙的游戏族和多证明者交互式证明*(2) 协议

接下来，我们讨论有间隙情形。在这种情形下，问题的分布确实会产生影响，因此我们采用 [JNV+20] 的形式化方法。他们将多证明者交互式证明* 协议定义为一对图灵机：一个采样器，以随机种子作为输入，为两名玩家生成一对问题；以及一个判定器，根据一对问题和答案判定他们是否赢得了博弈。在有间隙情形下，已知的压缩定理对采样器的形式施加了严格条件，因此有关定义请参阅 [JNV+20 的第 5] 节。

对于以n为索引的有间隙游戏族，或对于一个多证明者交互式证明* 协议，我们可以讨论问题长度和答案长度$q(n)$、$a(n)$，以及采样器 和判定器的运行时间$t_S(n)$、$t_d(n)$。我们以与无间隙情形类似的方式定义这些量，但有一个重要区别：我们要求$q(n)$ 既是问题长度的上界，也是采样器可以读取的其输入中的比特数 的上界（非正式地说，即采样器可以用来生成问题的随机比特数）。在检查器形式化中，问题长度与检查器读取的比特数相同；而在采样器形式化中，两者可能不同。为简化记号，我们使用$q(n)$ 作为这两个量的上界。

[JNV+20] 的压缩结果仅适用于带有标准形式采样器的博弈：该文将其定义为使用特定类型的映射（“条件线性函数”）作用于输入随机种子来生成问题对的采样器。此处我们不需要了解该定义的细节。不过，其中有一点会派上用场：标准形式采样器的定义包含这样的功能：在给定一个特殊输入值时，返回$q(n)$的值。这意味着我们不再需要单独使用图灵机Q 来计算它；可以将该功能并入采样器S的定义中。利用这一点，我们现在可以用采样器和判定器来定义间隙游戏族。

定义 16。 间隙游戏族 由一对图灵机(S,D) 指定，其中(S,D)构成 *[JNV+20 第5节中定义的标准形验证器 4]*。更具体地说，S 和 D 的形式如下：

1. S 接受一个自然数 n 和另一个参数采样器参数作为输入。[5] 对于输入 n，S 最多读取（n）比特采样器参数，运行时间至多为 t_S（n）。此外，如果采样器参数 = 维度，则 S 对输入（n，维度）的输出为 q（n）。*2.* D 接受一个自然数 n 和一个元组（x，y，a，b）作为输入。D 最多读取 x，y 的 q（n）比特，以及 a，b 的 a（n）比特，运行时间至多为 t_d（n）。

输入 n 称为索引。我们称游戏族（S，D）具有问题长度q（n）、答案长度a（n）、采样器运行时间t_S（n），以及判定器运行时间t_d（n）。

有间隙游戏族中的第n个非局域游戏 关于游戏族中的第 n 个非局域游戏 (S,D)的精确定义，请参阅 [JNV+20，第 5] 节。概括而言，游戏G_n中与由$G = (S,D)$ 指定的游戏族中的第n个游戏相对应的验证者会执行以下步骤：(1) 将采样器参数设为维度，并在$(n$、维度$)$ 上运行S，以计算问题大小$q(n)$；(2) 在长度为$q(n)$ 的随机种子上运行S，计算一对要发送给

[5]由于其他参数较为复杂，我们将传递给S 的其他参数抽象为采样器参数。更多详情请参见 [JNV+20，第4节2]。

证明者的问题；(3) 在问题和证明者的答案上运行D，以判定他们是否赢得了博弈。

现在，我们依照 [JNV+20] 定义一般的（双玩家、单轮）多证明者交互式证明*（2）协议。请注意，在下述定义中，与定义 16 不同，我们不要求S、D 构成标准形验证器。

定义 17。语言 L 属于多证明者交互式证明* 当且仅当存在两台概率图灵机 S 和 D，满足以下性质。

1. 效率：对于每个 $z \in \{0,1\}^*$，都存在一个博弈 $G^z = (\mathcal{X}, \mathcal{Y}, \mathcal{A}, \mathcal{B}, \mu, D)$，使得：

（a）图灵机 S 在输入 z 时，运行时间为poly（$|z|$），并返回一对（x, y）$\in \mathcal{X} \times \mathcal{Y}$，使得在 S 的随机选择下，（x, y）的分布为 μ。（b）图灵机 D 的输入为 z 和一个元组（x, y, a, b）$\in \mathcal{X} \times \mathcal{Y} \times \mathcal{A} \times \mathcal{B}$，运行时间为poly（$|z|$），并返回 D（x, y, a, b）。[6]

2. 完备性：若 $z \in L$，则$\mathrm{val}^*(G^z) \geq 2/3$

3. 可靠性：若 $z \notin L$，则$\mathrm{val}^*(G^z) \leq 1/3$。

我们称这一对(S, D) 构成语言 L 的一个多证明者交互式证明* 协议 。

定义 16 和 17 再次并不完全兼容：前者规定采样器必须是标准形式，并以索引n为输入；后者不要求采样器是标准形式，并以字符串z为输入。下面给出的n 索引多证明者交互式证明*(2) 协议弥合了这一差异。事实证明，我们构造的所有多证明者交互式证明*(2) 协议都是n索引协议。

定义 18。一个 n 索引多证明者交互式证明*(2)$[q(\cdot), a(\cdot), t_S(\cdot), t_d(\cdot)]$ 协议是一对图灵机 $GenG$，N，使得

- $GenG$ 以 z 为输入，并在多项式时间内输出由采样器—判定器对 Sz,Dz 指定的非局域博弈族的描述，该对构成一个标准形验证器 *[JNV+20，第4节.2]*。
- N 以 z 为输入，并在多项式时间内输出一个自然数 n，其中 n = 多项式$(|z|)$。
- 对于任意 z，Sz 以自然数 n 和另一个参数采样器参数为输入。当 $n = N(z)$时，Sz 至多读取采样器参数 的 $q(|z|)$ 比特，且运行时间至多为 $ts(|z|)$。此外，如果采样器参数 = 维度，S 在输入$(N(z),$维度$)$ 时输出 $q(|z|)$。
- 对于任意 z，Dz 以自然数 n 和元组(x,y,a,b)为输入。当 $n = N(z)$时，Dz 至多读取 x,y 的 $q(|z|)$ 比特，以及 a,b 的 $a(|z|)$ 比特，且运行时间至多为 $td(|z|)$。

默认情况下，提到多证明者交互式证明* 而未指定 q、a、t_S、t_d 时，我们假设它们是多项式函数。如果对任意 z，S、D 所指定的协议都能判定语言 L，那么我们称该协议判定 L：

- 完备性：如果 $z \in L$，那么游戏族 $Gz = (Sz、Dz)$中的第 $N(z)$个非局域游戏（记作 $GzN(z)$）的博弈值为 $\omega q(GzN(z)) = 1$。
- 可靠性：如果 $z \notin L$，那么游戏族 $Gz = (Sz、Dz)$中的第 $N(z)$个非局域游戏（记作 $GzN(z)$）的博弈值为 $\omega q(GzN(z)) \leq 1/2$。

我们指出，如果存在一个由n索引的 MIP*(2) 协议来判定语言L，那么也存在一个 MIP*(2)协议来判定语言L。

[6]请注意，即使输入 a、b 很长，D 的运行时间也应为 poly$(|z|)$。可以通过让D 在x、y、a、b 相对于 $|z|$过长时返回 0 来保证这一点。

2.4.4 无间隙与有间隙定义之间的关系

读者会注意到，在无间隙情形中，我们定义的交互式证明类称为 $\mathrm{AM}_0^*(2)$；而在有间隙情形中，我们定义的类称为 MIP^*。这种差异（使用“AM(2)”而非“MIP”）的原因在于：自由博弈表述——其中验证者是通过检查器和判定器而非采样器和判定器来定义的——在无间隙情形中不失一般性，但在有间隙情形中并非如此。事实上，在无间隙情形中，可以按照与 MIP^* 相同的方式（即通过采样器和判定器）定义一个类 MIP_0^*，只是将可靠性间隙设为 0。显然，$\mathrm{AM}_0^*(2) \subseteq \mathrm{MIP}_0^*$；这是因为，给定一个检查器，可以定义一个等价的采样器，它根据随机种子生成一对均匀随机的问题(x,y)，对其运行检查器；如果检查器未通过，则改为输出一个“中止”问题对$(\perp,\perp)$。类似地，$\mathrm{MIP}_0^* \subseteq \mathrm{AM}_0^*(2)$：在零间隙情形中，不失判定能力，我们可以假设问题分布是均匀且自由的，因为任何定义在有限集 $\mathcal{S} \subseteq \mathcal{X} \times \mathcal{Y}$ 上的非均匀相关问题分布，都可以替换为一个自由问题分布，该分布仅仅是在 $\mathcal{X} \times \mathcal{Y}$ 上均匀分布；而我们仍会以非零概率“命中”证明者无法通过的问题对。在关于非一致复杂度界的章节中，我们将给出 MIP_0^* 的下界，因而这也将推出两者 MIP^* 和 $\mathrm{AM}_0^*(2)$ 的界。

在有间隙情形下，自由博弈通常不如一般博弈强大——问题长度为常数这一特殊情形除外。具体而言，使用我们在第2.4.2节定义 $\mathrm{AM}_0^*(2)$ 时采用的判定器-检查器形式体系，定义一个有间隙类 $\mathrm{AM}^*(2)$，但完备性-可靠性差距为常数。若问题大小为常数，则显然有 $\mathrm{MIP}^*[\mathrm{q(n)} = \mathrm{O(1)}] \subseteq \mathrm{AM}^*(2)[\mathrm{q(n)} = \mathrm{O(1)}]$；这是因为检查器可以对所有可能的种子（数量为常数）运行 MIP^* 采样器，并高效生成所有有效问题对的列表。最终，我们将在第5节展示一个针对 RE 的协议，其属于 $\mathrm{MIP}^*[\mathrm{q(n)} = \mathrm{O(1)}]$，从而推出一个针对 RE 的 $\mathrm{AM}^*(2)[\mathrm{q(n)} = \mathrm{O(1)}]$协议。

2.5 $\mathrm{QMA}(2)$ 及相关类别

关于这一类别的更全面论述，请参阅 [HM13]。

定义 19. $\mathrm{QMA}(2)$ 是这样一类量子 *Merlin-Arthur* 证明系统：*Arthur* 是一台多项式时间量子机器，并从 *Merlin* 收到一个见证 $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$，且保证该见证在固定划分下为张量积。若对于任意输入 $x \in L$，都存在一个见证态 $|\psi_1\rangle \otimes |\psi_2\rangle$ 使 *Arthur* 以至少 c 的概率接受（即完备性概率）；并且对于任意输入 $x \notin L$，不存在任何张量积形式的见证态能使 *Arthur* 以大于 s 的概率接受（即可靠性概率），则称一个$\mathrm{QMA}(2)$ 协议判定语言 L；除非另有说明，我们假设 $c = 2/3$ 且 $s = 1/3$。

定义 20. $\mathrm{BellQMA}(2)$ 是这样一类$\mathrm{QMA}(2)$ 证明系统：验证者对应于接受测量结果的 *POVM* 元素是贝尔测量（见定义 *3*）。

3 针对3SAT的$\mathrm{BellQMA}(2)$ 协议

3.1 协议

定义 21 (广义 K-着色)。 设 $K \in \mathbb{N}$，$\mathcal{G} = (V,E)$ 为一个图，并设 $R : E \times [K] \times [K] \to \{0,1\}$ 为一个函数。若存在赋值函数 $c : V \to [K]$，使得对于所有边 $e = (v_1,v_2) \in E$，$R(e,c(v_1),c(v_2)) = 1$，则称 $\mathcal{G}$ 关于 R 是广义 K-可着色的。

定义 22 (δ-GAP-KCOL)。 *δ-GAP-KCOL* 是一个承诺问题。*δ-GAP-KCOL* 的一个实例由一个图 $\mathcal{G} = (V,E)$、一个数 $K \in \mathbb{N}$以及一个函数 $R : E \times [K] \times [K] \to \{0,1\}$组成。

- $(\mathcal{G},K,R)$ 是 *δ-GAP-KCOL* 的一个 *YES*实例，当且仅当 $\mathcal{G}$ 关于 R 是广义 K-可着色的。
- （$\mathcal{G}$，K，R）是一个 *δ-GAP-KCOL NO*实例，当且仅当对于所有可能的赋值 c：$V \to [K]$,，至少存在$\delta|E|$ 条边 $e \in E$，使得 R（e，c（v_1），c（v_2））$= 0$。

定理 23。 存在一个归约 f：$\{0,1\}^* \to \{0,1\}^*$ 从*3SAT*到 *δ-GAP-KCOL*，其中常数为 $\delta > 0$，且常数 K 为 > 0，使得当 x 是一个 N子句*3SAT*实例时，$f(x)$ 是 *δ-GAP-KCOL* 的一个实例$(\mathcal{G}$，K，$R)$，满足 $|V| = O(N \cdot \mathrm{poly}\log N)$ 以及 $|E| = O(N \cdot \mathrm{polylog}\, N)$。

证明。 参见 [CD10]的定理 2。 □

现在我们给出一个用于 δ-GAP-KCOL 的 BellQMA(2) 协议。该协议依赖两个子测试：均匀性测试（图 2）和一致性测试（图 3）。我们将该协议中的验证者称为 Arthur，将双证明者称为 Alice 和 Bob。

固定一个 δ-GAP-KCOL 实例 ($\mathcal{G}$ = (V, E), K, R)。输入：令 n = |V|，m = |E|。协议中的所有参与方都将实例 ($\mathcal{G}$ = (V, E), K, R) 作为输入，同时还接收一个整数 k = O($\sqrt{n}$)，以及一个用于均匀性测试（图 2）的常数 $0 < \eta < 1$。诚实的证明者还会收到 $\mathcal{G}$ 的一个广义K-着色作为输入，该着色由函数 c : V $\to$ [K] 描述。协议如下：

1. Alice 和 Bob 都向 Arthur 发送一个状态；Alice 的状态长度为 $k(\log m + 2\log K)$ 个量子比特，Bob 的状态长度为 $k(\log n + \log K)$ 个量子比特。令他们发送的状态分别为 $|\psi_1\rangle$ 和 $|\psi_2\rangle$。诚实的证明者发送以下状态

$$|\psi_1\rangle = \left(\frac{1}{\sqrt{m}} \sum_{e=(v_1,v_2)\in E} |e\rangle|c(v_1), c(v_2)\rangle\right)^{\otimes k}$$

$$|\psi_2\rangle = \left(\frac{1}{\sqrt{n}} \sum_{v\in V} |v\rangle|c(v)\rangle\right)^{\otimes k}.$$

2. Arthur 抛掷一枚硬币。如果结果为正面，他就对 $|\psi_1\rangle$和 $|\psi_2\rangle$执行均匀性测试（图 2），并将 η 设为作为输入提供给他的 η 选项。均匀性测试还需要两个自然数参数，K' 和 Q。对于在 $|\psi_1\rangle$上进行的均匀性测试，他设定

$$K' = K^2, Q = m,$$

对于在 $|\psi_2\rangle$上进行的均匀性测试，他设定

$$K' = K, Q = n.$$

如果结果为反面，Arthur 就对 $|\psi_1\rangle \otimes |\psi_2\rangle$执行一致性测试（图 3），并将 $\mathcal{G}$、K、R 设为作为输入提供给他的选项。

图 1： 针对 δ-GAP-KCOL 的 BellQMA(2)协议。

引理 24(完备性)。 如果 $\mathcal{G}$ 关于 R 是广义 K-可着色的，那么图 *1* 所述的诚实策略被接受的概率为 $1 - \exp(-\Omega(\sqrt{n}))$。

证明。 当 $\mathcal{G}$ 是广义K-可着色的，且双证明者诚实时，一致性测试以概率 1 接受。根据 [CD10 第 3 节的分析，诚实的证明者执行时，针对 $|\psi_1\rangle$ 的均匀性测试和针对 $|\psi_2\rangle$ 的均匀性测试各自以概率 $1 - \exp(-\Omega(\sqrt{n}))$ 通过。由并合界即可得到所需结论。 □

在接下来的章节中，我们分析该协议的可靠性。

3.2 均匀性测试的可靠性

为便于说明，我们先对均匀性测试进行零误差分析。在引理 26 的证明中，我们将展示下文给出的论证如何推广到存在非零误差的情形。

引理 25。 假设 $|\psi\rangle$ 以确定无疑的方式通过均匀性测试。那么存在一个由 $\mathcal{S}$ 个 $[k]$ 的子集构成的集合，使得，

1. 对所有 $T \in \mathcal{S}$，都有 $|T| \geq k K'$（1 − η），并且

输入：两个数 K'、$Q \in \mathbb{N}$，另一个数 $0 < \eta < 1$，以及一个状态 $|\psi\rangle_{Q_1A_1\ldots Q_kA_k}$，作用于寄存器 $Q_1A_1 \ldots Q_kA_k$。寄存器 Q_i 称为问题寄存器，寄存器 A_i 称为答案寄存器。1. 对每个答案寄存器执行傅里叶变换 $\mathcal{F}_{K'}$，然后在标准基下对其进行测量。2. 令 $Z = \{i$ 表示答案寄存器 A_i 测量得到 $0\}$ 的结果。如果 $|Z| < (1-\eta)\, K'$，则拒绝；否则继续。3. 对步骤1中测量结果为 0 的每个答案寄存器 A_i，对第 i 个问题寄存器 Q_i 执行傅里叶变换 $\mathcal{F}_Q$，并在标准基下进行测量。如果此步骤中得到任何非零测量结果，则拒绝。否则接受。^{1} η 是必要的，因为即使诚实的 Merlin 也不总能通过均匀性测试；相反，他们只能使 $|Z| = k$ K' 的平均值达到 $|$，因此 η 是必要的，这样才能应用切尔诺夫界并达到 $1 - \exp(-k)$ 的完备性。更多详情请参见 [CD10，第 3 节。1]

图 2： 均匀性测试。

输入：

- 一个状态 $|\psi\rangle_{Q_1A_1\ldots Q_kA_k} \otimes |\psi'\rangle_{Q'_1A'_1\ldots Q'_\ell A'_\ell}$ 位于寄存器 $Q1A1 \ldots Q_kA_kQ'_1A'_1 \ldots Q'_\ell A'_\ell$ 上。寄存器 Q_i 和 Q'_j（$i \in [k], j \in [\ell]$）称为问题 寄存器，而寄存器 A_i 和 A'_j 称为答案 寄存器。

- 一个图 $\mathcal{G} = (V, E)$。

- 一个数值 $K \in \mathbb{N}$。

- 一个关系 $R : [K] \times [K] \to \{0,1\}$。1. 在标准基下测量所有寄存器。将寄存器 Qi（$i \in [k]$,）中的每个测量结果解释为向 Alice 提出的问题，并将相应答案寄存器 Ai 中的测量结果解释为她对该问题的答案。（因此，Alice 会收到 k 个问题，并逐一作答。）将寄存器 Q′j（$j \in [\ell]$）中的每个测量结果解释为向 Bob 提出的问题，并将相应答案寄存器 A′j 中的测量结果解释为他对该问题的答案。2. 将 Alice 的每个问题解释为一条边 $e \in E$，并将相应的 Alice 答案解释为 $[K]$ 中的一对颜色，分别对应构成 e 端点的顶点。将 Bob 的每个问题解释为一个顶点 $v \in V$，并将相应的 Bob 答案解释为 v 在 $[K]$ 中的一种颜色。令 $A \subseteq E$ 为 Alice 的问题所得到的所有边的集合，$B \subseteq V$ 为 Bob 的问题所得到的所有顶点的集合。3. 对于每条边 $e \in A$ 和每个满足 $v \in e$ 的顶点 $v \in B$，检查 Alice 和 Bob 的着色是否一致，并检查 e 的两个端点所对应的颜色是否满足函数 $R(e, \cdot, \cdot)$。

图 3： 一致性测试。

2. 对 $|\psi\rangle$ 的问题寄存器在标准基下进行测量所得到的分布 μ_Q，可以分解为一个混合分布

$$\mu_Q = \sum_{T\in\mathcal{S}} p(T)\mu_T^{unif} \otimes \mu_{\overline{T}}^{junk},$$

其中 p：$\mathcal{S} \to [0,1]$ 是在 $\mathcal{S}$ 上的一个分布，$\mu^{unif}T$ 是在 T 中索引上的 $[Q]^{|T|}$ 均匀分布，而 $\mu^{junk}_{\overline{T}}$ T 是在 $[k]-T$ 中索引上的任意分布。

证明。假设我们对 $|\psi\rangle$ 执行均匀性测试（图 2）的步骤1，即在傅里叶基下测量 $|\psi\rangle$ 的所有答案寄存器。令 $\rho_{\vec{r}}$ 表示该测量后、条件为测量结果为 $\vec{r}$时的测量后状态。假设 $|\psi\rangle$ 以确定概率通过均匀性测试，则 $\vec{r} = r_1, \ldots\ldots, r_k$ 必定满足 $r_i = 0\ \forall i \in T$，其中 T 是某个子集 $T \subset [k]$，且 $|T| \geq kK'(1-\eta)$。此外，$\rho_{\vec{r}}$ 现在通过均匀性测试步骤3的概率仍然为 1。因此，

$$\rho_{\vec{r}} = (|\bar{0}\rangle\langle\bar{0}|)^{\otimes T} \otimes \rho_{\overline{T}},$$

其中，记号 $(|\bar{0}\rangle\langle\bar{0}|)^{\otimes T}$ 表示索引属于 T 的寄存器处于傅里叶基中的全零态，并与其他寄存器构成张量积。

因此，在标准基中测量 $\rho_{\vec{r}}$，会使寄存器 T 上的结果均匀随机且独立同分布，而其他寄存器上的结果则服从某个任意分布。

最后，为了得到该引理，注意到（令 ρ 表示步骤1中不加条件地进行傅里叶测量后的测量后状态）

$$\rho = \sum_{\vec{r}} q_{\vec{r}}\,\rho_{\vec{r}},$$

对于某个分布 $q_{\vec{r}}$。因此，结论得证。 □

现在我们转向本节的主要技术引理，它是引理 25 的一个允许常数误差的版本。

引理 26。假设 $|\psi\rangle$ 以概率 $1-\varepsilon > 0$通过均匀性测试。那么存在一个由 $[k]$ 的子集构成的集合 $\mathcal{S}$，使得，

1. 对所有 $T \in \mathcal{S}$，均有 $|T| \geq kK'(1-\eta)$，并且

2. 在标准基下测量 $|\psi\rangle$ 的问题寄存器后得到的分布 μ_Q 可以分解为如下混合分布

$$\mu_Q \simeq_{\delta(\varepsilon)} \sum_{T\in\mathcal{S}} p(T)\mu_T^{unif} \otimes \mu_{\overline{T}}^{junk},$$

其中

(a) p：$\mathcal{S} \to [0,1]$ 是 $\mathcal{S}$ 上的一个分布；*(b)* $\mu^{unif}T$ 是在 T 中索引上的 $[Q]^{|T|}$ 均匀分布；*(c)* $\mu^{junk}_{\overline{T}}$ T 是 $[k]-T$ 中索引上的任意分布；*(d)* 记号 $\simeq_\delta$ 表示两边之间的总变差距离为 δ；*(e)* $\delta(\varepsilon) = O(\varepsilon^{1/4})$。

证明。假设我们对 $|\psi\rangle$ 执行均匀性测试（图 2）的第一步，即在傅里叶基下测量 $|\psi\rangle$ 的所有答案寄存器。令 $\rho_{\vec{r}}$ 表示在测量结果为 $\vec{r}$ 的条件下测量后的状态，令 ρ 表示不以任何特定结果为条件时该测量后的总体状态。令 $q_{\vec{r}}$ 表示获得任意给定结果 $\vec{r}$ 的概率。

设 $p_{success,\vec{r}}$ 是一个将密度矩阵映射到 $[0,1]$ 的函数，使得 $p_{success,\vec{r}}(\sigma)$ 给出给定混合态 σ 在均匀性测试的步骤3中接受测试时的概率，并且 $\vec{r}$ 是均匀性测试的步骤1中得到的结果。设 $\mathbf{1}_{\vec{r}}$ 是一个指示函数，用于指示给定向量 $\vec{r}$ 是否通过均匀性测试的步骤2（即，是否 $\vec{r}$ 满足

存在$T \subseteq [k]$，使得 $|T| \geq k\,K'(1-\eta)$，且$r_i = 0\,\forall i \in T$）。使用这一记号，$|\psi\rangle$ 通过均匀性测试的概率可以表示为

$$\sum_{\vec{r}} q_{\vec{r}} \cdot \mathbf{1}_{\vec{r}} \cdot p_{success,\vec{r}}(\rho_{\vec{r}}) \geq 1-\varepsilon.$$

改写为

$$\sum_{\vec{r}} q_{\vec{r}} (1 - \mathbf{1}_{\vec{r}} \cdot p_{success,\vec{r}}(\rho_{\vec{r}})) \leq \varepsilon.$$

因此（利用马尔可夫界），以至少 $1-\frac{1}{\alpha}$ 的概率，步骤1中得到的 $\vec{r}$ 满足

$$(1 - \mathbf{1}_{\vec{r}} \cdot p_{success}(\rho_{\vec{r}})) \leq \alpha\varepsilon. \tag{4}$$

令 $\alpha = \frac{1}{\sqrt{\varepsilon}}$，并将任意这样的 $\vec{r}$ 定义为良好。根据 α 的定义，$\vec{r}$ 以至少 $1-\sqrt{\varepsilon}$ 的概率是良好的。注意，对于任意良好的 $\vec{r}$，均匀性测试的步骤2必定通过（否则 $\mathbf{1}_{\vec{r}} = 0$，公式（4）就会变成 $1 \leq \sqrt{\varepsilon}$）；而对 $\rho_{\vec{r}}$ 执行均匀性测试的步骤3，以至少 $1-\sqrt{\varepsilon}$ 的概率通过。

令 $\rho_{question|\vec{r}}$ 为 $\rho_{\vec{r}}$ 在其问题寄存器上的限制。对于任意固定的良好 $\vec{r}$（对 $\rho_{\vec{r}}$ 执行均匀性测试的步骤3时，以至少 $1-\sqrt{\varepsilon}$ 的概率通过），我们有

$$\mathrm{tr}[((|\bar{0}\rangle\langle\bar{0}|)^{\otimes T} \otimes I_{\overline{T}})\rho_{question|\vec{r}}] \geq 1-\sqrt{\varepsilon},$$

其中，记号$(|\bar{0}\rangle\langle\bar{0}|)^{\otimes T}$表示索引属于$T$的寄存器处于零傅里叶态，并与其他寄存器形成张量积。因此，根据温和测量引理 [Wil11，引理 9.4.1]，有

$$\|\rho_{question|\vec{r}} - \underbrace{(|\bar{0}\rangle\langle\bar{0}|)^{\otimes T} \otimes \sigma(\vec{r})_{\overline{T}}}_{\sigma(\vec{r})}\|_1 \leq 2\varepsilon^{1/4}. \tag{5}$$

根据构造，在标准基下测量 $\sigma(\vec{r})$，会得到一个分布 $\mu_{\vec{r}}$：它在 T 中的寄存器上产生均匀随机的独立同分布结果，而在其他寄存器上则产生某种任意分布。

因此，在标准基下测量 $\rho_{question|\vec{r}}$（对任意良好的 $\vec{r}$而言），会得到一个与 $\mu_{\vec{r}}$ 的总变差距离为 $O(\varepsilon^{1/4})$的分布，这是由变差距离与迹距离之间的关系得出的 [NC02，定理 9.1]。

令 $\rho_{question}$ 表示将此状态（在本证明第一段中定义）限制在其问题寄存器上的状态。为了讨论测量 $\rho_{question}$（不再以固定的良好 $\vec{r}$为条件）所得到的分布，注意到

$$\rho_{question} = \sum_{\vec{r}} q_{\vec{r}}\, \rho_{question|\vec{r}} = \sum_{\vec{r}\in BAD} q_{\vec{r}}\, \rho_{question|\vec{r}} + \sum_{\vec{r}\in GOOD} q_{\vec{r}}\, \rho_{question|\vec{r}}, \tag{6}$$

并回顾一下，$\vec{r}$ 以至少 $1-\sqrt{\varepsilon}$ 的概率是良好的。由此可知，存在一个在 $\rho_{question|\vec{r}}$s 上没有权重、且与 $\rho_{question}$ 的迹距离至多为$O(\sqrt{\varepsilon})$ 的状态，其中 $\vec{r}$ 属于 BAD。形式化地，若我们定义一个新状态

$$\rho'_{question} = \sum_{\vec{r}\in GOOD} q_{\vec{r}}\, \rho_{question|\vec{r}} + \left(\sum_{\vec{r}\in BAD} q_{\vec{r}}\right) \rho_{question|\vec{r}^*},$$

其中 $\vec{r}^*$ 是任意一个（具体而言，取字典序最先的）$\vec{r}$，且属于 $GOOD$，我们有

$$\|\rho'_{question} - \rho_{question}\|_1 = O(\varepsilon^{1/2}). \tag{7}$$

与此同时，请注意，$\rho'_{\text{问题}}$ 可以表示为一个和

$$\rho'_{question} = \sum_{\vec{r}\in GOOD} q'_{\vec{r}}\, \rho_{question|\vec{r}}, \tag{8}$$

其中 $q'_{\vec{r}}$ 是关于 $\vec{r}$的某个分布。对于任意良好的 $\vec{r}$，令 $T(\vec{r})$ 表示满足以下条件的集合：$T \subseteq [k]$，$|T| \geq k\,K'(1-\eta)$，$r_i = 0\,\forall i \in T$。根据迹距离的强凸性 [NC02、定理 9.3] 和公式（5），我们有

$$\left\|\rho'_{question} - \sum_{\vec{r}\in GOOD} q'_{\vec{r}} \left((|\bar{0}\rangle\langle\bar{0}|)^{\otimes T(\vec{r})} \otimes \sigma(\vec{r})_{\overline{T(\vec{r})}}\right)\right\|_1 \leq \sum_{\vec{r}\in GOOD} q'_{\vec{r}} \cdot 2\varepsilon^{1/4}. \tag{9}$$

因此，

$$\left\|\rho'_{question} - \sum_{\vec{r}\in GOOD} q'_{\vec{r}} \left((|\bar{0}\rangle\langle\bar{0}|)^{\otimes T(\vec{r})} \otimes \sigma(\vec{r})_{\overline{T(\vec{r})}} \right) \right\|_1 \leq 2\varepsilon^{1/4}. \tag{10}$$

由三角不等式可得，

$$\left\|\rho_{question} - \sum_{\vec{r}\in GOOD} q'_{\vec{r}} \left((|\bar{0}\rangle\langle\bar{0}|)^{\otimes T(\vec{r})} \otimes \sigma(\vec{r})_{\overline{T(\vec{r})}} \right) \right\|_1 = O(\varepsilon^{1/4}) + O(\varepsilon^{1/2}) = O(\varepsilon^{1/4}). \tag{11}$$

最后，根据完全正迹保持映射下迹距离的收缩性[NC02，定理 9.2]，同时测量 $\rho_{question}$ 和 $\sum_{\vec{r}\in GOOD} q'_{\vec{r}} \left((|\bar{0}\rangle\langle\bar{0}|)^{\otimes T(\vec{r})} \otimes \sigma(\vec{r})_{\overline{T(\vec{r})}} \right)$ 的标准基不会增大它们之间的迹距离。显然，在标准基下测量后者会得到如下形式的分布

$$\sum_{T\in\mathcal{S}} p(T)\mu_T^{unif} \otimes \mu_{\overline{T}}^{junk}$$

对于集合 $\mathcal{S} \{T: \exists \vec{r} \in GOOD$ 使得$T = T(\vec{r})\}$。因此，结论得证。

□

3.3 一致性测试的可靠性与主协议的可靠性

我们先给出几个定义。

定义 27 (一致性博弈**)**。给定任意图 $\mathcal{G} = (V,E)$、自然数 K 和关系 $R:[K]\times[K]\to\{0,1\}$，定义(k,ℓ)一致性博弈，记作 $G^{k,\ell}(\mathcal{G},K,R)$，或者在参数由上下文明确时简记为 $G^{k,\ell}$，它是如下的经典 双玩家自由博弈。（注意，该博弈与 *[AIM14]* 中的 k,ℓ 生日重复博弈相同。）

- *Alice* 收到从边集 E 中均匀随机选取的一个大小为 k 的子集 A，而 *Bob* 收到从顶点集 V 中均匀随机选取的一个大小为 ℓ 的子集 B。
- *Alice* 用颜色为 A 中边的所有端点顶点着色（即 *Alice* 为每个作为 A 中某条边端点的顶点指定一个 $[K]$ 中的数），而 *Bob* 为 B 中的所有顶点着色。
- 对于每条边 $e \in A$ 和每个顶点 $v \in B$，只要 $v \in e$，*Arthur* 就检查 *Alice* 和 *Bob* 的着色是否一致，以及 e 的两个端点所赋的颜色是否满足关系 $R(e,\cdot,\cdot)$。

定义 28 （具有特殊问题分布的自由博弈）。设 G 是一个双人自由博弈，其中问题对从问题集 $X\times Y$ 中均匀抽取，且令 $\mathcal{D}$ 为 $X\times Y$ 上的一个分布。那么，$G|_{\mathcal{D}}$表示这样一个博弈 G：问题对根据分布 $\mathcal{D}$抽取。

我们希望通过将第 3.1 节协议的可靠性归约为定义 27 中一致性博弈的可靠性，来证明该协议的可靠性；后者已在[AIM14]中作为“生日博弈”进行过分析。也就是说，给定第 3.1 节中我们 QMA(2) 协议的一种策略（即一对见证态），我们希望构造出一致性博弈的一种策略。我们想要证明的结论形式化为以下引理。

引理 29. 设$(\mathcal{G},K,R)$ 是一个 δ-*GAP-KCOL* 实例。假设在图 *1* 的协议中，两个状态 $|\psi_1\rangle,|\psi_2\rangle$ 以至少 $1-\varepsilon$ 的概率被接受。那么，存在一种针对 $G^{k'},k'(\mathcal{G},K,R)$, $k' = k\,K'(1-\eta)$ 的策略，其博弈值为 $1-\Theta(\varepsilon^{1/4})$。

我们将引理 29 的证明推迟到证明引理 31、32 和 33 之后。不过，显然，引理 29 与下面的引理 30 结合起来，就能为第 3.1 节的协议提供所需的常数可靠性。

引理 30. 设 $\mathcal{G} = (V,E)$ 是一个具有 n 个顶点和 $\Theta(n)$ 条边的图，$K \in \mathbb{N}$ 是一个常数，且 $R:E\times[K]\times[K]\to\{0,1\}$ 是一个函数。假设对于某个常数 $\delta > 0$，任何关于 $\mathcal{G}$ 且满足 R 的广义 K-着色，至少违反 δ比例的边。那么，对于 $k = \ell \equiv \Omega(\sqrt{n})$，一致性博弈 $G^{k,\ell}(\mathcal{G})$ 的经典值至多为 $1-c$，其中 $c > 0$是一个常数。

证明。这由 [AIM1 的定理 26 得出 4]. □

从 n 在本节中，我们固定一个 δ-GAP-KCOL 的实例$(\mathcal{G},K,R)$，并省略参数 e-ters in our 一致性博弈 $G^{k,\ell}$（$\mathcal{G}$,K、R）的记号。

引理 31。对于任意一对状态 $|\psi_1\rangle$、$|\psi_2\rangle$，如果它们在图 *3* 的一致性测试中以概率 $1-\nu$ 被验证者 QMA（2）*Arthur* 接受，则在 G^k、$^\ell$ 上存在一个关于问题对的乘积分布 $\mathcal{D}$（ψ_1、ψ_2）$=\mathcal{D}^A\otimes\mathcal{D}^B$，以及一个在 G^k、$^\ell|_{\mathcal{D}(\psi_1,\psi_2)}$ 上取得博弈值 $1-\nu$ 的随机化经典策略。

证明。为了得到 $\mathcal{D}$ 以及经典策略，对 $|\psi_1\rangle$ 和 $|\psi_2\rangle$进行标准基测量。

□

以下是引理 26 的另一种表述。

引理 32。对于 $|\psi_1\rangle$，$|\psi_2\rangle$ 它们各自以概率 $1-\nu$通过均匀性测试（图 *2*），测量 $|\psi_1\rangle$ 和 $|\psi_2\rangle$ 的 问题寄存器的标准基，得到的分布$\mathcal{D}(\psi_1,\ \psi_2)$ 具有如下形式

$$\mathcal{D}(\psi_1,\psi_2)=\mathcal{D}^A\otimes\mathcal{D}^B,$$

其中，对于 $W\in\{A,\ B\}$, $\mathcal{D}^W$ 具有如下形式的分解

$$\mathcal{D}^W=\sum_{T:T\subseteq[k],|T|\geq\frac{k}{K'}(1-\eta)}p^W(T)\mathcal{D}_T^{unif}\otimes\mathcal{D}_{\overline{T}}^{junk,W}+\mathcal{D}^{error,W},$$

其中 p^W 是一个将子集 $T\subseteq[k]$ 映射到 $[0,1]$, 和 $\|\mathcal{D}^{error,\ W}\|_1\leq\delta(\nu)=O(\nu^{1/4}$).

直观地说，引理 32 表明，如果 Alice 和 Bob 提供的状态 $|\psi_1\rangle,|\psi_2\rangle$ 以较高概率通过均匀性测试（图 2），那么通过测量 $|\psi_1\rangle$ 和 $|\psi_2\rangle$ 的问题寄存器的标准基，得到的关于 $G^{k,\ell}$ 的问题的分布，可以（在 Alice 和 Bob 各自一侧）表示为若干分布的凸混合；构成该凸混合的大多数分布在其索引的某个显著比例上是均匀的，其余分布（即 $\mathcal{D}^{error}$ 分布）则是任意的。

现在我们证明一个引理，它使我们能够将以这种方式抽取问题的一致性博弈的可靠性，归约为问题均匀随机抽取的较小一致性博弈实例的可靠性。

引理 33。设 $\mathcal{D}=\mathcal{D}^A\otimes\mathcal{D}^B$，其中 $\mathcal{D}^A$ 具有如下形式

$$\sum_{T:T\subseteq[k],|T|=k'}p^A(T)\mathcal{D}_T^{unif}\otimes\mathcal{D}_{\overline{T}}^{junk,A}$$

且 $\mathcal{D}^B$ 具有如下形式

$$\sum_{T:T\subseteq[\ell],|T|=\ell'}p^B(T)\mathcal{D}_T^{unif}\otimes\mathcal{D}_{\overline{T}}^{junk,B}$$

其中 $k'\leq k$，$\ell'\leq\ell$。则

$$\omega(G^{k,\ell}|_{\mathcal{D}})\leq\omega(G^{k',\ell'}).$$

证明。固定 S，它是博弈 $G^{k,\ell}|_{\mathcal{D}}$ 的一个策略。$G^{k,\ell}|_{\mathcal{D}}$ 的任意策略 S 都会自动诱导出 $G^{k',\ell'}$ 的一个策略 S′。具体而言，这个诱导策略的运作方式如下：给定来自 $G^{k',\ell'}$ 的 Alice 问题 x′，Alice 按照分布 p(T) 抽取一个集合 T，再从 $\mathcal{D}_{\overline{T}}^{junk}$ T 中抽取一个 x″，并令 x $=$ x′‖x″。随后，她使用自己在 $G^{k,\ell}|_{\mathcal{D}}$ 中的策略，为问题 x 抽取一个答案 a。a 必然会为 x′ 所表示的边集中所有边的端点指定颜色；Alice 只返回这些颜色，我们将其记为 a′。Bob 也以同样的方式操作：收到问题 y′ 后，抽取问题 y″，构造 y $=$ y′‖y″，得到问题 y 的答案 b，并返回 b′，即 b 中与 y′ 相关部分的限制。

我们可以通过一系列混合实验，分析S' 相对于S 的成功概率。

1. 在第一个混合中，采用策略 S 进行游戏 $G^{k,\ell}|_{\mathcal{D}}$。假设 S 在 $G^{k,\ell}|_{\mathcal{D}}$中的成功概率为 p 。

2. 在第二个混合中，我们为 $G^{k,\ell}|_{\mathcal{D}}$定义一个新策略 R。新策略的执行方式如下：Alice 从 $G^{k',\ell'}$的问题分布中抽取一个问题 x'，按照分布 p(T) 抽取一个集合 T，从 $\mathcal{D}_{\overline{T}}^{junk}$ T 中抽取一个 x''，并令 $x = x' \| x''$。随后，她针对问题 x 采用策略 S。Bob 也以同样的方式操作：抽取问题 y'，抽取问题 y'' 以构成 $y = y' \| y''$，并针对问题 y 采用策略 S。对于 $W \in \{A, B\}$，$\mathcal{D}_W$ 的形式意味着，在这个混合中，问题 x 和 y 的分布与它们在 $G^{k,\ell}|_{\mathcal{D}}$中的分布完全相同。因此，R 的成功概率仍为 p。

3. 在第三个混合中，Alice 和 Bob 在博弈 $G^{k',\ell'}$ 中采用本证明第一段所述的“诱导策略”S'。注意，对于博弈 $G^{k',\ell'}$ 中所有可能的问题 (x', y')，以及将 (x', y') 嵌入博弈 $G^{k,\ell}|_{\mathcal{D}}$ 中问题 (x, y) 的所有可能方式，博弈 $G^{k',\ell'}$ 的规则要求 Arthur 对 $a' \subseteq a, b' \subseteq b$ 执行的检查，都是博弈 $G^{k,\ell}|_{\mathcal{D}}$ 的规则要求 Arthur 对 a, b 执行的检查的子集。这意味着，对于博弈 $G^{k',\ell'}$ 中的任意有效问题 (x', y')，以及根据本证明第一段中的过程由 (x', y') 诱导出的任意 (x, y)，问题对 (x, y) 的获胜答案都会诱导出 (x', y') 的获胜答案。因此，从上一个混合到这一个混合，成功概率只会增加。

我们得出结论：如果存在策略S，使其在$G^{k,\ell}|_{\mathcal{D}}$ 中以概率p获胜，那么由S 诱导出的策略S' 在$G^{k',\ell'}$ 中获胜的概率至少为p。 □

现在我们准备证明引理 29。为方便起见，我们在下文将引理 29 重述为引理 34。**引理 34.** 设$(\mathcal{G}, K, R)$ 是 δ-*GAP-KCOL*的一个实例。假设在图 *1* 的协议中，状态 $|\psi_1\rangle, |\psi_2\rangle$ 以至少 $1-\varepsilon$的概率被接受。那么，存在一个策略，其博弈值为 $1 - O(\varepsilon^{1/4})$，适用于 $G^{k',k'}(\mathcal{G}, K, R)$, $k' = k\,K'(1-\eta)$。 —

证明。 令 $\mathcal{D} = \mathcal{D}^A \otimes \mathcal{D}^B$ 和 $\mathcal{S}$ 分别为$G^{k,k}$ 中问题的乘积分布，以及成功概率为 $1 - 2\varepsilon$ 的随机化经典策略；它们是在$G^{k,k}|_{\mathcal{D}}$ 中将引理 31 应用于 $|\psi_1\rangle, |\psi_2\rangle$后得到的。

现在，将引理 32 应用于 $\mathcal{D}^W$ for $W \in \{A,B\}$，我们得到如下分解

$$\mathcal{D}^W = \sum_{T:T\subseteq k, |T|\geq \frac{k}{K'}(1-\eta)} p^W(T)\mathcal{D}_T^{unif} \otimes \mathcal{D}_{\overline{T}}^{junk,W} + \mathcal{D}^{error,W},$$

其中误差项的 1-范数至多为 $\delta(\varepsilon) = O(\varepsilon^{1/4})$。我们

可以， ithout 不失一般性，重写这样的分解 n as

$$\mathcal{D}^W = \sum_{T:T\subseteq k, |T|=\frac{k}{K'}(1-\eta)} p^W(T)\mathcal{D}_T^{unif} \otimes \mathcal{D}_{\overline{T}}^{junk,W} + \mathcal{D}^{error,W}.$$

由于 $\mathcal{D}^W$ 中误差项的概率质量至多为 $\delta(\varepsilon)$，因此在 $G^{k,k}|_{\mathcal{D}}$ 中，Alice 或 Bob 的问题来自 $\mathcal{D}^{error,W}$ 的子博弈的概率质量至多为 $2\cdot\delta(\varepsilon)$。因此，我们可以从 $\mathcal{D}^W$ 中舍弃这些项，代价是使博弈 $G^{k,k}|_{\mathcal{D}}$ 的博弈值改变 $O(\delta(\varepsilon))$，从而得到一个新博弈 $G^{k,k}|_{\mathcal{D}'}$，其中问题分布 $\mathcal{D}' = (\mathcal{D}^A)' \otimes (\mathcal{D}^B)'$ 是仅由“好”项构成的混合分布，且 $(\mathcal{D}^A)'$ 和 $(\mathcal{D}^B)'$ 均如此；该博弈的博弈值至少为 $1 - 2\varepsilon - O(\delta(\varepsilon))$。

接下来，我们将引理 33 应用于 $G^{k,k}|_{\mathcal{D}'}$。由此可知，$\omega(G^{k,k}|_{\mathcal{D}'}) \leq \omega(G^{k',k'})$，其中 $k' = k\,K'(1-\eta)$。因此，

$$1 - 2\varepsilon - O(\delta(\varepsilon)) \leq \omega(G^{k',k'}).$$

至此，引理的证明得证。 □

此外，根据引理 30，$\omega(G^{k',k'})$ 至多为 $1-c$，其中 $k' = \Omega(\sqrt{n})$。结合引理 29，我们得到，在第 3.1 节的协议中，作弊的 Merlin 的成功概率至多为 $1-c'$，其中某个常数为 $c' > 0$：引理 30 所表达的一致性博弈的可靠性 $\omega(G^{k',k'})$ 要求

$$1 - O(\varepsilon^{1/4}) \leq 1 - c,$$

因此

$$\varepsilon \geq \Omega(c^4).$$

3.4 指数时间假设下 h^{Sep} 的下界

定义 **n 35** (h^{Sep})。令 $\mathcal{H}_{AB}:=\mathcal{H}_A\otimes\mathcal{H}_B$，其中 $\mathcal{H}_A$ 和 $\mathcal{H}_B$ 是有限维希尔伯特空间。令 $\mathcal{S}_{A\quad B}$ 为可分态集合在 $\mathcal{H}_{AB}$ 上，即满足以下条件的密度矩阵集合 ρ_{AB}：ρ_{AB} 可以写成

$$\rho_{AB}=\sum_k p_k\,\rho_{A,k}\otimes\rho_{B,k}$$

其中，对所有 k，$\rho_{A,\,k}$ 是 $\mathcal{H}_A$ 上的密度矩阵，$\rho_{B,\,k}$ 是 $\mathcal{H}_B$ 上的密度矩阵，且 p_k 是一个概率。给定 $\mathcal{H}_{AB}$ 上的厄米矩阵 M，$h^{\mathrm{Sep}}(\varepsilon,\ M,\ \mathcal{H}_{AB})$ 是估计以下数值的问题

$$\max_{\rho\in\mathcal{S}_{AB}}\ \mathrm{tr}(M\rho)$$

误差不超过 ε。

定理 36。设 $|\mathcal{H}|$ 表示希尔伯特空间 $\mathcal{H}$的维度。假设 $\mathscr{A}$是一个用于求解 $h^{\mathrm{Sep}}(\varepsilon,M,\mathcal{H}_{AB})$ 的算法，其中 ε 为常数，且 M 满足 $\{M,\mathbf{1}-M\}$ 是贝尔测量（见定义 *3*）。如果 $\mathscr{A}$的时间复杂度至多为

$$\exp(O(\log^{1-\nu}|\mathcal{H}_A|\log^{1-\mu}|\mathcal{H}_B|))$$

对于 $\nu+\mu>0$，那么对于含有 N 个子句的 *3SAT*，可在 $2^{N^{1-(\nu+\mu)/2}\cdot\text{多对数}}N$ 时间内求解。

证明。假设 $\mathcal{G}=$(V, E) 是一个有 n 个顶点和 m 条边的图，并设 ($\mathcal{G}$, K, R) 是 δ-GAP-KCOL 的一个实例（定义 22）。我们在第 3.1 节给出一个 BellQMA(2) 协议，用于判定任意这样的 δ-GAP-KCOL 实例；当 δ 和 K 都是常数时，该协议具有常数完备性-可靠性差距，且见证位于两个无纠缠寄存器上，其大小分别为 O($\sqrt{\mathrm{n}}$ log m) 和 O($\sqrt{\mathrm{n}}$ log n)。根据定理 23，我们可以将任意含 N 个子句的 3SAT 实例归约为一个 δ-GAP-KCOL 实例，其中 δ和 K 是常数，且 m、n $=$N poly log N。因此，我们可以令 $|\mathcal{H}_A|=|\mathcal{H}_B|=2^{\sqrt{\mathrm{N}}\cdot\mathrm{poly\,log\,N}}$。将假设的算法 $\mathscr{A}$应用于由我们的协议诱导的测量 $\{\mathrm{M},\mathbf{1}-\mathrm{M}\}$，可知 $\mathscr{A}$能够在以下时间内求解 3SAT:

$$\exp\left(O(\log^{1-\nu}|\mathcal{H}_A|\log^{1-\mu}|\mathcal{H}_B|)\right)\le\exp(N^{1-(\nu+\mu)/2}\cdot\mathrm{poly\,log}\,N).$$

□

假设指数时间假设成立（即N子句 3SAT 不存在运行时间为 $2^{o(N)}$ 的任何算法），定理 36 表明，不存在一种针对h^{Sep}、使用贝尔测量且运行时间至多为

$$\exp(O(\log^{1-\nu}|\mathcal{H}_A|\log^{1-\mu}|\mathcal{H}_B|))$$

对于任意常数 $\nu+\mu>0$ 都成立。因此，定理 36 表明，由 [BCY10] 给出的、针对h^{Sep} 且使用 LOCC 测量的算法是最优的（可能相差关于 $|\mathcal{H}_A|$ 和 $|\mathcal{H}_B|$的双对数因子）。LOCC 测量是贝尔测量的超类。

4 自由纠缠游戏：无间隙情形

本节中，我们将证明，任何零间隙多证明者交互式证明* 协议都可以压缩为问题长度为常数的协议，同时不会显著增加答案长度和验证器运行时间。因此，我们得到，在无间隙情形下，MIP* 与 AM* 相同。

必须谨慎解读这一结果：在无间隙情形下，判定一个自由博弈的博弈值是否为 1，显然与判定一般博弈的博弈值是否为 1 一样困难，因为只需让验证者独立地为两位证明者抽取问题，并对“无效”问题对自动接受，任何博弈都能转化为自由博弈。这一变换保留了博弈值为 1 的策略；如果原始博弈的博弈值与 1 有一定差距，变换后的博弈也会如此。因此，单凭结论 $\mathrm{MIP}_0^*=\mathrm{AM}_0^*(2)$ 并不 有趣。事实上，（按照我们在第 2 节中对 $\mathrm{AM}_0^*(2)$和 MIP_0^*所作的定义），[MNY20、MNY21]已经早已 证明了 $\mathrm{AM}_0^*(2)=\mathrm{MIP}_0^*=\Pi_2$。相反，本节结果真正 有趣之处在于，我们能够得到问题大小为常数的协议。在下一节中，我们将运用类似的技巧来得到协议

在有间隙情形下，使我们能够证明 $\mathrm{MIP}^* = \mathrm{AM}^*(2) = \mathrm{RE}$ 这一非平凡且新颖的事实。

本节的主要复杂性结果是定理 39。

定义 37。 语言 L 由所有作为图灵机描述的字符串 x 组成，其中$\forall y \in \{0,1\}^*$，存在一个时间 $t \in \mathbb{N}$，使得由 x_x 描述的图灵机 M 在输入 y 上经过 t 步后停机。

事实 38。 语言 L 是 Π_2^0完全的。

定理 39 （下方的定理 47）。 存在一个AM_0^*（2）[O（1），O（$\log^*$（$\log$（n））$\cdot\log$（n））， O（$n\log^*$（n））] 协议，用于 Π_2完全语言 L（定义 *37*）。

定理 39 通过证明一个无间隙的“超压缩”定理来得出，该定理将任意博弈的问题长度压缩为常数。该定理的另一个推论是，我们为n EPR 对获得了一种（非鲁棒）自检，且只需固定数量的问题。这是已知的首个此类测试；此前的结果都至少要求对数大小的问题，即使在零间隙（即非鲁棒）情况下也是如此 [˜SB20，表 1]。

定理 40 （下文的定理 48）。 存在一个博弈族 G^{EPR}，其问题数为 q（n）$= Q_0$, a（n）$= O$（n），t_c（n）$=$ 多项式（n），且 t_d（n $=$ 多项式（n），以及 $\mathcal{E}$（G_n^{EPR}）$= n$。

4.1 博弈的细粒度压缩定理

一些证明压缩定理的先前工作以游戏族的形式陈述这些定理（我们的游戏族定义见定义 13），同时遵循这样一种约定：压缩后，问题和答案长度以及验证器运行时间关于 n（与游戏族关联的索引）大致保持不变；压缩的效果则通过关联 $G_n^{\downarrow}$ 的博弈值与 $G_{2^n}^{\downarrow}$的博弈值来表达，其中 $G^{\downarrow}$ 是“压缩后”的游戏族，$G^{\downarrow}$ 是未压缩的游戏族。例如， [JNV$^+$20] 的问题缩减定理非正式地表述如下：给定一个验证器 $V^{\downarrow}$，它生成一个游戏族 $G^{\downarrow}$，其中问题长度为 $q^{\downarrow}(n)$，答案长度为 $a^{\downarrow}(n)$，则存在一个“压缩验证器”$V^{\downarrow}$，它生成一个游戏族 $G^{\downarrow}$，其中问题长度为 $\mathrm{poly}(q^{\downarrow}(n))$，答案长度为 $2^{a^{\downarrow}}(n) + 2^{q^{\downarrow}}(n) + \mathrm{poly}(n)$，并且 $G^{\downarrow}$ 中第 n 个博弈的博弈值与 $G^{\downarrow}$中第 2^n 个博弈的博弈值相近。我们将这一约定非正式地称为“放大设定”。

在本文中，我们倾向于将 [JNV$^+$20] 压缩定理表述如下：给定一个验证者 $V^{\downarrow}$，它生成一个博弈 $G^{\downarrow}$，其问题长度为 $q^{\downarrow}(n)$，答案长度为 $a^{\downarrow}(n)$；则存在一个“压缩验证器”$V^{\downarrow}$，它生成一个博弈 $G^{\downarrow}$，其问题长度为 $\mathrm{poly\,log}\, q^{\downarrow}(n)$，答案长度为 $a^{\downarrow}(n) + q^{\downarrow}(n) + \mathrm{poly\,log}(n)$，并且 $G^{\downarrow}$ 中第 n 个博弈的博弈值与 $G^{\downarrow}$中第 n 个博弈的博弈值相近。我们将此称为“缩小设定”。

我们倾向于采用“缩小”这一约定，是因为最终我们希望在保持索引 n 不变的同时，对单个协议（判定特定语言 L）反复应用压缩，从而得到一个问题更短、但判定同一语言的协议。缩小设定在记号上让我们更容易做到这一点。

4.1.1 无间隙问题约简

我们将首先在缩小设定下重新陈述 [MNY21] 的无间隙压缩定理，并给出更精确的问题和答案长度界（为了证明我们的超压缩定理，这些界是必需的）。

定义 41。 问题采样博弈 QS_n 是一个具有 $|\mathcal{X}_{MS}|\cdot n^2$ 个可能问题和 $|\mathcal{A}_{MS}|^2 + 2^n$ 个可能答案的博弈。因此，其问题和答案比特长度分别为 $q^{QS}(n) = \lceil 2\log n + \log|\mathcal{X}_{MS}|\rceil$ 以及 $a^{QS}(n) = \lceil 2\log|\mathcal{A}_{MS}|\rceil + n$。其检查器运行时间为 $t_c^{qs}(n) = O(\log n)$，判定器运行时间为 $t^{qs}d(n) = O(n)$。

博弈的精确定义见 [MNY21，第 3 节3]。

定理 42。存在一台具有以下性质的图灵机 *GaplessIntro*。设 $G = (D, C, Q)$ 是一个游戏族，其问题长度为 $q(n)$，答案长度为 $a(n)$，判定器运行时间为 $t_d(n)$，检查器运行时间为 $t_c(n)$，其中 $t_c(n)$、$t_d(n) = poly(n)$，并假设 Q 在输入 n 时能以 $O(\log n)$ 的时间计算 $q(n)$。那么，向 *GaplessIntro* 提供 D、C、Q 的描述后，它会输出一个游戏族 D^{intro}、C^{intro}、Q^{intro}，满足以下条件。

1.（问题长度：）G_n^{intro}的问题字母表大小为 $7 + |\mathcal{X}_{QS}(q(n))| = |\mathcal{X}_{MS}| \cdot (q(n))^2 + 7$。因此，$G_n^{intro}$的问题长度上界为 $q_{intro}(n) = \lceil 2\log q(n) + 7 + \log |\mathcal{X}_{MS}| \rceil$。*2.*（答案长度：）$G_n^{intro}$的答案长度为 $a(n) + q(n) + O(1)$。（此处，$O(1)$ 表示一个与 G 无关的普适常数。）*3.*（检查器：）检查器 C^{intro} 在输入 (n, x, y) 时，会在 $O(\log n)$ 时间内计算 $q_{intro}(n)$，然后在输入 (q, x, y) 时运行通用检查器 C^{intro}, ^{universal}，其运行时间为 $t_c^{qs}(q) + O(1)$。因此，检查器的总运行时间为 $t_c^{qs}(q_{intro}(n)) + O(\log n)$，其中 t_c^{qs}是问题采样博弈的检查器时间上界（且仅是 $q_{intro}(n)$ 的函数）。*4.*（判定器：）判定器 D^{intro} 的运行时间上界为 $t_d^{intro}(n) = t_d(n) + t^{qs}{}_d(q_{intro}(n)) + O(\log n)$，其中 $t^{qs}{}_d$ 是问题采样博弈的判定器时间上界（且仅是 $q_{intro}(n)$ 的函数）。*5.*（完备性：）对于 G_n的所有可预言化有限维同步策略，都存在一个 G_n^{intro}的可预言化有限维同步策略，其博弈值至少与之相同。*6.*（可靠性：）若 $\omega_q(G_n) < 1$，则 $\omega_q(G_n^{intro}) < 1$。*7.*（纠缠界：）$\mathcal{E}(G_n^{intro}) \geq max\{\mathcal{E}(G_n), 2^{2n}\}$。*8.*（高效可计算性：）*GaplessIntro* 的运行时间应为 $O($

$| \quad | + | \quad | + | \quad | \qquad | \quad ^{intro}| =$

$| \quad | + \quad 1 \qquad | \quad ^{intro}| = | \quad | + \quad 1 \qquad | \quad ^{intro}| = | \quad | + \quad 1$

$D\ C\ Q\ )$。此外，$D\ D\ O(\ )$、$C\ C\ O(\ )$，且 $Q\ Q\ O(\ )$。

证明。 图灵机 GaplessIntro 构造了 [MNY21 定理 4.1] 中的内省游戏。通过检查 [MNY21] 中的游戏，可得所声称的问题长度和答案长度界。 [MNY21] 直接证明了完备性、可靠性和纠缠界。

对于检查器运行时间，根据假设，计算 q(n) 需要 O(log n) 时间，因此计算 $q_{intro}(n) = \lceil 2\log q(n) + 7 + \log |\mathcal{X}_{MS}| \rceil$ 也需要 O(log n) 时间。计算出 $q_{intro}(n)$ 后， [MNY21] 中的“通用”检查器要么调用问题采样博弈的检查器，要么对特殊问题类型执行常数时间检查。因此，检查器的总运行时间为 $t_c^{qs}(q_{intro}(n)) + O(\log n)$，如所声称。

对于判定器运行时间， [MNY21] 的判定器会运行 D 的原始判定器、问题采样博弈的判定器，并可能执行一些常数时间额外操作。为了运行问题采样博弈的判定器，它必须计算 $q_{intro}(n)$，这需要 $O(\log n)$ 时间。因此，总运行时间为 $t_d(n) + t^{qs}{}_d(q_{intro}(n)) + O(\log n)$。

关于高效可计算性，只需检查博弈描述即可得出结论。

我们指出，在相应的定理 [MNY21], 中，结论仅对所有满足 $n \geq n_0^{intro}$ 的情况成立，其中 n_0^{intro} 可能取决于输入博弈的性质。然而，通过检查证明可以验证，对 n 的这一限制仅仅是由于 [MNY21] 所给界的非渐近形式。事实上，完备性和可靠性对所有 n 都成立，而我们在此给出的关于问题长度、答案长度，以及检查器和判定器运行时间的界，对所有n 也都成立。

□

备注 检查器 C^{intro} 实际上是通用的，完全不依赖于 G。

4.1.2 无间隙答案归约

以下定理本质上是 [MNY21 定理 5.1], ，但问题长度、答案长度和判定器运行时间的界更紧。

定理43。存在一台图灵机 *GaplessAnsReduce*，具有以下性质。设 $G = (D, C, Q)$ 是一个游戏族，其复杂度界分别为 $q(n)$、$a(n)$、$t_c(n)$、$t_d(n)$，其中 $a(n) \leq t_d(n) = poly(n)$，且 $q(n) = O(\log n)$。将 (D, C, Q) 的描述作为输入交给 *GaplessAnsReduce*，它会返回一个游戏族 $G^{ans} = (D^{ans}, C^{ans}, Q^{ans})$ 的描述，使得对于游戏族 G^{ans} 以及所有 n，均有

*1. (*问题长度：*)* 问题长度为 $q_{ans}(n) = 2q(n) + O(\text{对数}\,|D| + \text{对数}\,t_d(n))$，其中 $|D|$ 是图灵机 D 的描述长度。

*2. (*答案长度：*)* 答案长度为 $O(1)$。

*3. (*检查器运行时间：*)* 检查器的运行时间为 $t_c(n) + O(\log|D| + \log t_d(n))$。

*4. (*判定器运行时间：*)* 判定器的运行时间为多对数(n)。

*5. (*完备性：*)* 对于任意可预言化有限维同步策略 $\mathscr{S}$ *to* G_n，都存在一个可预言化有限维同步策略 $\mathscr{S}^{ans}$ *to* G_n^{ans}，使得

$$\omega_q(G_n^{ans}, \mathscr{S}^{ans}) \geq \frac{1}{2} + \frac{1}{2}\omega_q(G_n, \mathscr{S}).$$

*6. (*可靠性：*)* 若 $\omega_q^s(G_n) < 1$，则 $\omega_q^s(G_n^{ans}) < 1$。

*7.(*纠缠界：*)* $\mathcal{E}(G_n^{ans}) \geq \mathcal{E}(G_n)$。

*8. (*高效可计算性：*)* GaplessAnsReduce 应在时间 $O(|D| + |C| + |Q|)$内运行。此外，$|D^{ans}| = |D| + O(1)$，且 $|C^{ans}| = |C| + O(1)$，以及 $|Q^{ans}| = |Q| + O(1)$。

证明。 所声称的性质可由 [MNY21 定理 5.1] 的证明推出。与问题约简的情形一样，我们指出，在 [MNY21], 的相应定理中，结论仅陈述为对所有 $n \geq n_0^{intro}$ 均成立，其中 n_0^{intro} 可能取决于输入博弈的性质。不过，这只是因为该定理中所述界采用了非渐近形式；完备性和可靠性对所有 n 均成立，而我们所述的渐近界也对所有 n 均成立。

为了了解定理结论中的各项如何由 [MNY21], 得出，请回想答案约简后的博弈是如何得到的：

1. 首先，对博弈 G 进行预言机化：这会使问题和答案长度增加一倍，并使判定器运行时间增加$O(a_n)$。
2. 接下来，通过指示预言机化博弈中的证明者构造验证者对答案进行计算的图灵机配置表，即可得到博弈 G^{ans}，这与库克-列文定理中的做法相同。当且仅当该图灵机配置表满足一组局部约束时，验证者的计算才会接受证明者的答案；每个局部约束都作用于图灵机配置表中的常数个位置。现在，博弈 G^{ans} 中的验证者问题由来自博弈 G预言机化后得到的问题，以及图灵机配置表中的常数个索引组成。诚实证明者的答案由图灵机配置表中这些索引处所写的值组成。验证者会检查这些答案是否满足相应的局部约束。

在他们的证明中，图灵机配置表的长度记为 L，并证明了$L = \text{poly}(|D|, q(n), t_n) = \text{poly}(|D|, t_d(n))$。

1.（问题长度：）问题集 G^{ans} 由 G 的问题集与图灵机配置表中至多 3 个索引组成的所有元组的笛卡尔积构成。因此，G^{ans} 的问题长度至多为 $2q(n) + O(\log L) = q(n) + O(\log \text{poly}(|D|, t_d(n))) = 2q(n) + O(\log t_d(n) + \log |D|)$。

2.（**答案长度：**） [MNY21]中对此有所陈述；事实上，答案长度至多为 3 比特。

3.（**检查器运行时间：**） [MNY21 的表 5]给出了有效问题对的描述。据此可知，检查器需要运行原始博弈中的检查器 C，并进行一项额外检查，该检查的运行时间与证明者图灵机配置表中索引所占比特数呈线性关系。这便得到了所声称的运行时间。

4.（**判定器运行时间：**） [MNY21] 中指出，对于某个常数 γ，判定器的运行时间为 $\log^{\gamma} n$。

5. **(完备性、可靠性和纠缠界：)** 这些内容与[MNY21]中的陈述完全相同。

6. **(高效可计算性：)** 答案归约图灵机D 的描述由D 的代码以及答案归约变换（实质上是 Cook-Levin 归约）的代码组成，其大小为$O(1)$。对于检查器C^{ans}，根据 [MNY21 上有效问题对的描述，从表 5], 可知，C^{ans} 会在其输入的一部分上调用C，然后执行一项固定的额外检查，因此该图灵机的描述长度为 $|C| + O(1)$。对于Q^{ans}，这是因为答案归约验证器的问题长度可以从原验证器的问题长度高效计算得出。

□

4.1.3 无间隙压缩

通过组合问题约简和答案约简，可以得到一个无间隙压缩定理 [MNY21，定理 6。1]下面陈述我们得到的界。

定理 *44*。存在一台具有以下性质的图灵机 *GaplessCompress*。设 $G = (D, C, Q)$ 是一个具有复杂度界 $q(n)$、$a(n)$、$t_c(n)$、$t_d(n)$ 的游戏族，且 $t_c(n)$、$t_d(n) = poly(n)$。那么，在输入 (G, D, Q) 时，*GaplessCompress* 返回一个具有参数 $q'(n)$、$a'(n)$、$t'c(n)$、$t'd(n)$ 的游戏族 $G' = (D', C', Q')$ 的描述，使得

1.（问题长度：）$G'n$ 的问题长度为 $q'(n) = O(\log q(n) + \log t_d(n) + \log |D|)$。*2.*（答案长度：）$G'n$ 的答案长度为 $a'(n) = O(1)$。*3.*（检查器运行时间：）检查器运行时间为 $t'c(n) = O(\log n + \log t_d(n) + \log |D|)$。*4.*（判定器运行时间：）判定器运行时间为 $t'd(n) = poly\log(n)$。*5.*（完备性：）对于 G_n 的任意可预言化同步有限维策略 $\mathscr{S}$，存在一个 $G'n$ 的可预言化同步有限维策略 $\mathscr{S}'$，使得 $\omega_q(G'n, \mathscr{S}') \geq \frac{1}{2} + \frac{1}{2}\omega_q(G_n, \mathscr{S})$。*6.*（可靠性：）如果 $\omega^s_q(G_n) < 1$，那么 $\omega^s_q(G'n) < 1$。*7.*（纠缠界：）$\mathcal{E}(G'n) \geq max\{\mathcal{E}(G_n)$。*8.*（高效可计算性：）*GaplessCompress* 应在 $O(|D| + |C| + |Q|)$ 时间内运行。此外，$|D'| = |D| + O(1)$，$|C'| = |C| + O(1)$，且 $|Q'| = |Q| + O(1)$。

证明。 组合定理 42 和定理43。 □

4.2 无间隙超压缩

定理 *45*。设 $G = (GenG^{\prime}, N^{\prime})$ 是一个 n-索引 $AM^*_0(2)[q^{\prime}(\cdot), a^{\prime}(\cdot), t^{\prime}_c(\cdot), t^{\prime}_d(\cdot)]$ 协议。存在一台独立于 G 的图灵机 *GaplessHypercompress*，它以一对图灵机 $(GenG^{\prime}, N^{\prime})$ 的描述作为输入，并输出一对图灵机 $G^{\bullet\prime} = (GenG^{\bullet\prime}, N^{\bullet\prime})$ 的描述，具有以下性质：$G^{\bullet\prime}$ 是一个 n-索引 $AM^*_0(2)[Q_0, a^{\bullet\prime}(\cdot), t^{\bullet\prime}_c(\cdot), t^{\bullet\prime}_d(\cdot)]$ 协议，其中 $N^{\bullet\prime} = N^{\prime}$ 且

1. 问题长度：Q_0 a 为一个普适常数，使得对于所有 $\ell > Q0, \lceil 2\log \ell + 7 + + \log |\mathcal{X}_{MS}| \rceil < \ell$。*2.* 答案长度：对于任意 n，$a^{\prime}(n) = a^{\prime}(n) + \log^*(q^{\prime}(n))(q^{\prime}(n) + O(1))$。*3.* 检查器运行时间：对于任意 n，$t^{\bullet\prime}_c = O(1)$。*4.* 判定器运行时间：对于任意 n，$t^{\prime}(n) = t^{\prime}_d(n) + (|D^{\prime}| + |C^{\prime}| + |Q^{\prime}|)$ $poly$ $q^{\prime}(n)$。

5. 完备性： 设 z 为一个问题实例，设 $G^{\prime} = (D^{\prime}, C^{\prime}, Q^{\prime})$ 为 $GenG^{\prime}(z)$输出的游戏族，并设 $G^{\bullet\prime} = (D^{\bullet\prime}, C^{\bullet\prime}, Q^{\bullet\prime})$ 为 $GenG^{\bullet\prime}(z)$输出的游戏族。设 $G^{\prime}_n$ 为 $G^{\prime}$中的第 n 个族，$G^{\bullet\prime}$ 为 $G^{\bullet\prime}$中的第 n 个博弈。对于所有 n，如果 $G^{\prime}_n$ 具有博弈值为1 的可预言化有限维同步策略 $\mathscr{S}^{\prime}$，那么 $G^{\bullet\prime}_n$ 也具有博弈值为1 的可预言化有限维同步策略 $\mathscr{S}^{\bullet\prime}$。

6. 可靠性：对于所有 n，若 $\omega_q^s(G_n^\downarrow) < 1$，则 $\omega_q^s(G_n^\downarrow) < 1$ 也成立。

7. 纠缠界：对于所有 n，$\mathcal{E}(G_n^\downarrow) \geq \mathcal{E}(G_n^\downarrow)$。

证明。对于任意输入 z，$GenG^\downarrow$ 在输入 z 上运行 $GenG^\downarrow$，以生成一个判定器 $D^\downarrow$ 和一个检查器 $C^\downarrow$。$GenG^\downarrow$ 随后输出以下判定器 $D^\downarrow$ 和检查器 $C^\downarrow$ 的描述。

1. **检查器：**在输入 C x、y）时，忽略 n，并在输入 $(n^*$、x、$y)$ 上运行定理 42 中的检查器 C^{intro}，其中取满足 $q_{intro}(n^*) = Q_0$ 的 n^* 值。
2. **判定器：** 该判定器执行算法 1 中的算法。

```
1 输入：n、x、y、a、b
2 初始化 i := 0, ℓ_0 := q^↓(n), D^comp = D^↓, C^comp = C^↓, Q^comp = Q^↓。
3 当 ℓ_i > Q_0 时执行
4 |   (D^comp, C^comp, Q^comp) := GaplessIntro(D^comp, C^comp, Q^comp)
  |   /* GaplessIntro 在定理 42 中定义                                  */
5 |   ℓ_{i+1} := ⌈2对数 ℓ_i + 7 + 对数 |X_MS|⌉
6 |   i := i + 1
7 结束
8 运行 D^comp(n、x、y、a、b)。若接受则接受，否则拒绝。
```

伪代码1： 超压缩博弈。

检查器与判定器运行时间 显然，检查器 $C^\downarrow$ 在常数时间内运行。

为了界定判定器的运行时间，我们需要计算两项：（1）调用 GaplessIntro 的循环的运行时间；（2）在 n、x、y、a、b 上运行的最终判定器 D^{comp} 的运行时间。

首先请注意，每次调用 GaplessIntro 都会使 ℓ_{i+1} 相对于 ℓ_i 缩小一个指数因子：我们可以取足够大的 Q_0，使得对于所有 $\ell_i > Q0$，$\ell_{i+1} = \lceil 2\log \ell + 7 + \log |\mathcal{X}_{MS}| \rceil \leq 3 \log \ell_i$。令循环的迭代次数为 k。前述论证表明 $k = O(\log^*(q^\downarrow(n)))$，其中 $\log^*$ 是迭代对数。

现在，在每次迭代中，调用 GaplessIntro 所需的时间与 D^{comp}、C^{comp} 和 Q^{comp} 的描述长度成线性关系。根据定理 42 的第 8 项，每次调用 GaplessIntro 都会使 $D^\downarrow$、$C^\downarrow$ 和 $Q^\downarrow$ 的描述长度增加一个固定的加法常数，因此在第 i 次迭代时，$|D^i_{comp}| = |D^\downarrow| + ci$，$|C^i_{comp}| = |C^\downarrow| + ci$，$|Q^i_{comp}| = |Q^\downarrow| + ci$，其中 c 是某个常数。因此，循环中调用 GaplessIntro 所花费的总时间随以下量增长：

$$\sum_{i=1}^{k} (|D^\downarrow| + |C^\downarrow| + |Q^\downarrow| + 3ci) = O\left((\log^*(q(n)))^2 + \log^*(q(n)) \cdot (|D^\downarrow| + |C^\downarrow| + |Q^\downarrow|)\right).$$

现在我们来计算最终判定器的运行时间。根据定理 42 的第 4 项，当第 i 次应用 GaplessIntro 时，判定器的运行时间会增加 $t^{qs\,d}(\ell_i) + O(\log n)$。（定理 42 的第 4 项给出的界表明，应用一次压缩会使判定器的运行时间增加 $t^{qs\,d}(q_{intro}) + O(\log n)$；在算法 2 中，我们将每个 ℓ_i 设为第 i 次应用 GaplessIntro 所输出博弈的问题长度的上界。）因此，最终判定器的运行时间

有界于

$$\begin{aligned} t_d^{\downarrow}(n) =& t_a^{\downarrow}(n) + \sum_{i=1}^{k} (t_d^{qs}(\ell_i(n)) + O(\log n)) \\ \leq& t_a^{\downarrow}(n) + \sum_{i=1}^{k} (t_d^{qs}(\ell_0(n)) + O(\log n)) \\ \leq& t_a^{\downarrow}(n) + \log^*(q^{\downarrow}(n)) \cdot \mathrm{poly}(q^{\downarrow}(n)) \\ =& t_a^{\downarrow}(n) + \mathrm{poly}(q^{\downarrow}(n)). \end{aligned}$$

问题长度 循环终止时，我们可以保证 $\ell \leq Q_0$，而且 ℓ 是与D^{comp}相关联的博弈的问题长度。因此，问题长度至多为Q_0。

答案长度 循环运行 $k = O(\log^*(q^{\downarrow}(n)))$ 次迭代。因此，根据定理42的第2项，最终判定器的答案长度为

$$a^{\downarrow}(n) \leq a^{\downarrow}(n) + \sum_{i=1}^{k} (\ell_i(n) + O(1)) \leq a^{\downarrow}(n) + \log^*(q^{\downarrow}(n))(q^{\downarrow}(n) + O(1)).$$

完备性 这可通过反复应用定理42的第5项得到。

可靠性 这可通过反复应用定理42的第6项得到。

纠缠界 这可通过反复应用定理42的第7项，并（宽松地）将最大值下界估计为 $\mathcal{E}(G_n^{\downarrow})$得到。

□

定理 46。 存在一个以 n 为索引的 $\mathsf{AM}_0^*(2)[q = O(\log(n))$，一个 $= O(1)$，$t_c =$多对数(n)，$t_d =$多对数$(n)]$协议，用于 L。

证明。 该定理由对[MNY21]的主要结果应用一轮无间隙压缩得出。该工作明确证明，计算非局域游戏精确q-博弈值的问题是 Π_2-完全的。我们逐步追踪该归约，从而得到一个 $\mathsf{AM}_0^*(2)$ 协议，其界如所述（其中许多并未写入 [MNY21]的定理陈述中）。

根据n-索引 $\mathsf{AM}_0^*(2)$ 协议的定义（定义 15），这意味着我们必须找到一对图灵机$GenG^L$、N^L，使其满足以下性质（这里的表述略显非正式）：

- $GenG_L$ 接收输入z，并在 $\mathrm{poly}(|z|)$ 时间内输出图灵机D_z、C_z和Q_z 的描述，用以指定一个非局域游戏族。
- 当且仅当 $z \in L$ 时，游戏 $G = (DzN(|z|), CS\ N(|z|))$ 的博弈值为 $\omega q(G) = 1$；其问题、答案和运行时间复杂度分别按 $Qz(N(|z|)) = O(\log(|z|))$、$O(1)$ 和 $\mathrm{poly}(|z|)$ 缩放。

在 证明的其余部分中，我们将说明如何构造 $GenG^L$,N^L，以及为何其性质成立。

我们将首先通过追溯 [MNY21 引理 6.7]，为 L 构造一个 n 索引的 $\mathsf{AM}_0^*(2)$ 协议，其问题和答案长度均为多项式。给定一个实例z，定义可计算谓词$\phi(y,t)$：当且仅当图灵机M_x 在输入y 上运行t 个时间步后停机时，该谓词为真。则$z \in L$ 当且仅当以下Π_2^0 句子S 为真：

$$S = \forall y, \exists t \phi(y, t).$$

依照 [MNY21]，中的证明，对于每个 m，定义 Σ_1 句子（其中我们将自然数 $1, \ldots, m$ 视为二进制比特串，以便将它们作为 ϕ 的输入）

$$S_m = \exists t_1, \ldots, t_m \bigwedge_{i=1}^{m} \phi(i, t_i),$$

对于任意给定的 m，博弈 HaltingGame(S_m) $=(q_m=(m|S|)^{\lambda_{Halt}}, D_m, C_m)$ 是 [JNV+20] 中用于判定 Σ_1 = RE 句子 S_n 的博弈，其运行时间、问题长度和答案长度均由 $(m|S|)^{\lambda_{Halt}}$ 界定，其中 λ_{Halt} 是一个普适常数。此外，根据 [JNV+20 的定理 12.6]，游戏族 $\{\text{HaltingGame}(S_m)\}_m$ 实际上由三元组图灵机 (D, C, Q) 生成（按定义 13 的含义），其中 m 为索引；这些图灵机的运行时间为多项式时间，描述长度由 poly(|z|) 界定。（图灵机 Q 就是这样一台图灵机：它以 m 为输入，输出 $(m|S|)^{\lambda_{Halt}}$。

现在，将 SuperCompress [MNY21 定理 6.2] 应用于游戏族 (D, C, Q)，可得到一个游戏族 $G^{super}=(D^{super}, C^{super}, Q^{super})$、一个 $\lambda=O(\lambda_{Halt})$ 和一个 $\kappa=\text{poly}(|D|, |C|, \lambda_{Halt}+1, m0, \lambda^{\text{poly}(\lambda)})=\text{poly}(|z|, \lambda_{Halt})$，使得对于所有 $m \geq \kappa$，博弈 G_κ^{super}的博弈值为 1，当且仅当 HaltingGame(S_m) 的博弈值为 1。换言之，句子 S 为真，当且仅当博弈 G_κ^{super}的博弈值为 1。根据 [MNY21 定理 6.2]，D^{super}、C^{super}、Q^{super}的描述可由 D、C、Q 的描述在多项式时间内计算得到（因此所需时间为 poly(|z|)）。此外，根据 [MNY21 的证明中给出的 κ 的显式表达式，κ 可在时间 poly(|z|) 内计算。因此，给定 z，我们可以在时间 poly(|S|) 内计算 D_κ^{super}、C_κ^{super}、Q_κ^{super}的描述。此外，根据 [MNY21 定理 6.2], 的条目 1，D_κ^{super}、C_κ^{super}、Q_κ^{super}的运行时间至多为 $\kappa^\lambda=\text{poly}(|z|)$。

此时，我们已经为L构造了一个以n为索引的 $\text{AM}_0^*(2)[\text{poly}(n), \text{poly}(n), \text{poly}(n), \text{poly}(n)]$ 协议。为此，我们定义如下图灵机 $GenG^\circ$,N°：

- $GenG^\circ$ 首先解析输入 z，然后在 poly(|z|) 时间内计算出 D_{super}、C_{super} 和 Q_{super} 的描述。
- N° 使用上文提到的显式表达式计算 $\kappa(|z|)$。

然而，我们希望为L 获得一个以n为索引的 $\text{AM}_0^*(2)$ 协议，其问题复杂度为对数级，答案复杂度为常数 。为此，我们需要进行一轮无间隙压缩。无间隙压缩定理（定理 44）要求输入一个以n为索引的博弈序列；对于任意输入z，我们将$GenG^\circ(z)$ 的输出作为该序列。应用定理 44 后，我们得到一组三台新的图灵机$(D^{z,\downarrow}, C^{z,\downarrow}, Q^{z,\downarrow})$，使得

- 令 $G_{z,\downarrow n}$ 为由 $G_{z,\downarrow}=(D_{z,\downarrow}, C_{z,\downarrow})$ 定义的游戏族中的第 n 个博弈。$G_{z,\downarrow n}$ 的问题复杂度为 O(log n $+\log |D_{super}|)=O(\log n+\log |z|)$，答案复杂度为 O(1)。
- $D_{z,\downarrow n}$、$C_{z,\downarrow n}$和$Q_{z,\downarrow}$的运行时间有 poly log n 上界。
- 对于所有$n \geq n0$，$G_{z,\downarrow n}$ 都模拟G_{supern}。
- 可以根据D_{super}和C_{super}的描述，在多项式时间内计算$D_{z,\downarrow}$、$C_{z,\downarrow}$和$Q_{z,\downarrow}$的描述。

不失一般性，假设已选取 κ，使得 $\kappa(|z|) > n_0$。现在终于可以定义图灵机$GenG^\downarrow$,$N^\downarrow$，它们构成一个针对L 的、以n为索引的 AM^* 协议，且具有所需的复杂度界。

- $GenG^\downarrow$ 首先解析输入 z，并在时间 poly(|z|) 内计算 D_{super}、C_{super}、Q_{super} 的描述。接着，它在时间 $\text{poly}(|D_{super}|)=\text{poly}(|z|)$ 内计算 $D_{z,\downarrow}$、$C_{z,\downarrow}$、$Q_{z,\downarrow}$的描述，并将其作为输出返回。
- $N^\downarrow$ 计算 $\kappa(|z|)$（它与上文定义的 N 完全相同）。

输入 z 时，此协议执行的博弈恰好是博弈 $G_\kappa^\downarrow$。我们知道，$\omega_q(G_\kappa^\downarrow)=1$ 当且仅当$\omega_q(G_\kappa^{super})=1$，而这当且仅当 $z \in L$。因此，此协议判定 L。由上文讨论可得所声称的问题、答案和运行时间上界。

□

定理 *47.* 对于递归可枚举语言 L 中的完全语言，有一个 $AM_0^*(2)[q(n)=Q_0, a(n)=O(\log^*(\log(n)) \cdot \log(n)), t_c(n)=O(1), t_d(n)=O(n \log^*(n))]$ 协议，其中 Q_0 是定理 *45* 中的普适常数。

证明。 根据定理 46，我们知道L 具有一个n索引 $\mathrm{AM}_0^*(2)[\log(n), O(1), \mathrm{poly}(n)]$ 协议。应用定理 45 即得结论。 □

定理 48。 存在一个游戏族 G^{EPR}，其问题数 $q(n) = Q_0$，其答案大小 $a(n) = O(n)$，$t_c(n) = O(1)$，且 $t_d(n) =$ 多项式(n)，并且 $\mathcal{E}(G_n^{EPR}) = n$。

证明。 对来自 [MNY21]的问题采样应用定理 45。 □

5 自由纠缠游戏：有间隙情形

我们对有间隙情形的处理大体遵循无间隙情形的思路。为方便起见，本节沿用无间隙情形中类似的记号。例如，我们为有间隙超压缩定理得到的通用常数问题规模在此也记作Q_0，尽管它未必与无间隙情形中的常数相同。

5.1 细粒度有间隙压缩定理

5.1.1 有间隙问题约简

以下定义陈述了来自 [JNV+20的 7.3]泡利基测试的性质。

定义 49. 泡利基测试 PB_n 是一个游戏族，其问题长度为 $q_{PB}(n) =$多项式对数(n)，答案长度为 $a_{PB}(n) = O(n)$，采样器运行时间为 $t_s^{PB}(n) =$多项式对数(n)，判定器运行时间为 $t_d^{PB}(n) = O(n)$。

以下定理结合了 [JNV+20] 的内省定理和间隙放大定理。

定理 50. 存在一台图灵机 GappedIntro，具有以下性质。设 $G = (S,D)$ 是一个有间隙游戏族，其问题长度为 $q(n)$，答案长度为 $a(n)$，判定器运行时间为 $t_d(n)$，采样器运行时间为 $t_s(n)$，其中 $t_s(n),t_d(n) =$多项式(n)，且该采样器是一个 ℓ-级条件线性采样器，并满足 $\ell \le 10$。那么，GappedIntro 接收 S, D 的描述作为输入，并输出一个元组 (S^{intro}, D^{intro})，用于定义游戏族 G^{intro}，使其满足以下性质。

1. (问题长度：) 问题长度至多为 $q^{intro}(n) = \max\left(C\log^{\beta}(q(n)), C\log^{\beta}(q^*)\right)$，

其中 C、β、q^* 均为普适常数。*2.*（答案长度：）G_n^{intro} 的答案长度为 $O((a(n) + q(n) + O(1)) \cdot poly\ log\ q(n))$。*3.*（采样器：）采样器 S^{intro} 在输入 n 上计算 $q_{intro}(n)$，然后在输入 q 上运行通用采样器 $S^{intro,universal}$。后者的运行时间为 $poly\ log\ q(n) \cdot O(t_s^{PB}(q))$。因此，采样器的总运行时间为 $t_s^{intro}(n) = O(poly\ log\ q(n) \cdot t_s^{PB}(q(n)))$。采样器 S^{intro} 是一个 ℓ' 级条件线性采样器，具有 $\ell' = 5$。*4.*（判定器运行时间：）判定器 D^{intro} 的运行时间至多为 $t_d^{intro}(n) = (t_d(n) + t_d^{PB}(q(n)) + O(\log n)) \cdot poly\ log\ q(n)$。*5.*（完备性：）对于 G_n 的所有可预言化有限维同步策略，都存在一个 G_n^{intro} 的可预言化有限维同步策略，其博弈值至少同样高。*6.*（可靠性：）如果 $\omega_q(G_n) \le 1/2$，则 $\omega_q(G_n^{intro}) \le 1/2$。*7.*（高效可计算性：）$GappedIntro$ 的运行时间为 $O(|D| + |S|)$。此外，$|D^{intro}| = |D| + O(1)$ 且 $|S^{intro}| = |S| + O(1)$。

证明。 这个定理与 [JNV+20] 的内省定理有几处重大差异，下面将逐一详述。为使记号清晰，我们将 [JNV+20] 中构造的内省游戏称为 $G^{BareIntro}$，以便与本定理中构造的内省游戏区分开来。

- **参数**在 [JNV+20] 中，内省定理是在“放大”设置下陈述的（如第4.1节所述）：博弈 $G_{BareIntron}$ 的博弈值与 G_N（其中 $N = 2^n$）的博弈值相关。相比之下，本文将在“缩小”设置下工作：我们希望将 G_{intron} 与 G_n 联系起来。

- **λ-有界性**在 [JNV+20] 中，假设要进行压缩的博弈 G 是“λ-有界”的：G_n 的问题长度、答案长度和运行时间均假设由 n^λ 所界定，而内省博弈的复杂度则用 n 和 λ 来表示。压缩过程需要将 λ 作为输入，以确定用于采样问题的泡利基测试实例的大小。这里采用这种表述，便于讨论博弈压缩映射的不动点，但对我们而言并不充分，因为我们希望问题长度和答案长度能够分别伸缩。因此，我们不指定指数 λ，而是要求采样器S 高效计算 $q(n)$（运行时间为 $t_S(n)$）。压缩过程将运行 S，以确定要运行的泡利基测试实例的大小。

- **平行重复：** [JNV+20] 中的内省博弈并非“间隙保持”。相反，它具有以下可靠性保证：若 $\omega_q(G_{BareIntron}) \geq 1-\varepsilon$，则 $\omega_q(G_n) \geq 1-\delta(\varepsilon,n)$。为了得到 $\delta \leq 1/2$，我们必须令 ε 为关于n 的一个趋于零的函数。

  我们将通过对游戏$G^{BareIntro}$进行平行重复来解决这一问题。 [JNV+20] 也使用平行重复来放大可靠性间隙。遗憾的是，直接应用 [JNV+20] 中使用的 [BVY17] 强锚定并行重复定理，对我们来说并不足够。这是因为该定理给出的界依赖于游戏的答案长度；当k 小于答案长度时，这个界就会变得毫无意义。在我们的设定中，k 必须只依赖于问题长度。因此，我们转而采用较早的 [DSV15], 平行重复界，该界适用于投影游戏。正如 [DSV15], 中所指出的，我们可以通过预言机化将任意游戏转换为投影游戏，且可靠性间隙只付出常数因子的代价。（预言机化并不总能保持完备性；但在我们的情形下可以，因为我们假设输入游戏在完备性情形下具有完美可预言机化策略。）游戏经过预言机化后， [DSV15] 的结果告诉我们，只要取足够多次重复k，若 $\omega_q(G_n^{BareIntro}) \leq 1-\varepsilon(n)$，则 $\omega_q((G^{BareIntro}_{,n} \quad ^{orac})^{\otimes k}) \leq 1/2$，正如所需。

我们不再详细描述内省游戏 $G^{intro} = (S^{intro}, D^{intr}$ 的构造， $^{o})$ 并证明 定理中所声称的性质。

裸内省： 我们首先按照 [JNV+20 的第 8], 节进行一种内省，但作出以下修改

- **采样器：** 采样器设置 $R = q(n)$（而不是 $R = N^\lambda$；后者由它调用$S(n,$ 维度$)$计算得出）。

- **判定器：** 判定器设置 $N = n$（而非 2_n），且不会中止或超时。

预言机化： 接下来，我们执行一种改进版的预言机化，该版本基于[JNV+20第 9] 节中的版本。唯一的区别在于类型图：我们移除了类型 A 和 B 之间的边。这意味着得到的博弈是一个投影游戏：要么两位玩家收到相同的类型，此时他们必须返回相同的答案；要么一位玩家收到预言机类型，另一位玩家收到 A 或 B 类型，此时前者的答案唯一确定了后者的正确答案。

平行重复： 最后，我们按照 [JNV+20 第 11], 节所述执行平行重复，但不进行锚定变换。为了计算所需的重复次数，我们必须回顾裸内省过程的可靠性。以下陈述给出了这一点：如果 $\omega_q(G_n^{BareIntro}) \geq 1-\varepsilon$，那么

$$\omega_q(G_n) \geq 1-\delta(\varepsilon,n), \qquad \delta(\varepsilon,n) = a((\log q(n))^a \varepsilon^b + (\log q(n))^{-b}), \tag{12}$$

其中 > 0 a 和 b $0 <$ b < 1 是仅取决于 ℓ 的常数。（就我们而言，界 $\ell \leq 10$ 已经固定，因此可以将 a 、 b 取为普适常数。）设 ε(n) 是一个函数，使得对于所有 n $\in \mathbb{N}$，只要 q(n) $> q^* \forall$n，就有 $\delta(\varepsilon$(n), n)$< \frac{1}{2}$；其中 q^* 是一个仅取决于 b 的普适常数。注意，可以选择 ε(n)，使得 $1/\varepsilon$(n) $\leq$ poly log(q(n))。（假设 q(n) $> q^* \forall$n 不失一般性，因为我们总可以在开始之前将问题填充到超过某个常数长度。）我们希望找到一个 k，使得如果 $\omega_q(G_n^{BareIntro}) < 1-\varepsilon$(n)，那么

$\omega_q\left(\left(G^{BareIntro}、_n \quad ^{orac}\right)^{\otimes k}\right) < \frac{1}{2}$；这将意味着，如果 $\omega_q\left(\left(G^{BareIntro}、_n \quad ^{orac}\right)^{\otimes k}\right) \geq \frac{1}{2}$，那么 $\omega_q\left(G_n^{BareIntro}\right) \geq 1-\varepsilon(n)$，进而意味着 $\omega_q(G_n) \geq 1-\delta(\varepsilon(n)、n) \geq \frac{1}{2}$。

现在， [DSV15] 的结果表明：存在普适常数C、c，使得

$$\begin{aligned}\omega_q((G_n^{BareIntro,orac})^{\otimes k}) &\leq (1-C(1-\omega_q(G_n^{BareIntro,orac}))^c)^{k/2} \\ &\leq (1-C(\varepsilon)^c)^{k/2} \\ &\leq \exp\left(-C(\varepsilon)^c \cdot \frac{k}{2}\right),\end{aligned}$$

其中，最后一步用到了对所有$n > 0$，$(1-\varepsilon)^n \leq \exp(-\varepsilon n)$。若我们选择$k$使得

$$k \geq \frac{2\log 2}{C}\varepsilon^{-c} = \mathrm{poly}(\log q(n)), \tag{13}$$

那么，$\omega_{q((G^{BareIntro},_n \quad ^{orac})^{\otimes k})} \leq 1/2$，正如所需。

对于这个k的取值，所得博弈$(G^{BareIntro},^{orac})^{\otimes k}$就是内省游戏$G^{intro}$。下面说明如何证明定理陈述中声称的性质。

- **问题长度：**裸内省游戏的问题长度为$O(\log q(n))$。预言机化会使其增加一倍，平行重复则会使其增加$k(n) = \mathrm{poly}\log q(n)$倍，最终问题长度为$\mathrm{poly}\log q(n)$。

- **答案长度：**裸内省游戏的答案长度为$q(n)+a(n)+O(1)$。预言机化和平行重复会使其增加$\mathrm{poly}\log q(n)$倍，最终答案长度为$O((q(n)+a(n)+O(1))\cdot \mathrm{poly}\log q(n))$。

- **采样器：** 该采样器本质上需要并行运行$k(n)$份裸内省采样器的预言机化版本。每份所需时间为$O(t_{PBs}(q(n))+O(1))$，因此总运行时间为$O(\mathrm{poly}\log q(n)\cdot t_{PBs}(q(n)))$。

- 判定器运行时间：裸内省判定器的运行时间为 $\mathrm{td(n)} + \mathrm{tPBd\ (n)} + \mathrm{O(log\ n)}$，其中 tPBd (n) 是泡利基测试的判定器运行时间，而 O(log n) 来自 Q 的运行时间。总运行时间等于裸运行时间乘以重复次数，即 $\mathrm{poly\ log\ q(n)}$。因此，总运行时间为 $\mathrm{poly\ log\ q(n)}\cdot(\mathrm{td(n)} + \mathrm{tPBd\ (n)} + \mathrm{O(1)})$。

- **完备性：** 这是裸内省的完备性、预言机化和平行重复的直接推论。

- **可靠性：** [JNV+20] 中裸内省的可靠性分析给出了一个关于n的界，与问题长度无关。然而，通过考察[JNV+20第 8 节中的可靠性论证，我们看到，可靠性函数 $\delta(\varepsilon,n)$ 仅取决于 ε 和 $R(n)$，后者是待压缩问题的随机种子的比特长度。事实上，我们有

$$\delta(\varepsilon,n) = a((\log R(n))^a\varepsilon^b + (\log R(n))^{-b}).$$

在我们的设定中，$R(n) = q(n)$，从而得到方程（12）中所述的可靠性界。

因此，根据裸内省的可靠性，如果 $\omega_q\mathrm{(G)} \leq 1/2$，那么 $\omega_q(\mathrm{G}^{BareIntro}) \leq 1-\varepsilon\mathrm{(n)}$；进而，根据预言机化的可靠性，$\omega_q(\mathrm{G}^{BareIntro,orac}) \leq 1-2\varepsilon\mathrm{(n)}$。结合 [DSV15] 的平行重复定理以及 k(n) 的选取，可知，如果 $\omega_q(\mathrm{G}^{intro}) \leq (1-\mathrm{C}(2\varepsilon(\mathrm{n}))^c)^{k/2} \leq 1/2$，则结论成立。

- **高效可计算性：** 这可以通过检查G^{intro}的采样器和判定器得出。

□

5.1.2 间隙答案缩减

定理 *51*。存在一台名为 *GappedAnsReduce* 的图灵机，具有以下性质。设 $G = (S, D)$ 是一个游戏族，其复杂度界分别为 $q(n)$、$a(n)$、$t_s(n)$、$t_d(n)$，其中 $a(n) \leq t_d(n)$ 且 $q(n) \leq t_s(n)$，并且 (S, D) 是一个 ℓ 级标准形验证者。那么，*GappedAnsReduce* 接收 S、D 的描述作为输入，并输出一个游戏族 $G^{ans} = (S^{ans}, D^{ans})$ 的描述，使得对于游戏族 G^{ans} 以及所有 $n \geq 2$，我们有

1.（条件采样器：）(S^{ans}, D^{ans}) 是一个 $max(\ell + 2, 5)$ 标准形验证者。*2.*（问题长度：）问题长度为 $q^{ans}(n) = poly(t_s(n), log(t_d(n)), log|D|)$，其中 $|D|$ 是图灵机 D 的描述长度。*3.*（答案长度：）答案长度为 $a^{ans}(n) = poly(log(t_d(n)), log(|D|))$。*4.*（采样器运行时间：）采样器运行时间为 $poly(t_s(n), t_d(n), |D|)$。如果 S 是一个 ℓ 级条件线性采样器，那么采样器 S^{ans} 是一个用于 $\ell' = max(\ell + 2, 5)$ 的 ℓ' 级条件线性采样器。*5.*（判定器运行时间：）判定器运行时间为 $poly(t_s(n), t_d(n), |D|)$。*6.*（完备性：）如果 G_n 有一个博弈值为 *1* 的有限维可预言化同步策略，那么 G_n^{ans} 有一个博弈值为 *1* 的有限维可预言化同步策略。*7.*（可靠性：）如果 $\omega_q^s(G^{ans}) \geq 1 - \varepsilon$，那么 $\omega_q^s(G_n) \geq 1 - \delta(\varepsilon, n)$，其中 $\delta(\varepsilon, n) = a((\log t_d(n) + \log|D|)^a \varepsilon^b + (\log t_d(n) + \log|D|)^{-100b})$，$a$ 是一个普适常数，满足 $a > 0$，b 是一个普适常数，满足 $0 < b < 1$。*8.*（高效可计算性：）*GappedAnsReduce* 的运行时间为 $O(|D| + |S|)$。此外，$|D^{ans}| = |D| + O(1)$，且 $|S^{ans}| = |S| + O(1)$。

证明。这个定理本质上是 [JNV+20 中的定理 10，27], 但对 $|D|$ 的依赖更好。这是通过采用一种略有不同的概率可检验证明构造得到的，该构造更适合我们的“缩小规模”设定：我们设想将答案大小从多项式级降至多对数级，同时不缩短判定器的运行时间。这与 [JNV+20] 中的情况形成对比：其中答案约简将索引 n 上的答案大小从指数级降至多项式级，同时也将判定器的运行时间从指数级降至多项式级。我们将使用的概率可检验证明构造略有不同，因此先简要回顾放大规模情形。

放大规模情形：回顾 在 [JNV+20] 中，为了进行答案约简，首先对指数运行时间的判定器应用库克-列文定理，构造一个简洁电路可满足性问题的实例。该实例由另一个电路 $\mathcal{C}$ 指定，该电路由 $s = \text{poly}(|D|)$ 个门组成，并接收多项式多个输入，这些输入标记为 x、o。然后，使用 Tseitin 变换和一些额外的构造组件（如 [JNV+20 第 10.3] 节所述），将该电路转换为一个 5-SAT 公式 $\mathcal{F}(x, o, w)$，其中 $w \in \mathbb{F}_q^s$。在这一变换中，我们需要添加 s 个新变量，并将它们标记为 w——本质上每条电路线路对应一个变量——以使每个变量的次数保持为常数。原始的简洁电路可满足性问题实例可满足，当且仅当以下条件成立：

$$\forall x, o, \exists w \mathcal{F}(x, o, w) = 1.$$

为检验这一点，[JNV+20] 中将答案化简后的判定器计算了 $\mathcal{F}$ 的算术化表示，并将其转换为多项式 $\mathcal{F}_{arith}$：$\mathbb{F}^{m'}{}_q$，其中 m' 是变量 x、o、w 的总数。将子集 $H \subset \mathbb{F}_q$ 与 $\{0,1\}$ 对应起来，$\mathcal{F}_{arith}$ 在 $H^{m'}$ 上的取值恰好等于布尔公式 $\mathcal{F}$ 在 $\{0,1\}^m$ 中各布尔赋值上的取值。

现在，为了检验所需的谓词，判定器要求证明者计算低次多项式$g_1, \ldots\ldots, g_5$，以编码对w变量的赋值。它对这些多项式以及一些额外的低次多项式进行查询，以证明

$$\mathcal{F}_{arith}(x, o, w)(g_1(x) - o_1) \ldots (g_5(x) - o_5).$$

次数较低，并且在$H^{m'}$上恒等于 0。

缩小设定 在我们的设定中，我们改为从一个多项式时间判定器出发，并将使用库克-列文定理把它转换为一个电路可满足性实例。给定一个电路 $\mathcal{C}$，我们像之前一样构造一个 5-SAT 公式 $\mathcal{F}(a,b,w)$。不过，现在我们想要检验的谓词只是

$$\exists a,b,w\mathcal{F}(a,b,w)=1.$$

公式 $\mathcal{F}$ 是若干子句的合取，每个子句至多依赖来自块 a、b、w_1,w_2,w_3的各一个变量。

现在我们将把这个公式转换为多项式。先固定一个域 $\mathcal{F}_q$（其大小 q 稍后确定），并定义 H 为与 $\{0,1\}$ 相关联的 $\mathbb{F}_q$ 中的两个点。定义多项式 ϕ 如下：

$$\phi(x_1,x_2,\ldots,x_5,o_1,o_2,\ldots,o_5)=\begin{cases}1 & \text{if } a_{x_1}^{o_1}\vee b_{x_2}^{o_2}\vee w_{1,x_3}^{o_3}\vee w_{2,x_4}^{o_4}\vee w_{3,x_5}^{o_5} \text{ is a clause in } \mathcal{F}\\ 0 & \text{otherwise}\end{cases},$$

其中 x_1,。 $\ldots,x_5$是 $[n]$ 中的索引，对应于子立方体 H^m上的点。为显式构造 ϕ，回顾指示多项式

$$\begin{aligned}\mathrm{ind}_{m,y}(x)&=\begin{cases}1 & \text{if } x=y\\ 0 & \text{otherwise}\end{cases} &(14)\\ &=\prod_{i:y_i=1}x_i\prod_{i:y_i=0}(1-x_i). &(15)\end{aligned}$$

这个多项式对每个变量的单变量次数均为 1（因此总次数为 m）。利用这一点，我们可以将 ϕ 写成若干项之和，每一项都是分别关于 a、b、w_1,w_2,w_3,o_1,。 $\ldots,o_5$变量的 10 个指示函数的乘积。总体而言， ϕ 对每个变量的单变量次数均为 1，总次数为 $5m+5$。

公式 $\mathcal{F}$可满足，当且仅当对于所有 $x_1,\ldots,x_5\in H^m$ 以及 $o_1,\ldots,o_5\in H$,

$$c_0(x_1,\ldots,x_5,o_1,\ldots,o_5)=\phi(x_1,\ldots,x_5,o_1,\ldots,o_5)\cdot(g_1(x_1)-o_1)(g_2(x_2)-o_2)\ldots(g_5(x_5)-o_5)$$

其值等于 0。也可以通过子立方体上为零测试来验证：我们检查 g 是否属于在 H^{5m+5} 上为零的多项式理想，方法是要求将其表示为该理想生成元的线性组合。具体而言，如果我们可以写成

$$c_0(z)=\sum_{i=1}^{5m+5}c_i(z)\cdot\mathrm{zero}(z_i),$$

其中 $z\in\mathbb{F}_q^{5m+5}$是 $5m+5$ 个变量 $x_1,\ldots,x_5,o_1,\ldots,o_5$,的简写；每个 $c_i(z)$ 都是次数适当的任意多项式，d 而 $\mathrm{zero}(\cdot)$ 是一个在 H上为零的固定单变量多项式，那么我们就证明了 c_0 在 $H^{m'}$上为零。子立方体上为零测试通过在 $\mathbb{F}_q^{5m+5}$中的随机点和子空间上查询 c_0和 c_i 来完成。

参数设置 设 $G=(S、D、Q)$ 是我们希望对其执行答案约简的游戏族，设 $q(n)$、$a(n)$、$t_S(n)$、$t_d(n)$ 是其复杂度界。现在我们将为概率可检验证明选择参数，以执行答案约简。

首先，对判定器 D 应用库克-列文定理，可得到一个 5-SAT 实例，其中包含 $s=\mathrm{poly}(t_d(n),|D|)$ 个变量和子句。（有关库克-列文归约的详细描述，请参见 [JNV+20]；注意，此处我们不需要所得公式的简洁表示。）

接下来，我们必须如下选择概率可检验证明参数 q、m、m'、d。我们将令 γ 为一个自然数值参数，稍后再设置；我们将用它按需调整可靠性。并令a、b 为普适常数，这些常数将在下文定义 δ_{LD}时给出。

1. Let $m=\lceil\log s\rceil=O(\log t_d(n)+\log|D|)$.
2. 令$m'=5m+5$。

3. 令$q = 2^k$ 其中k 是满足以下条件的最小奇数 的：

$$k \leq \gamma m \tag{16}$$

$$2^{-kb} \leq m^{-(\gamma b)} \tag{17}$$

$$km'/2^k \leq m^{-b\gamma}, \tag{18}$$

且 2^k 可被m'整除

4. 令$d = k$。

注意，从渐近意义上看，这给出$d = k = O(m) = O(\log t_d(n) + \log |D|)$。要计算该 PCP 的可靠性，我们需要低次测试的可靠性函数，其定义如下

$$\delta_{LD}(\varepsilon, q, m, d, r) = a(dmr)^a(\varepsilon^b + q^{-b} + 2^{-bmd}). \tag{19}$$

这意味着，对于域大小q、含m 个变量、单变量次数为d的r-同步低次测试的任意策略，其成功概率 $1-\varepsilon$ 都可以舍入为一种策略，使其从 $\mathbb{F}_q^m$上单变量次数为d的r 个多项式构成的元组中进行采样；舍入造成的误差为 δ_{LD}。采用上述参数后，我们有：

$$\delta_{LD}(\varepsilon, q, m', d, m'+6) = a(dm'(m'+6))^a(\varepsilon^b + q^{-b} + 2^{-bm'd}) \tag{20}$$

$$\leq a(dm'(m'+6))^a(\varepsilon^b + q^{-b}) \tag{21}$$

$$\leq a(c\gamma m^3)^a(\varepsilon^b + q^{-b}) \tag{22}$$

$$\leq a(c\gamma)^a(m^{3a}\varepsilon^b + m^{3a}m^{-(3a+\gamma b)}) \tag{23}$$

$$= a(c\gamma)^a(m^{3a}\varepsilon^b + m^{-\gamma b}), \tag{24}$$

其中c 是某个普适常数。这里，从第一行到第二行，我们用到了$2^{m'd} = 2^{m'k} \geq 2^k = q$。从第二行到第三行，我们用到了公式（16）。从第三行到第四行，我们用到了公式（17）。

问题、答案和测试的运行时间复杂度 答案归约验证器根据原始博弈G的问题分布计算出一对问题(x,y)，并将它们发送给证明者。对于特定的(x,y)，答案归约验证器随后会向概率可检验证明查询由x、y诱导的判定谓词。这些查询包括对上文定义的多项式c_0和$c_1, \ldots\ldots$、$c_{m'}$的查询，以及对查询多项式$g_1, \ldots\ldots$、g_5的查询；后者应当是字符串a、b、w_1,w_2,w_3的低次扩展。总计有$m'+1+5 = m'+6$ 个定义在 $\mathbb{F}^{m'}{}_q$ 上的多项式，每个变量的单变量次数至多为d。问题和答案的复杂度主要由对这$m'+6$ 个多项式同时进行的低次测试决定。

在此测试中，问题大小（以比特计）为

$$q^{ans}(n) = q(n) + O(m' \log q) = \mathrm{poly}(t_s(n), \log t_d(n), \log |D|),$$

这里使用了原始博弈的问题长度$q(n)$ 不超过采样器运行时间$t_s(n)$这一上界。答案大小为$O((m'+6) \cdot (d+1) \cdot \log q)$——指定$m'+6$ 个次数至多为d的单变量多项式的$\mathbb{F}_q$值系数所需的比特数。其增长规模为

$$a^{ans}(n) = O(m^3) = \mathrm{poly}(\log t_d(n), \log |D|).$$

对于判定器运行时间，答案归约判定器必须首先计算针对原始判定器 D 通过 Cook-Levin 归约生成的 SAT公式。这需要 poly(|D|, $t_s(n)$, $t_d(n)$) 的时间。接下来，答案归约判定器对该 SAT公式执行 PCP验证器以及低次测试。这需要 poly(|D|, $t_d(n)$, m′, d, log q) 的时间。因此，判定器的总运行时间按 poly($t_s(n)$, $t_d(N)$, |D|) 的规模增长。对于采样器运行时间，也可以得到类似的界。

可靠性分析 在我们修改后的答案约简中，我们执行了与 [JNV+20 第 7], 节相同的测试，但采用了修改后的多项式 c_0, 定义，并且不使用 w 变量。通过适当调整参数，大部分可靠性分析都可以复用。特别地，在 [JNV+20 定理 10.27]的可靠性部分证明中，已经证明：对于答案归约游戏中以概率 $1-\varepsilon$ 获胜的任意策略，都可以得到原始博弈中以概率 $1-\delta$ 获胜的策略，其参数为 $\delta = O((\delta_{LD}(\varepsilon,q,m',d,m'+6)^{1/2} + (m'd/q))^{1/2})$。在我们的参数设置下，这给出

$$\begin{aligned}\delta &\le \left(Ca^{1/2}(c\gamma)^{1/2}(m^{3a}\varepsilon^b + m^{-\gamma b})^{1/2} + \left(\frac{m'd}{q}\right)^{1/2}\right)^{1/2} \\ &\le \left(Ca^{1/2}(c\gamma)^{1/2}(m^{3a}\varepsilon^b + m^{-\gamma b})^{1/2} + m^{-\gamma b/2}\right)^{1/2} \\ &\le \left(2Ca^{1/2}(c\gamma)^{1/2}m^{1.5a}\varepsilon^{0.5b} + (2Ca^{1/2}(c\gamma)^{1/2}+1)m^{-\gamma b/2}\right)^{1/2} \\ &\le 4C^{1/2}(ca\gamma)^{1/4}m^{0.75a}\varepsilon^{0.25b} + 2(2C(ca\gamma)^{1/2}+1)^{1/2}m^{-0.25\gamma b}.\end{aligned}$$

其中，从第一行到第二行时，我们使用了方程（18）；在后续步骤中，我们使用了 $\sqrt{x}+y \le 2(\sqrt{x}+\sqrt{y})$。若令 $\gamma = 100$，并回想起 $m = O(\log t_d(n) + \log|D|)$，这便具有定理所述的形式。

高效可计算性 新采样器 S^{ans} 生成来自 S 的问题对，以及答案归约验证器执行低次测试时所用的问题对。生成这些额外问题的图灵机的描述长度为 $O(1)$，因此S^{ans} 的总描述长度为 $|S|+O(1)$。同样，对于判定器，答案归约判定器会计算原始判定器 D 所求值的布尔电路，应用 Cook-Levin 归约将其转换为 SAT 公式，然后执行相应的概率可检验证明验证器。执行这些步骤的图灵机的描述长度为 $|D|+O(1)$。S^{ans} 和D^{ans} 都可以通过将S、D 的描述与常数长度的字符串拼接来计算，因此 GappedAnsReduce 所声称的运行时间上界随即成立。

□

定理52。 存在一台具有以下性质的图灵机GappedAnsPR 。设 $G = (S,D)$ 是一个有间隙游戏族，其问题长度为 $q(n)$，答案长度为 $a(n)$，判定器运行时间为 $t_d(n)$，采样器运行时间为 $t_s(n)$，其中 $t_s(n),t_d(n) = \mathrm{poly}(n)$，且采样器是一个具有 $\ell \le 10$ 的 ℓ 级条件线性采样器。给定 S,D 的描述后，GappedAnsPR 输出一个三元组 S^{ansPR},D^{ansPR}，用于定义一个游戏族 G^{ansPR}，并满足以下性质。

令 $q^{ans}(n)$ 按照定理 *51* 中的方式，根据 $t_s(n),t_d(n),|D|$ 来定义。令 $k(n)$ 为一个满足 $k(n) = \mathrm{poly}(\log t_d(n) + \log|D|)$ 的参数。

*1. (*问题长度：*)* 问题长度上界为 $q^{ansPR}(n) = k(n)\cdot\mathrm{poly}(t_s(n),\log(t_d(n)),\log|D|)$。

*2. (*答案长度：*)* G_n^{ansPR}的答案长度为 $k(n)\cdot\mathrm{poly}(\log(t_d(n)),\log(|D|))$。

*3. (*采样器：*)* 采样器的总运行时间为 $t_s^{ansPR}(n) = k(n)\cdot\mathrm{poly}(t_s(n),t_d(n),|D|)$。若 S 是一个 ℓ-级条件线性采样器，则采样器 S^{ansPR} 是一个 ℓ'-级条件线性采样器，其中$\ell' = \max(\ell+4,7)$。

*4. (*判定器运行时间：*)* 判定器 D^{ansPR} 的运行时间上界为 $t_d^{ansPR}(n) = k(n)\cdot\mathrm{poly}(t_s(n),t_d(n),|D|)$。 *5. (*完备性：*)* 若存在一个可预言化有限维同步策略，使其在 G_n 上的博弈值为1，则存在一个可预言化有限维同步策略，使其在 G_n^{ansPR}上的博弈值为1。 *6. (*可靠性：*)* 若 $\omega_q(G_n)\le\frac{1}{2}$，则 $\omega_q(G_n^{ansPR})\le\frac{1}{2}$。

7.（高效可计算性：）GappedAnsPR 的运行时间为 $O(|D|+|S|)$。此外，$|D^{ansPR}| = |D|+O(1)$，且 $|S^{ansPR}| = |S|+O(1)$。

证明。该定理是将 [DSV15] 的平行重复应用于定理 51 得到的。具体而言，给定定理 51 输出的三元组 (S^{ans}, D^{ans})，令 $\varepsilon \geq 0$ 使得 $\omega_q(G_n^{ans}) \leq 1-\varepsilon$。我们将 [DSV15] 的平行重复应用于该博弈，其中重复次数 k按定理陈述中的设定取值。这会直接使问题和答案长度、采样器以及判定器运行时间都乘以 k。为了得到所声称的可靠性界，注意到 [DSV15] 给出

$$\omega_q((G_n^{ans})^{\otimes k}) \leq (1 - C \cdot (1-\omega_q(G_n^{ans}))^c)^{k/2} \tag{25}$$
$$\leq (1 - C \cdot (\varepsilon)^c)^{k/2} \tag{26}$$
$$\leq \exp\left(-C(\varepsilon)^c \cdot \frac{k}{2}\right), \tag{27}$$

其中C、c 是普适常数。

与内省情形一样，我们需要处理这样一个事实：答案约简不是间隙保持的。更确切地说，它具有以下可靠性保证：如果 $\omega_q(G_n^{ans}) \geq 1-\varepsilon$，那么存在常数$a > 0$、$0 < b < 1$，使得

$$\omega_q(G_n) \geq 1 - \delta(\varepsilon, n), \qquad \delta(\varepsilon, n) = a((\log t_d(n) + \log|D|)^a \varepsilon^b + (\log t_d(n) + \log|D|)^{-100b}). \tag{28}$$

设 $\varepsilon(n)$ 是一个满足以下条件的函数：对所有$n \geq 2$，$\delta(\varepsilon(n), n) < \frac{1}{2}$。不失一般性地，我们可以假设这样的 $\varepsilon(n)$ 通过填充D 的运行时间，使得 $\delta(0,2) < 1/2$，总是可以得到。

注意，可以选择 $\varepsilon(n)$，使得 $1/\varepsilon(n) \leq \mathrm{poly}(\log t_d(N) + \log|D|)$。我们希望找到一个 k，使得如果 $\omega_q(G_n^{ans}) < 1-\varepsilon(n)$，那么 $\omega_q\left((G_n^{ans})^{\otimes k}\right) < \frac{1}{2}$；这将意味着，如果 $\omega_q\left((G_n^{ans})^{\otimes k}\right) \geq \frac{1}{2}$，那么 $\omega_q(G_n^{ans}) \geq 1-\varepsilon(n)$，进而意味着 $\omega_q(G_n) \geq 1-\delta(\varepsilon(n), n) \geq \frac{1}{2}$。利用公式（27），我们看到，如果选择 k(n) 使得

$$k(n) \geq \frac{2\log 2}{C}\varepsilon(n)^{-c} = \mathrm{poly}(\log t_d(n) + \log|D|), \tag{29}$$

那么 $\omega_q((G_n^{ansPR})^{\otimes k}) \leq 1/2$，正如所需。这正是定理陈述中$k(n)$ 所对应的情形。

还需证明两点：采样器的层数以及高效可计算性。关于前者，[JNV+20 的定理 11.4] 证明，若答案约简后的采样器有 ℓ' 层，则平行重复后的采样器有 $\ell' + 2$ 层，因此可由定理 51 中关于层数的界得出结论。关于高效可计算性，这是因为G^{ansPR} 的描述由G^{ans} 的描述以及生成平行重复的代码组成，而后者的大小为$O(1)$。

□

5.1.3 有间隙压缩

通过组合问题约简（定理 50）和平行重复后的答案约简（定理52），可以得到一个有间隙压缩定理。下面给出所得的界。

定理 *53*。存在一台具有以下性质的图灵机 *GappedCompress*。固定一个普适常数 q^*。设 $G = (S, D)$ 是一个复杂度界分别为 $q(n)$、$a(n)$、$t_s(n)$、$t_d(n)$ 的游戏族，且 $q(n) > q^* \; \forall n \in \mathbb{N}$。那么，在输入 (S, D) 时，*GappedCompress* 返回一个参数为 $q'(n)$、$a'(n)$、$t's(n)$、$t'd(n)$ 的游戏族 $G' = (S', D')$，使得

1. (问题长度：) $G'n$ 的问题长度为

$$q'(n) = \mathrm{poly}(\log q(n) \cdot t_s^{PB}(q(n)),\ \log t_d(n),\ \log t_d^{PB}(q(n)),\ \log|D|,\ \log\log n).$$

2. (答案长度：) $G'n$ 的答案长度为

$$a'(n) = \mathrm{poly}(\log\log q(n),\ \log t_d(n),\ \log t_d^{PB}(q(n)),\ \log|D|,\ \log\log n).$$

3. (采样器：) 采样器运行时间为

$$t'_s(n) = \mathrm{poly}(\log q(n) \cdot t_s^{PB}(q(n)),\ t_d(n),\ t_d^{PB}(q(n)),\ |D|,\ \log n).$$

如果 S 是 ℓ 级条件线性的，且满足 $\ell \le 10$，那么 S' 是条件线性的，且满足 $\ell \le 9$。

4. (判定器运行时间：) 判定器运行时间为

$$t'_d(n) = \mathrm{poly}(\log q(n) \cdot t_s^{PB}(q(n)),\ t_d(n),\ t_d^{PB}(q(n)),\ |D|,\ \log n).$$

5. (完备性：) 如果存在一个可预言化有限维同步策略，使 G_n 的博弈值1，则存在一个可预言化有限维同步策略，使 G_n^{ansPR} 的博弈值1。

6. (可靠性：) 如果 $\omega_q(G_n) < \frac{1}{2}$，那么 $\omega_q(G'n) < \frac{1}{2}$。

7. (高效可计算性：) GappedCompress 的运行时间为 $O(|D| + |S|)$。此外，$|D'| = |D| + O(1)$，且 $|S'| = |S| + O(1)$。

证明。 结合定理 50 和定理52。参数变化如下。

- (问题长度：) 回想一下，k(n) = poly(log tintrod (n) + log |Dintro|) = poly(log td(n) + log tPBd (q(n)) + log log(n) + log log q(n) + log |D|)。问题长度为

$$\begin{aligned} q'(n) &= k(n) \cdot \mathrm{poly}(t_s^{intro}(n), \log(t_d^{intro}(n)), \log|D^{intro}|) \\ &= \mathrm{poly}(\log q(n) \cdot t_s^{PB}(q(n)), \log t_d(n), \log t_d^{PB}(q(n)), \log\log(n), \log|D|). \end{aligned}$$

- **(答案长度：)** 答案长度为

$$\begin{aligned} a'(n) &= k(n) \cdot \mathrm{poly}(\log(t_d^{intro}(n)), \log(|D^{intro}|)) \\ &= \mathrm{poly}(\log t_d(n), \log t_d^{PB}(q(n)), \log\log(n), \log\log q(n), \log|D|). \end{aligned}$$

- **(采样器运行时间：)** 采样器运行时间为

$$\begin{aligned} t'_s(n) &= k(n) \cdot \mathrm{poly}(t_s^{intro}(n), t_d^{intro}(n), |D|) \\ &= \mathrm{poly}(\log q(n) \cdot t_s^{PB}(q(n)), t_d(n), t_d^{PB}(q(n)), \log q(n), \log(n), |D|). \end{aligned}$$

- **(判定器运行时间：)** 判定器运行时间为

$$\begin{aligned} t'_d(n) &= k(n) \cdot \mathrm{poly}(t_s^{intro}(n), t_d^{intro}(n), |D^{intro}|) \\ &= \mathrm{poly}(\log q(n) \cdot t_s^{PB}(q(n)), t_d(n), t_d^{PB}(q(n)), \log q(n), \log(n), |D|). \end{aligned}$$

其余性质可由定理 50 和定理52 直接复合得到。供参考，G^{intro} 的参数见下表。

G	G^{intro}
$q(n)$	$\mathrm{poly}\log q(n)$
$a(n)$	$(a(n) + q(n) + O(1)) \cdot \mathrm{poly}\log q(n)$
$t_s(n)$	$\mathrm{poly}\log q(n) \cdot t_s^{PB}(q(n))$
$t_d(n)$	$(t_d(n) + t_d^{PB}(q(n)) + O(\log(n)) \cdot \mathrm{poly}\log(q(n))$
$\|D\|$	$\|D\| + O(1)$
$\|S\|$	$\|S\| + O(1)$

□

5.2 有间隙超压缩

定理 *54*。存在一台图灵机 *GappedHypercompress*，给定一个图灵机元组 $G^{\prime} = (S^{\prime}, D^{\prime})$ 的描述作为输入，该机器会输出一个元组 $G^{\prime} = (S^{\prime}, D^{\prime})$ 的描述，并具有以下性质。设 $G^{\prime} = (S^{\prime}, D^{\prime})$ 是一个 $MIP^{*}[q^{\prime}(n), a^{\prime}(n), t_s^{\prime}(n), t_d^{\prime}(n)]$ 协议。那么，$G^{\prime}$ 是一个 $MIP^{*}[Q_0, a^{\prime}(n), t_s^{\prime}(n), t_d^{\prime}(n)]$协议，且

1. 问题长度：Q_0 是一个普适常数，使得对所有 $\ell > Q_0, \max(C\log^{\beta}(\ell), C\log^{\beta}(q^{*})) < \ell$，其中 C，β，q^{*} 是定理 *50* 中所引问题长度里的普适常数。*2.* 答案长度：$a^{\prime}(n) = a^{\prime}(n) \cdot$ 多项式对数(n)。

3. 采样器运行时间：$t_s^{\prime} = O(1)$。

4. 判定器运行时间：$t^{\prime}(n) =$ 多项式$(n) + O((\text{loglog log } q^{\prime}(n))^2 \cdot (|D^{\prime}| + |S^{\prime}|))$*5.* 完备性：对于所有 n，如果 $G_n^{\prime}$ 具有博弈值为1 的可预言化有限维同步策略 $\mathscr{S}^{\prime}$，那么 $G_n^{\prime}$ 也具有博弈值为1 的可预言化有限维同步策略 $\mathscr{S}^{\prime}$。*6.* 可靠性：对于所有 n，如果 $\omega_q^s(G_n^{\prime}) \leq 1/2$，那么 $\omega_q^s(G_n^{\prime}) \leq 1/2$ 也成立。

证明。 协议 $G^{\prime} = (S^{\prime}, D^{\prime})$ 由以下采样器和判定器组成。

1. **采样器 器：** 该采样器与定理 50 中问题长度为 Q 时的采样器 S^{intro} 相同 $_0$.

2. **判定器：** 判定器执行算法 2 中的算法

1 输入：n, x, y, a, b 2 初始化 i := 0, ℓ_0 := q′(n), D^{comp} = D′, S^{comp} = S′. 3 当 $\ell_i > Q_0$ 时执行 4 D^{comp}, S^{comp} := GappedIntro(D^{comp}, S^{comp})5 $\ell_{i+1} := \lceil C \log^{\beta} \ell \rceil$ i := i + 1 6 结束 7 运行 D^{comp}(n, x, y, a, b)。若其接受则接受，否则拒绝。

伪代码 2： 超压缩博弈。

1. **问题长度：** 对于任意的 $G^{\prime}$，超压缩博弈 $G_n^{\prime}$ 的问题长度至多为 Q_0。

   这由 G 的定义可知 $_n$（如果问题长度大于 Q_0，，我们就可以再应用一次*Intro* ，从而严格缩短问题长度）。

2. 运行时间：首先，我们声称，对于任意问题长度为 q′(n) 的博弈 G′，超压缩博弈 $G_n^{\prime}$ 可通过至多 m = O(log log log(q′(n))) 次将 GappedIntro 应用于 G′ 而得到。为证明这一点，令 f(ℓ) = C $\log^{\beta} \ell$。根据前一项，我们知道 $G_n^{\prime}$ 的问题长度至多为 Q_0。令 g(ℓ) 表示 f 迭代多少次后达到 Q_0。我们可以用以下递推关系定义 g:

$$g(\ell) = \begin{cases} 0 & \ell \leq Q_0 \\ 1 + g(f(\ell)) & n > Q_0. \end{cases} \tag{30}$$

   我们声称，只要Q_0取值足够大，就存在某个常数G，使得$g(\ell) \leq G\,\text{loglog log}(\ell)$。（事实上，这个上界并不紧，$g$ 的增长慢得多，但这对我们的

目的已经足够了。）我们用归纳法证明这一点。基础情形是 $\ell \le Q_0$, ，此时上界成立。对于归纳步骤，写作

$$\begin{aligned} g(\ell) &= 1 + g(f(\ell)) && (31)\\ &= 1 + g(C\log^{\beta}(\ell)) && (32)\\ &\le 1 + G\log\log\log(C\log^{\beta}(\ell)) && (33)\\ &= 1 + G\log\log(\log C + \beta\log\log\ell) && (34)\\ &\le 1 + G\log\log(2\beta\log\log\ell) && (35)\\ &= 1 + G\log\log 2\beta + G\log\log\log\log\ell && (36)\\ &\le 3G\log\log\log\log\ell && (37)\\ &\le G\log\log\log\ell. && (38) \end{aligned}$$

这里，在第一个不等式中，我们使用了归纳假设，并假设所选择的Q_0 满足：对所有 $\ell > Q_0$, $C\log^{\beta}\ell < \ell$均成立；在第二个不等式中，我们假设Q_0 足够大，使得 $\beta\log\log Q_0 \ge \log C$；在第三个不等式中，我们假设$Q_0$足够大，使得 1 和$G\log\log\ 2\beta$ 都小于或等于$G\log\log\log\log Q_0$, ；在第四个不等式中，我们假设 $\log\log\log\log Q_0 \le \frac{1}{3}\log\log\log Q_0$。

这给出了循环迭代次数的界。每次迭代都会调用过程 GappedIntro，其运行时间为 O(|D_i| + |S_i|) = O(|$D^{⌟}$| + (i + 1)|$S^{⌟}$|)。因此，循环的总运行时间有界于 O(m|$D^{⌟}$| + m^2|$S^{⌟}$|) = O((log log log q$^{⌟}$(n))^2 · (|$D^{⌟}$| + |$S^{⌟}$|))。
最后，我们必须确定循环结束后调用的判定器的运行时间。该时间关于最终博弈的答案长度为多项式；下一项将证明，该答案长度为$O(\text{poly}\log(n)\cdot a^{⌟}(n)) = \text{poly}(n)$。因此，最终判定器的运行时间总计为 $\text{poly}(n)$，所以整个判定器的运行时间为 $\text{poly}(n) + O((\log\log\log q^{⌟}(n))^2\cdot(|D^{⌟}| + |S^{⌟}|))$。

3. **答案长度：**在循环的第i次迭代中，博弈的答案长度会按照以下公式从$a_i(n)$增加到$a_{i+1}(n)$：

$$a_{i+1}(n) = A(a_i(n) + \ell_i(n) + O(1))\cdot\log^{\alpha}\ell_i(n), \tag{39}$$

其中A、 α 为常数。我们可以用一个略显粗糙的界来估计它：

$$a_{i+1}(n) \le A' a_i(n)\cdot\log^{\alpha} n, \tag{40}$$

对于某个常数A'，利用以下界：对于所有i</style}，$(n) \le a_i(n)$ 以及 $\ell_i(n) \le \text{poly}(n)$，可以得到稍微更紧的界。为此，我们可以找到一个常数A' 使得

$$\begin{aligned} a_1 &\le A' a(n)\cdot\log^{\alpha} n, && (41)\\ a_{i+1} &\le A' a_i(n)\log^{\alpha}(\log^{\beta} n) \quad \text{for all } i \ge 1. && (42) \end{aligned}$$

注意，后一个方程的右侧等于 $A' a_i(n)\cdot\beta^{\alpha}(\log\log n)^{\alpha}$。为简化记号，我们将把 β 吸收到 A' 中。

经过$m = g(\ell) = G\log\log\log n$ 次重复后，答案大小为

$$\begin{aligned} a_m &\le (A'(\log\log n)^{\alpha})^m (A' a^{⌟}(n)\cdot\log^{\alpha} n) && (43)\\ &= 2^{(\log A' + \alpha\log\log\log n)\cdot G\log\log\log n}\cdot(A' a^{⌟}(n)\cdot\log^{\alpha} n) && (44)\\ &= O\left(2^{A''(\log\log\log n)^2}\cdot a^{⌟}(n)\log^{\alpha} n\right) && (45)\\ &= O\left(2^{\log\log n}\cdot a^{⌟}(n)\log^{\alpha} n\right) && (46)\\ &= O\left(\log n\cdot\log^{\alpha} n\cdot a^{⌟}(n)\right) && (47)\\ &= \text{poly}\log n\cdot a^{⌟}(n). && (48) \end{aligned}$$

4. 完备性与可靠性： 这些结论可通过反复应用定理 50 中相应的条目得到。

□

定义 55。 语言 L_{HALT} 由所有满足以下条件的字符串 x 组成：x 是一台图灵机 M_x的描述，并且该图灵机在空输入带上运行时会停机。该语言是 递归可枚举语言完全的。

定理 56。 存在一个以 n 为索引的 多证明者交互式证明*[多项式(n)，多项式(n)，多项式(n)，多项式(n)] 协议 ($GenG^{\circ}$，N°) 来判定 L_{HALT}。

证明。 这是 [JNV+20] 的主要结果。 □

定理 57。 存在一个以 n 为索引的 多证明者交互式证明*[多项式对数(n)，多项式对数(n)，多项式(n)，多项式(n)] 协议 ($GenG^{\lrcorner}$，$N^{\lrcorner}$)来判定 L_{HALT}。

证明。 我们通过将定理 53 应用于定理 56 来推导这一结果。具体而言，$GenG^{\lrcorner}$和 $N^{\lrcorner}$ 的描述如下：

- $GenG^{\lrcorner}$ 在输入 z 时，首先运行 $\mathrm{GenG}^{\circ}(z)$ 以获得一个游戏族（$S^{z,\circ}$, $D^{z,\circ}$）的（描述）。然后，将定理 53 中的过程 GappedCompress 应用于（$S^{z,\circ}$, $D^{z,\circ}$），从而获得一个游戏族（$S^{z,\lrcorner}$, $D^{z,\lrcorner}$,$Q^{z,\lrcorner}$），并输出（$S^{z,\lrcorner}$, $D^{z,\lrcorner}$）。
- $N^{\lrcorner}$ 在输入 z 时计算并输出 $N^{\circ}(z)$。

注意，$\mathrm{GenG}^{\lrcorner}$ 的运行时间为 $O(|D^{z,\circ}| + |S^{z,\circ}|) = \mathrm{poly}(|z|)$，因为 $|D^{z,\lrcorner}|$ 和 $|S^{\circ,\lrcorner}|$ 都有 $\mathrm{poly}(|z|)$ 的上界（它们由 GenG° 在 $\mathrm{poly}(|z|)$ 时间内生成）。$\mathrm{N}^{\lrcorner}$ 的运行时间与运行 N° 所需的时间相同。

还需证明参数界如所述：$q^{\lrcorner}(n) = \mathrm{poly\,log}(n)$，$a^{\lrcorner}(n) = \mathrm{poly\,log}(n)$，$t_s^{\lrcorner}(n) = \mathrm{poly}(n)$，$t_d^{\lrcorner}(n) = \mathrm{poly}(n)$。注意到 $q^{\circ}(n) = \mathrm{poly}(n)$、$t_d^{\circ}(n) = \mathrm{poly}(n)$、$|D^{\circ}| = \mathrm{poly}(n)$，以及对所有 $q \in \mathbb{N}$，$t_s^{PB}(q) = \mathrm{poly\,log}(q)$、$t_d^{PB}(q) = \mathrm{poly}(q)$，再将这些量代入定理 53，即可得出结论。

□

定理 58. 存在一个以 n 为索引的多证明者交互式证明*$[O(1), \mathrm{polylog}(n), O(1), \mathrm{poly}(n)]$ 协议$(GenG^{\lrcorner}, N^{\lrcorner})$ 来判定 L_{HALT}。

证明。 通过将定理 54 应用于定理 57，可类似于定理 57 的证明得出结论。

□

6 柯尔莫哥洛夫复杂度给出的界

描述多证明者交互式证明的复杂度多证明者交互式证明* **协议**每个多证明者交互式证明* 协议（更完整的定义见定义 17）都由一对图灵机(S,D)指定，分别称为采样器和判定器。本节为多证明者交互式证明* 协议定义以下资源界；这些资源界都要求不超过输入实例长度n 的多项式：

- $r(n)$，S 所用随机种子的比特长度（更准确地说，是S 读取的随机输入比特数的上界）。
- $q(n)$，向单个玩家提出的问题的比特长度（通过填充，我们假设对于所有大小为n的实例，两个玩家收到的问题比特长度始终相同）。注意，如果问题分布是自由的（且均匀的），我们可以假设 $2q(n) = r(n)$，但当问题分布相关时，这不一定成立。
- $a(n)$，单个玩家答案的比特长度（再次通过填充，我们假设所有答案的比特长度都相同）。

• $t(n)$，这是采样器 S 在给定随机种子时的运行时间，以及判定器 D 在给定一对问题和一对答案时的运行时间的上界。

注 59. 在这里，我们对参数 $r(n)$ 和 $q(n)$ 的定义与第 *2* 节中的定义略有不同（尤其是定义 *16* 和定义 *18*）。在第 *2* 节中，我们令 $r(n)$ 和 $q(n)$ 相同（将 $q(n)$ 视为问题长度和 S 读取的随机种子长度的共同上界）；而在本节中，我们将使用独立的参数来跟踪这两个量。之所以有所不同，是因为在证明上界时，令 $q(n)$ 和 $r(n)$ 相同可以简化记号，因为我们构造的所有协议都具有相近的 $q(n)$ 和 $r(n)$；然而，在证明下界时，我们希望模型尽可能一般，因此希望考虑 $r(n)$ 可能远大于 $q(n)$的协议。

在本节中，我们还将 $t_S(n)$ （采样器运行时间）和 $t_d(n)$ （判定器运行时间）合并为单个参数 $t(n)$，因为对于我们的任何界而言，都无须将任一运行时间限制得比 n 的多项式界更严格。

引理 60. 假设 $L \in$ 多证明者交互式证明$^*[r(n), q(n), a(n), t(n)]$。那么存在一个常数 δ，使得 $L \in$ 确定性时间复杂度$[h(n)]/2^{g(n)}$，其中

$$h(n) = 2^{r(n)+2(q(n)+a(n))} \cdot t(n), \quad g(n) = (2q(n) + \delta + 1) \cdot 2^{2(q(n)+a(n))}.$$

或者，若 $L \in$ 多证明者交互式证明$^*_0[r(n), q(n), a(n), t(n)]$，，那么 $L \in$ 确定性时间复杂度$[h(n)]/2^{g(n)}$，其中

$$h(n) = 2^{r(n)+2(q(n)+a(n))} \cdot t(n), \quad g(n) = 2^{2(q(n)+a(n))}.$$

证明。证明的基本结构如下。假设 L $\in$ 多证明者交互式证明*[r(n)、q(n)、a(n)、t(n)]；那么，对于任意实例 x，都存在一个双玩家纠缠博弈 G_x，其参数为 r(|x|) 、 q(|x|) 、 a(|x|) 、 t(|x|)，使得当 x $\in$ L 时，G_x 的博弈值为 1；而当 x $\notin$ L 时，博弈值为 $\leq \frac{1}{2}$。我们构造一台确定性图灵机，在读取一些辅助信息后判定 x $\in$ L。辅助信息只需包含每个参数为 r(|x|)、q(|x|)、a(|x|)、t(|x|) 的可能的 MIP*(2) 博弈各自对应的一个比特；该比特说明相关博弈的博弈值是 $= 1$ 还是 $\leq \frac{1}{2}$ （或者在零间隙情形下是 $= 1$ 还是 < 1）。随后，确定性图灵机可以查出用于判定 L 的博弈值，而不必与两个纠缠证明者进行博弈来估算其博弈值。

要指定一个双人博弈，只需填写下表：

^{问题_A,问题_B,答案_A,答案_B}	给定(问题$_A$,问题$_B$)，生成(问题$_A$,问题$_B$) (答案$_A$, 答案$_B$) 这一被接受的问答对的概率?
.....	

此表有$(2^{q(n)})^2(2^{a(n)})^2$ 行。要计算存储每一行所需的比特数，我们必须指定概率表示的精度。

在有间隙情形下，是情形与否情形之间的游戏值间隙为常数，因此只需将问题对(问题$_A$,问题$_B$) 上的概率分布表示到总变差距离中的加性常数误差范围内。为此，只需将每个概率表示到$O(2^{-2_{q(n)}})$的精度。因此，我们可以将概率表示为有理数，用 $2q(n)+\delta$ 比特来指定，其中常数 δ 取决于游戏值间隙。现在，每一行总共用 $2q(n) + \delta$ 比特存储概率，并用一比特表示该问答对是否被接受。因此，需要

$$g(n) := (2q(n) + \delta + 1) \times 2^{2(q(n)+a(n))}$$

比特来指定一个博弈表。因此，至多有

$$G(n) := 2^{g(n)} = 2^{(2q(n)+\delta+1)\cdot 2^{2(q(n)+a(n))}}$$

种可能的博弈。

在游戏值要么为 1、要么严格小于 1 的无间隙情形下，不失一般性，我们可以假设问题分布在其支撑集上是均匀的，正如预备知识中所述。因此，在无间隙情形下，我们不需要中间列，且至多有

$$G(n) = 2^{2^{2(q(n)+a(n))}}$$

可能的博弈。

现在，假设 L 是 MIP*[r(n), q(n), a(n), t(n)] 中的一种语言。我们指定一台确定性图灵机 M，它判定 L，并使用 G(n) 比特的辅助信息。输入长度为 n 的辅助信息串由每个可能的博弈各对应一个比特组成，这些博弈对应于一个 MIP*[r(n), q(n), a(n), t(n)] 协议；这个比特指出该博弈的纠缠值是否大于 2/3（或者，在无间隙情形下，是否等于 1）。图灵机 M 随后执行以下操作：

1. 给定实例 x，计算用于判定 L 的多证明者交互式证明* 博弈的博弈表 T。这可以通过以下过程完成。

   (a) 首先，计算问题对的表（在有间隙情形下，还要计算近似概率）。这可以通过遍历长度为 $r(n)$ 的所有可能随机种子来完成；对于每个种子 s，计算问题对 q_A,q_B （即多证明者交互式证明* 采样器 S 在种子 s 下的输出），并增加其对应的计数。此过程需要 $O(t(n)\cdot 2^{r(n)})$ 时间。(b) 接下来，对于每个生成的问题对 q_A,q_B，遍历所有可能的答案对 a_A, a_B，并在 q_A,q_B, a_A, a_B 上运行判定器。将此信息存入表中相应的行。

   部分 (a) 需要 $O(t(n)\cdot 2^{r(n)})$ 时间。部分 (b) 所需时间等于 $t(n)$ 乘以问题对和答案对的数量。问题对和答案对的数量至多为 $2^{2q(n)}\cdot 2^{2a(n)}$。因此，生成博弈表的总运行时间为 $O(t(n)\cdot 2^{r(n)+2(q(n)+a(n))})$。

2. 查阅辅助信息串中的博弈表 T。根据辅助信息串中针对 T列出的是 1 还是 0，决定输出是或否。

在有间隙情形下，上述过程计算出的博弈表 T 指定了一个博弈，其博弈值与决定 L 的多证明者交互式证明* 博弈的博弈值相差 $\varepsilon(\delta)$，其中 $\varepsilon(\delta)$ 是一个取决于精度常数 δ 的常数。因此，将 δ 取得足够小，并考虑到多证明者交互式证明*博弈的「是」实例与「否」实例之间存在常数间隙，我们可以确保 M 能正确判定 L。

在无间隙情形下，博弈表 T 指定了一个博弈，该博弈的博弈值必然为 1，当且仅当决定 L 的多证明者交互式证明* 博弈的博弈值为 1。

此外，M 的运行时间和辅助信息长度符合定理陈述中的要求。 □

引理 61 $.\mathsf{EEXP} \not\subseteq$ 确定性时间复杂度$[2^{kn^k}]/\varepsilon 2^{cn}$，对于任意常数 $k \geq 1$ 以及任意满足 c, ε 和 $c+\varepsilon<1$ 条件的常数。

证明。 以下论证基于 [HM95] 第 2 节中的论证。我们首先定义一些记号。对于任意 $n \in \mathbb{N}$，定义如下：

1. 为方便记号，令 $m := 2^{cn}$。

2. 令 C 为稍后确定的某个常数。

3. 令 τ_n为 $\{0,1\}^m$中不属于 $K[m-2、C\cdot 2^{2k(\frac{1}{c}\log m)^k}]$的字典序最小字符串。（关于 K 的定义，见定义 4。注意，就 n 而言，这给出的建议长度界为$2^{cn}-2$，运行时间界为 $C\cdot 2^{2kn^k}$。）根据计数论证，该字符串总是存在：$\{0,1\}^m$中有 2^m个字符串，而 $\bigcup_{m=1}^{-2}\{0,1\}^i$中只有 2^{m-1} 个字符串。

4. 如果对于某些长度为 n 的字符串 $w_1,\ldots\ldots、w_\ell$，有 $\tau_n = w_1\|w_2\|\ldots\ldots\|w_\ell$，我们称字符串 $w_1,\ldots\ldots、w_\ell$为 τ_n 的“n-块”。令 A_n 为集合 $\{w_i:\ w_i \text{ 是 } \tau_n\}$ 的一个 n-块。令 A （一个语言）为并集$\bigcup_{n\in\mathbb{N}} A_n$。

引理 62。$A \subseteq \mathsf{EEXP}$。

证明。 我们描述一台判定A的图灵机。该机器对长度为n的输入x 执行以下操作：

1. 写下 τ_n。为此：

   (a) 对长度为 $\leq 2^{cn}-2$ 的所有字符串运行 T （定义 4 中的通用模拟器），运行 2^{2kn^k} 步，然后按字典序列出所有结果字符串。(b) 找出 $\{0,1\}^{2^{cn}}$ 中第一个不在 (a) 所列清单中的字符串。将结果设为 τ_n。

2. 将 x 与 τ_n 的每个 n 块进行比较，以判定 x 是否属于 A_n。

该过程耗时 $2^{2^{cn}} \cdot 2^{2kn^k} + O(2^{cn})$，相对于$n$是双指数级的。 □

引理 63。 假设 $A \subseteq$ 确定性时间复杂度$(2^{kn^k})/\varepsilon 2^{cn}$，我们可以生成 τ_n，使用长度为$(c+\varepsilon)2^{cn}$ 的辅助信息，并在 $C \cdot 2^{2kn^k}$ 时间内完成，其中 C 是某个常数。

证明。 固定一个n。令M 为判定A的确定性时间复杂度$(2^{kn^k})/\varepsilon 2^{cn}$ 机器。M 使用辅助信息a，其中 $|a| = \varepsilon 2^{cn}$，并可在$O(2^{kn^k})$ 时间内判定是否属于A。

令$LEX(A_n)$ 为A_n中所有字符串按字典序排列的列表。为了重构 τ_n，我们需要以下辅助信息：

- a，提供给M的辅助信息，
- z，一份列表，列出所有i 对应的i个n块在$LEX(A_n)$ 中的位置，其中n块组成 τ_n。

a 的长度为 $\varepsilon 2^{cn}$。z 的长度为

$$|z| = \frac{|\tau_n|}{n} \cdot \log(|A_n|) \leq \frac{2^{cn}}{n} \cdot (cn - n) \leq c2^{cn}.$$

因此，我们所需的辅助信息总量为 $(c+\varepsilon)2^{cn}$。

为了重构 τ_n，我们将执行以下操作：

1. 通过按字典序遍历所有长度为 n 的字符串，并在每个字符串上运行 M，生成 $LEX(A_n)$ 。2. 对于每个 $i \in [\frac{|\tau_n|}{n}]$，读取 z中的相应索引，并从 A_n中复制出正确的 n块。

该过程所需时间至多为 $2^n \cdot 2^{kn^k} + O(2^{cn})$。利用假设 $k \geq 1$，可将其写为$O(2^{2kn^k})$。

□

鉴于 $c + \varepsilon < 1$，引理 63 与 τ_n 的定义相矛盾，因为对于充分大的 n，$(c+\varepsilon)2^{cn} < 2^{cn} - 2$。我们得出 EEXP $\not\subseteq$ 确定性时间复杂度$[2^{kn^k}]/\varepsilon 2^{cn}$。 □

定理 64. EEXP $\not\subseteq$ MIP[r(n), q(n), a(n), t(n)] 若存在常数 n_0 和 $\gamma < \frac{1}{2}$，使得对所有 $n > n_0$，$q(n) + a(n) \leq \gamma$ log(n)，且 t(n)、r(n) $=$ poly(n)。将 MIP*[r(n), q(n), a(n), t(n)] 替换为 MIP_0^*[r(n), q(n), a(n), t(n)]，同样的结论仍然成立。*

注释 65. 注意，$q(n)$ 和 $a(n)$ 是单个证明者的问题和答案长度的界；因此，MIP* 协议中的总通信量可由 $2(q(n) + a(n))$作为上界。这或许会让 $\gamma < 1/2$ 要求显得更自然。

Proof. 我们给出有间隙情形的证明；无间隙情形的证明完全类似。 .

假设 EEXP $\subseteq$ MIP*$[r(n), q(n), a(n), t(n)]$，其中 r、q、a、t 如定理陈述所述。根据引理 60，我们知道

$$\mathsf{MIP}^*[r(n), q(n), a(n), t(n)] \subseteq \mathsf{DTIME}[t(n) \cdot 2^{r(n)+2(q(n)+a(n))}]/2^{g(n)},$$

其中 $g(n) = (2q(n) + \delta + 1) \cdot 2^{2(q(n)+a(n))}$ 对某个常数 δ 成立。

注意，如果 $t(n)$、$r(n) = \mathrm{poly}(n)$，那么存在某个常数 k，使得在渐近极限下$t(n) \cdot 2^{r(n)+2(q(n)+a(n))} \leq 2^{kn^k}$。根据引理 61，我们知道，对于任意常数$k$ 以及任意常数 c，γ，只要 $\varepsilon + c < 1$，就有 EEXP $\not\subseteq$ 确定性时间复杂度 $[2^{kn^k}]/\varepsilon 2^{cn}$。因此，如果对于任意 常数$\varepsilon$，$c$，只要 $\varepsilon + c < 1$，在渐近极限下有 $2^{g(n)} \leq \varepsilon 2^{cn}$，就会产生矛盾，因为那样我们就会得到以下包含关系链

$$\mathsf{EEXP} \subseteq \mathsf{MIP}^*[r(n), q(n), a(n), t(n)] \subseteq \mathsf{DTIME}[2^{kn^k}]/\varepsilon 2^{cn}.$$

对两边取对数，我们得出，不可能出现以下情况：

$$(2q(n) + \delta + 1) \cdot 2^{2(q(n)+a(n))} \leq cn + \log \varepsilon.$$

代入 $q(n) + a(n) \leq \gamma \log n$，可知左边至多为 $(2\gamma \log(n) + \delta + 1)n^{2\gamma}$。因此，当 $\gamma < 1/2$ 时，我们得到矛盾，因为可以选择常数 c 和 ε，使得 $2\gamma < c < 1$且 $\varepsilon < 1 - c$；并且在渐近极限下，对于代入的这些 c 和 ε 取值，右边将支配左边。

□

注释 *66.* 请注意，定理 *64* 并未推出，对于 $\gamma < \frac{1}{2}$，$q(n) + a(n) \leq \gamma log(n)$ 的 MIP^* 是可判定的。事实上，可以通过填充论证构造出属于此类的不可判定语言。例如，考虑任意一个满足 $q(n) = poly(n)$ 且 $a(n) = poly(n)$ 的 MIP^* 语言 L；然后考虑 $L' := \{x\#^{2^{2^n}} : x \in L\}$。$L'$ 属于 $q(n) = O(loglog\ n)$ 且 $a(n) = O(loglog\ n)$ 的 MIP^*，但 L' 仍然不可判定。然而，定理 *64* 表明，没有任何在多项式时间归约下为 *EEXP* 困难的语言——例如二进制停机问题——能够属于满足 $q(n) + a(n) < \frac{1}{2} log\ n$ 的 MIP^* 类。特别是，这意味着 $q(n) + a(n) < \frac{1}{2} log\ n$ 的 MIP^* 不可能等于 *RE*。

7 致谢

我们感谢 AramHarrow、Hamoon Mousavi、Chris Umans 和 Ryan Williams 提供了有益的交流。TZ 的部分研究经费来自 Akamai 总统奖学金。

参考文献

[ABD+09] Scott Aaronson、Salman Beigi、Andrew Drucker、Bill Fefferman 和 Peter Shor。《非纠缠的力量》。《计算理论》，5：1–42，2009年，arXiv:0804.0802。[AIM14] S. Aaronson、R. Impagliazzo 和 D. Moshkovitz。含多个 Merlin 的 AM。载于《计算复杂性》（*CCC*），*2014*年 *IEEE*第*29*届会议，第44–55页，2014年6月，arXiv:1401.6848。doi:10.1109/CCC.2014.13。[ALM+98] Sanjeev Arora、Carsten Lund、Rajeev Motwani、Madhu Sudan 和 Mario Szegedy。证明验证与近似问题的困难性。《美国计算机协会会刊》（*JACM*），45(3)：501–555，1998年。[AS98] Sanjeev Arora 和 Shmuel Safra。证明的概率检验：NP 的一种新刻画。《美国计算机协会会刊》（*JACM*），45(1)：70–122，1998年。[BCY10] Fernando Brand˜ão、Matthias Christandl 和 J ohn Yard。量子可分性问题的准多项式时间算法。2010年，arXiv:1011.2751。[BFL91] L´ászl´o Babai、Lance Fortnow 和 Carsten Lund。非确定性指数时间具有双证明者交互协议。《计算复杂性》，1(1)：3–40，1991年。[BH13] Fernando GSL Brand˜ão 和 Aram W Harrow。局部测量下的量子 de Finetti 定理及其应用。载于第四十五届 *ACM* 计算理论研讨会论文集，第861–870页，2013年。[BT09] Hugue Blier 和 Alain Tapp。NP 中的所有语言都有极短的量子证明。载于*2009*年第三届国际量子、纳米与微技术会议，第34–37页。IEEE，2009年，arXiv:0709.0738。[BVY17] Mohammad Bavarian、Thomas Vidick 和 Henry Yuen。通过锚定放大量子纠缠博弈的困难性。载于第*49*届年度 *ACM SIGACT*计算理论研讨会论文集，第303–316页。ACM，2017年，arXiv:1509.07466。[CD10] J. Chen 和 A. Drucker。无纠缠测量的 SAT 短多证明者量子证明，2010年，arXiv:1011.0716。[CF11] Alessandro Chiesa 和 Michael J. Forbes。含多个证明者的 QMA 的可靠性改进。2011年，arXiv:1108.2098。

[CGS17] Andrea Coladangelo、Koon Tong Goh 和 Valerio Scarani。所有纯双体纠缠态都可以自检。《自然·通讯》，8(1)：15485，2017年，arXiv:1611.08062。[CHTW04] Richard Cleve、Peter Hoyer、Benjamin Toner 和 John Watrous。非局域策略的后果与局限。载于《论文集：第19届IEEE计算复杂性年度会议》，2004年，第236–249页。IEEE，2004年，arXiv:quant-ph/0404076。[CY13] Matthew Coudron 和 Henry Yuen。使用常数数量的设备实现无限随机性扩展与放大。2013年，arXiv:1310.6755。[dlS22] Mikael de la Salle。群与非局域博弈的谱隙和稳定性。2022年，arXiv:2204.07084。[DSV15] Irit Dinur、David Steurer 和 Thomas Vidick。纠缠投影游戏的平行重复定理。《计算复杂性》，24(2)：201–254，2015年，arXiv:1310.4113。[FNT14] Tobias Fritz、Tim Netzer 和 Andreas Thom。能否计算算子范数？《美国数学会会刊》，142(12)：4265–4276，2014年，arXiv:1207.0975。[Fu22] Honghao Fu。常数规模的关联足以对无界维数的最大纠缠态进行自检。《Quantum》，6：614，2022年，arXiv:1911.01494。[HM95] Steven Homer 和 Sarah Mocas。指数时间复杂度类的非一致下界。载于《国际计算机科学数学基础研讨会》，第159–168页。施普林格，1995年。[HM13] Aram W Harrow 和 Ashley Montanaro。乘积态测试、量子 Merlin-Arthur 博弈与张量优化。《美国计算机协会会刊》，60(1)：1–43，2013年，arXiv:1001.0017。[IV12] Tsuyoshi Ito 和 Thomas Vidick。一种对纠缠证明者仍具可靠性的 NEXP 多证明者交互式证明。载于《2012年IEEE第53届计算机科学基础年度研讨会》，第243–252页。IEEE，2012年，arXiv:1207.0550。[Ji17] Zhengfeng Ji。量子多证明者交互式证明的压缩。载于《第49届年度 ACM SIGACT计算理论研讨会论文集》，第289–302页。ACM，2017年，arXiv:1610.03133。[JNV+20] Zhengfeng Ji、Anand Natarajan、Thomas Vidick、John Wright 和 Henry Yuen。MIP* = 递归可枚举语言。2020年，arXiv:2001.04383。[MNY20] Hamoon Mousavi、Seyed Sajjad Nezhadi 和 Henry Yuen。论零间隙 MIP*的复杂性。2020年，arXiv:2002.10490。[MNY21] Hamoon Mousavi、Seyed Sajjad Nezhadi 和 Henry Yuen。非局域博弈、压缩定理与算术层级。2021年，arXiv:2110.04651。[MV05] Peter Bro Miltersen 和 N Variyam Vinodchandran。利用击中集对 Arthur–Merlin 博弈去随机化。《计算复杂性》，14(3)：256–279，2005年。[NC02] Michael A Nielsen 和 Isaac Chuang。《量子计算与量子信息》，2002年。[NV18] Anand Natarajan 和 Thomas Vidick。撤稿：双玩家纠缠博弈是 NP 困难的。2018年。doi:10.4230/LIPICS.CCC.2018.20。[NW19] Anand Natarajan 和 John Wright。NEEXP ⊆ MIP*。载于《2019年IEEE第60届计算机科学基础年度研讨会（FOCS）》，第510–518页。IEEE，2019年，arXiv:1904.05870。[RUV13] Ben W Reichardt、Falk Unger 和 Umesh Vazirani。对量子系统的经典控制。《自然》，496(7446)：456，2013年，arXiv:1209.0448。

[˘SB20] Ivan ˘Supi´c 和 Joseph Bowles。《量子系统的自检：综述》。*Quantum*，4:337，2020年9月。doi:10.22331/q-2020-09-30-337。[Vid22] Thomas Vidick。《近似同步量子关联》。数学物理学杂志，63(2):022201，2022年，arXiv:2103.02468。doi:10.1063/5.0056512。[Weh06] Stephanie Wehner。《具有二元答案的交互式证明系统中的纠缠》。载于*STACS 2006*，第162–171页。Springer Berlin Heidelberg，2006年。doi:10.1007/11672142 12。[Wil11] Mark M Wilde。《从经典香农理论到量子香农理论》。*arXiv* 预印本 *arXiv:1106.1445*，2011年，arXiv:1106.1445。