arXiv:2303.01625v1 [quant-ph] 2 Mar 2023

量子霸权认证随机性

Scott Aaronson* Shih-Han Hung†

摘要

我们提出了近期期量子设备的一项应用：生成经密码学认证的随机比特，以便（例如）用于权益证明加密货币。我们的协议重新利用了现有的“量子霸权”实验；这些实验基于随机线路采样，自2019年起已由 Google 和中国科学技术大学（USTC）成功开展。我们证明，只要这些实验的输出通过当前标准的线性交叉熵基准（LXEB），在合理的困难性假设下，它们必然包含 $\Omega(n)$ 的最小熵，其中 n 是量子比特的数量。为了实现随机性的净增益，我们使用一个较小的随机种子来生成伪随机挑战线路。作为对挑战线路的响应，量子计算机生成输出字符串；经过验证后，这些字符串可以输入随机性提取器，以生成经认证的近均匀比特——从而实现从伪随机性到真正随机性的“自举”。我们从两个意义上证明了协议的可靠性：（i）在称为长列表量子霸权验证的困难性假设下；我们在随机预言机模型中论证了该假设的合理性；以及（ii）在随机预言机模型中，对于可能与设备共享任意纠缠的窃听者，无条件地成立。（请注意，即使是能够看到随机预言机的计算无界对手也无法预测我们协议的输出。）目前，我们协议的主要缺点是验证成本呈指数增长；在实践中，这将把其实现限制在最多 $n \sim 60$ 个量子比特的范围内——这是一个攻击代价高昂但并非不可能的规模。除去这一缺点，我们的协议似乎是唯一一种既需要量子计算机（QC）又能在今天实现的量子计算实际应用。

*德克萨斯大学奥斯汀分校。电子邮箱：aaronson@cs.utexas.edu。获美国国防部范内瓦·布什奖学金、伯克利 NSF-QLCI CIQC 中心、西蒙斯研究者奖以及西蒙斯“比特源于量子”合作项目支持。

†德克萨斯大学奥斯汀分校。电子邮箱：shung@cs.utexas.edu。获美国能源部科学办公室国家量子信息科学研究中心量子系统加速器支持。

目录

1 引言 **4**

1.1 我们的贡献.5 1.2 实践考量.7 1.3 相关工作.8 1.4 本文的历史.10 1.5 未来方向.10

2 技术概述 11

2.1 我们的基本结果（不含纠缠对手）.11 2.2 纠缠对手与理想测量.14 2.3 完全通用的设备.15 2.4 熵累积.16 2.5 伪随机性与统计零知识.17

3 预备知识 **18**

3.1 复杂性类.19 3.2 多项式方法.21 3.3 量子信息论.21 3.4 Haar 随机酉矩阵.23 3.4.1 狄利克雷分布.23 3.4.2 完美装置的性能.25

4 熵累积定理 28

5 无侧信息的一般设备 34

5.1 长列表量子优越性验证问题.35 5.2 LLHA 蕴含认证随机性.35 5.3 熵累积.41 5.4 相对于随机预言机的 LLHA.43 5.4.1 双消息量子交互式证明.44 5.4.2 加强困难性.48

6 设备实现　　成理想测量 5 **1**

6.1 单轮分析.52 6.1.1 Holevo信息.52 6.1.2 高XHOG得分意味着Holevo信息较少.53 6.1.3 单轮分析.54 6.2 熵累积.56

7 一个完全一般的设备 **57**

7.1 给定样本访问时对 Haar 随机酉矩阵的模拟.58

7.1.1 从电路预言机到态制备预言机.58 7.1.2 从规范态制备预言机到资源态 60
7.1.3 从资源态到样本.62 7.2 单轮分析.63 7.2.1 一种简化设备.64 7.2.2 一般设备的分析.69
7.3 熵累积.70

8 伪随机性与统计零知识 **71**
8.1 伪随机函数.72 8.2 伪随机酉算子.75 8.3 随机性扩展.78

1 引言

经过三十年的量子计算理论与实验发展，世界终于拥有了含噪量子设备，这些设备具有 $50-60$ 量子比特或 ~ 100 光子，能够以一种推测可胜过现有任何经典计算机的方式解决特殊采样问题。这些设备包括 Google 的53量子比特“Sycamore”芯片 [12], 中国科学技术大学的“九章” [65] 和“祖冲之” [62], 以及最近 Xanadu 的“Borealis” [40]。这些采样问题包括随机线路采样 [7]和玻色子采样 [4], ，它们直接源于量子复杂性理论中的研究，其起点大约可追溯至 2010年。

需要明确的是，当前设备在哪些意义上实现了“量子霸权”这一里程碑，仍存在争议。Preskill 于 2012年 创造了这一术语 [51]，用来指称在某个定义明确（但不一定有用）的计算任务上，性能比所有已知经典方法快出若干个数量级。另一方面，自 Google 于 2019年 最初宣布这一成果以来 [12], ，采样实验不断取得进展，例如在量子比特数量和线路深度（对于 RCS）方面 [62], ，以及在光子数量和测量保真度（对于玻色子采样）方面 [40]。预计未来还会有进一步改进。另一方面，针对这些实验的经典模拟攻击也 有所进步——有些攻击基于张量网络缩并（例如 [49]），另一些则利用设备中的噪声（例如 [13]）。但值得注意的是，能够完全复现 Google 设备观测性能的攻击（例如 [49], ）仍然具有固有的指数级扩展特性，而且似乎仍需要一台百亿亿次级超级计算机，才能追平或超过 Google 设备 ~ 3 分钟的运行时间。粗略估算，Summit超级计算机的功耗为 13 兆瓦，而 Google [12, 在附录 H] 中估计，其 53 量子比特量子计算机的稀释制冷机功耗为 ~ 20 千瓦。因此，尽管 量子计算机对制冷的需求极高，但按电力成本衡量，它仍胜出数百倍。

对一些人来说，近期的量子霸权演示之所以重要，主要是因为它们展示了未来容错、可扩展量子计算机所需的许多关键要素；同样重要的是，这些演示没有检测到任何会使容错量子计算变得不可能的相关错误。然而，对另一些人来说，这些实验的意义更大：它们开启了“含噪中等规模量子”（NISQ）计算时代，这也是 Preskill 创造的另一个术语 [52]。NISQ 的希望在于，即使在实现容错之前，拥有多达（比如）1000 个量子比特的含噪量子计算机，也可能已经能解决某些实际问题，就像各种模拟计算设备在晶体管的发明开启数字时代之前就已发挥作用一样。

遗憾的是，尽管迄今已有数十亿美元投入对 NISQ 的期待，但 NISQ 设备缺乏显而易见的“杀手级应用”，已成为这一领域的标志性事实。

也许 NISQ设备可用于凝聚态物理学模拟，甚至用于量子化学模拟。遗憾的是，尽管已有一些令人振奋的量子模拟方案只需数百个量子比特（例如， [56]），但这些方案无一例外都有一个缺陷：需要数千甚至数百万门层。若无法解决这一问题，这些方案就完全超出了 NISQ 设备的能力范围。又或者，NISQ 设备可以通过量子退火或量子近似优化算法（QAOA）[29]，在优化问题上实现加速。遗憾的是，尽管研究人员多年来进行了大量理论和实证研究，却始终难以证明量子退火或 QAOA 在任何实际优化问题上相较于经典计算具有明确优势——更不用说这种优势能否在 NISQ 设备上实现了。

还应补充一点，近年来，关于如何展示量子霸权，出现了一些引人注目的新思路。这些思路包括利用陷门单向函数的交互式协议[20, 35], ，以及 Yamakawa 和 Zhandry 的卓越成果 [63], ，后者相对于随机预言机，为一个 NP 搜索问题带来了指数级量子加速。遗憾的是，在取得某项

突破之前，这些思路似乎都无法在含噪中等规模量子设备上实现。

1.1 我们的贡献

据我们所知，本文首次研究当前基于采样的量子优越性实验是否本身可能在物理学之外具有实用价值。[1] 我们重点研究密码学认证随机比特的生成。

不用说，我们可以轻松地利用量子计算机——甚至只需将盖革计数器放在某种放射性物质旁边——生成任意数量的随机比特：量子力学本身预言，这些比特从根本上说是不可预测的。问题在于，我们如何向一位无法接触我们硬件、只能通过互联网与我们联系的怀疑者证明，这些比特确实是随机的，而不是暗中被植入后门的？这并非纯粹的理论担忧：例如，作为爱德华·斯诺登2013年披露事件的附带结果，世人得知，美国国家标准与技术研究院的一项名为 Dual_EC_DRBG 的伪随机性标准确实被美国国家安全局植入了后门。[2]

认证随机性已成为一个重要的实际问题——尤其是随着权益证明加密货币的兴起，其中一个著名例子是以太坊[3]（撰写本文时的市值为1630亿美元），该网络于2022年9月15日完成迁移。在权益证明系统中，人们持续进行抽签，以决定哪位货币持有者可以将下一个区块添加到区块链中。没有可信的权威机构来管理这些抽签，但整个系统都建立在这样的假设之上：抽签过程诚实进行且不存在偏置。认证随机性的其他应用还包括非交互式零知识证明、金融审计和选举审计。

认证随机性问题的一种方法是将区块链本身用作随机比特的来源——其论据是，任何能够预测这些比特的人，都可以利用这种可预测性来发财 [19]。其他方法则从社会或自然界中寻找可公开验证的熵来源：例如，可以使用道琼斯工业平均指数的最低有效位，或者使用太阳表面形成的颗粒图案。

对我们而言更相关的是，自2009年以来，一系列令人振奋的研究成果展示了如何利用对纠缠粒子的测量作为物理认证的随机性来源 [24, 50, 60, 25, 46, 47]。其基本思想是，如果观测到测量结果违反贝尔/CHSH不等式，那么仅凭这一事实，这些结果不可能 是秘密确定的，除非“爱丽丝”和“鲍勃”探测器之间存在秘密通信。此外，根据实验设置的不同，这种通信可能还必须以超光速进行。因此，这些结果必然包含真正的熵，而这些熵可以输入随机性提取器，将其提纯为近似均匀分布的随机比特。技术上的难点在于，在贝尔/CHSH实验中，测量基本身也 必须是不可预测的——因此，如果我们希望随机性总体上有所净增益，就必须谨慎地选择它们。这正是这系列研究工作 [24, 50, 60, 25, 46, 47] 如今几乎已经完全解决的问题。

基于贝尔/CHSH的认证随机性协议已经通过实验得到验证[18], , 甚至正在考虑将其实际部署于 NIST 随机信标 [36]„ 该信标每分钟生成 512 个随机比特。

这些协议的主要缺点在于，用户从互联网下载所谓的随机比特时，显然无法验证“爱丽丝”和“鲍勃”探测器之间是否无法通信——而这是安全性所需的关键假设。事实上，在某些贝尔/CHSH实验中，

[1]早期的一些研究探讨了玻色子采样是否可能有助于（例如）计算分子振电光谱[34] 或进行图相似性检测 [57], , 但高效的经典模拟粉碎了这些希望。[2]https://en.wikipedia.org/wiki/Dual_EC_DRBG [3] https://en.wikipedia.org/wiki/Ethereum

“爱丽丝”和 “鲍勃”就在几英尺之外！但即便他们不在附近，又如何证明这一点呢 d?

本文的核心洞见是，基于采样的量子霸权实验为认证随机性提供了一条截然不同的途径——这条途径只需要单个量子设备，而且如今切实可行。在我们的协议中，经典验证者使用一个较短的随机种子，伪随机地生成 n 量子比特的挑战电路 C_1、C_2.....随后，验证者将这些 C_i 电路逐个提交给量子计算机服务器，想必是通过标准互联网提交。对于每个 C_i，服务器都需要迅速作出响应——例如在一秒内——并返回来自 C_i 输出分布的独立样本 s_1、.....、s_k：也就是说，这一分布是在初始态 $|0^n\rangle$ 上运行 C_i，再在计算基中测量 $\{0,1\}^n$ 所得到的分布。

验证者可以从容地计算所谓的线性交叉熵基准，

$$\text{LXEB} := \sum_{j=1}^{k} |\langle s_j|C_i|0^n\rangle|^2,$$

针对至少一些挑战电路 C_i。如果 LXEB 分数足够高，我们的分析表明，在合理的计算假设下，验证者便可以确信，返回的样本中必定含有 $\Omega(n)$ 比特的真实最小熵。

换言之：即使是量子计算机，也需要 $\exp(n)$ 时间，才能生成通过 LXEB测试、却暗中是 C_i 的确定性或近乎确定性函数的样本。对于典型电路 C_i，输出分布中的诚实样本将包含 $n - O(\log n)$ 比特的最小熵。不诚实量子计算机可以 在一定程度上 降低返回样本的熵——例如，生成大量样本，然后只返回以 0 比特开头的样本。但要做得更好，例如找出通过 LXEB测试的字典序最小样本，或使 LXEB 得分最大化的样本，即便对量子计算机而言也应当是指数级困难的，需要使用振幅放大或类似方法（而次指数时间的经典算法则毫无胜算）。我们将在 第 2 节详细说明安全性归约，其目的只是将这些简单直觉形式化。

假设返回的样本（或足够多的样本）通过 LXEB测试，我们协议的最后一步是将它们输入经典的带种子的随机性提取器，以生成与均匀随机分布在全变差距离上呈指数级接近的输出比特。

退一步来看，许多人都指出了以下两者之间的密切类比：

1. 贝尔/CHSH实验排除了局域隐变量理论（并因此获得了诺贝尔物理学奖），以及 2. 基于抽样的量子霸权实验旨在排除“经典多项式时间隐变量理论”。

本文表明，这种类比还不止于此。在这两种情况下，实验最初的目的都只是证明某种量子现象确实存在，并排除任何经典解释；但随后，我们又将认证随机性作为证明的“免费副产品”获得。在这两种情况下，整个实验设置都取决于一个数值不等式——任何经典解释都必须满足该不等式，而量子力学预测该不等式可以被大幅违反，现实实验虽能违反该不等式，但违反程度低于量子力学所预测的最大值。在这两种情况下，任何 对该不等式的违反，最终都足以用于认证随机性。

最后需要指出的是，我们的协议本质上要求使用量子计算机。原因如下：考虑任意一个能够在经典概率多项式时间内模拟的服务器。

那么，根据定义，就不存在高效的方法来区分该服务器与这样一种模拟：其随机性已被伪随机数生成器的输出所替代。事实上，如果该伪随机数生成器的种子长度为 m 位，那么最优区分算法预计需要 exp(m) 时间——这意味着，即使给定我们允许用于验证的 $\sim 2^n$ 时间，验证者仍然无法区分诚实服务器与真熵仅有 m 位的服务器，对任意 $m \gg n$ 都是如此。

我们的实际量子协议如何避开上述不可能性论证？答案很简单：量子复杂性理论中一个反复用到的事实——我们无法从量子算法中"抽取随机性"（或量子性），例如将其替换为伪随机性；这与经典随机算法所能做到的类似操作不同。也可以这样说：我们的协议的安全性分析将依赖一个计算假设，即"长列表量子霸权验证"问题对于复杂性类 QCAM 来说是困难的，而它的经典对应版本显然并非如此。这背后的原因又与经典计算和量子计算之间一个根本差异密切相关：PostBPP（输出经过后选择的 BPP）包含于多项式层级之中，且可用近似计数进行模拟；而 PostBQP = PP 可以表达 #P 完全问题。

1.2 实践考量

我们的认证随机性协议可以在现有设备上进行演示，使用 $n = 60$ 个量子比特，或使用"量子霸权区间"内的其他数量。不过，在将该协议用于权益证明加密货币或任何其他关键应用之前，还有一些实际问题乃至概念性问题需要解决。

验证成本。目前，我们的协议有一个主要缺陷：为了检查服务器的输出，经典验证者需要计算线性交叉熵分数，而这预计需要 $\sim 2^n$ 时间——与经典欺骗所需的时间相近。这个缺陷直接源自随机线路采样以及其他所有当前的 NISQ 量子霸权方法本身。

由于验证成本，n（量子比特数）必须选得足够小，使得 2^n仍处于现有最强大经典超级计算机的能力范围之内。然而，这样一来，问题显而易见：只要经典欺骗者投入足够资源，2^n 也同样 在其能力范围内；这样一来，它就能预测并控制那些据称随机的比特。

尽管如此，我们认为并非毫无希望。关键在于，欺骗若要奏效，就必须持续进行：例如，如果每秒提交一次挑战电路，那么欺骗者也几乎必须每秒运行一次。即使（例如）每隔一 秒才使用一次真正的量子计算机，输出中也会包含大量真正的最小熵，足以确保协议安全。欺骗还必须快速——速度要与量子计算机本身一样快。

有人可能会反驳说，由于大多数模拟量子电路的经典算法都高度可并行化，要在严格的时限内仿冒我们的协议，"不过"是多花些钱购置经典计算硬件的问题。然而，当（例如） $n = 60$时，我们估计，要以每秒 exp(60) 次运算的速度运行，所需开支将高达数十亿美元，除了企业和民族国家之外，其他人都难以负担。

相比之下，验证只需偶尔进行。借助极少量的种子随机性，验证者可以选择协议中的 $O(1)$ 个随机轮次，并仅对这些轮次进行抽查。这样一来，恶意服务器即使伪造了（比如说）10% 的轮次，也几乎必然会被发现。验证还可以从容进行：只要验证者愿意事后抓住欺骗者，验证者就可以花费数小时甚至数天，而欺骗者所需的时间还不到

一秒。事实上，为了让服务器保持诚实，验证甚至未必真的需要进行：只要可信地威胁说它可能会进行验证，就足够了！

话虽如此，当然，如果能以 $n^{O(1)}$ 时间完成验证，同时以某种方式保留协议的“近中期量子特性”，那就更好了。

在我们看来，能否在含噪中等规模量子设备上实现基于采样的量子霸权，并进行高效的经典验证，已成为量子计算理论中最迫切的开放问题之一，即便不考虑本工作也是如此。我们的工作进一步凸显了这一问题的重要性：我们展示了解决该问题如何将安全、实用的认证随机性转变为量子计算机的首个真正应用。

交互性。 我们的协议面临的第二个实际问题，是验证者需要不断生成新的挑战电路，使其对量子计算服务器而言不可预测。我们完全可以问：如果验证者具备这种能力，那为什么还需要 量子计算机来生成随机比特呢?

简而言之，我们的协议在不可预测性方面实现了“升级”：挑战电路只需是伪随机的 （原因将在后文解释，针对的是量子统计零知识对手）。因此，验证者可以从单个初始随机种子确定性地生成所有电路。相比之下，协议的输出则保证是真正 随机的。

事实上，我们的协议具有一项颇具吸引力的“前向保密”特性。也就是说，即使我们设想验证者的伪随机数生成器未来会被攻破，只要服务器在协议运行时无法攻破伪随机数生成器，就不得不生成真正随机的比特。当然，无论密码分析未来取得怎样的进展，只要不依赖于这些比特本身，这些比特仍将不可预测。

谁来验证验证者? 不过，仍然存在一个难题：验证者会检查量子计算机的输出，但谁来检查验证者？如果验证者只是想将随机比特用于自己的私人用途，那就没有问题：例如，验证者可以使用我们的协议，检查由从不可信制造商处购买的量子计算机生成的随机比特。但请考虑权益证明加密货币这样的应用，其中经认证的随机比特需要与全世界共享。全世界会指定某个组织来担任验证者吗？如果是，那为什么这个组织不会像拥有量子计算机的组织一样遭到腐化或渗透呢？这就让我们回到了最初的问题。

经典密码学为这一困境提供了多种可能的解决方案。例如，可以由十几名或更多经典验证者分别生成各自的伪随机序列，再将这些序列进行异或运算，得到一个序列，用它生成挑战电路并发送给量子计算服务器。只要哪怕只有一名验证者希望该序列对服务器不可预测，那么它就会是不可预测的，前提是没有任何验证者能在其他验证者提交自己的序列之前看到该序列。

同样，我们可以问：如果我们信任这样的异或协议，为什么不直接使用它的输出，而跳过量子计算机呢？我们的回答仍然诉诸“随机性自举”：只要我们认同异或运算后的序列在实践中、就目前而言是不可预测的，那么量子计算机的输出就会从根本上 不可预测。因此，我们的协议提升了不可预测性的层级。

1.3 相关工作

我们并非首批提出利用量子计算机生成经认证的随机比特，并使其在某种计算困难性假设下保持安全的人。Brakerski、Christiano、Mahadev、Vazi-

rani 和 Vidick [20]提出了一种优雅的方案，该方案基于带误差学习（LWE）问题被认为是困难的这一假设。在后续工作中，Mahadev、Vazirani 和 Vidick [41] 证明，Brakerski 等人的协议每轮生成 $\Omega(n)$个随机比特，与我们的协议相当。

与我们的协议相比，Brakerski 等人协议的核心优势在于，其输出可在经典多项式时间内验证。另一方面，与我们的协议不同，他们的协议似乎难以甚至无法在含噪中等规模量子设备上实现，因为它要求在输入的叠加态上计算复杂的密码学函数。此外，他们的协议要求量子计算机在与验证者交互时保持相干叠加态，而交互很可能是通过互联网进行的。目前，这只有在某些硬件平台上才可行，例如囚禁离子平台；而在超导量子比特平台上则不可行（其相干时间以微秒计）。

最近，作为其关于相对于随机预言机实现 NP 搜索指数级量子加速这一突破的副产品，Yamakawa 和 Zhandry [63] 提出了另一种交互式协议，用于在随机预言机模型下认证 $\Omega(\log n)$ 个随机比特，并且还假设所谓的*Aaronson-Ambainis* 猜想 [3]。我们不知道 Yamakawa-Zhandry 协议是否仍能抵御纠缠对手，也不知道它是否会在多轮交互中累积熵。无论如何，他们的协议同样需要在输入的叠加态上计算复杂函数，这意味着几乎没有希望在含噪中等规模量子设备上运行该协议。

与这些早期工作不同，我们在此采用“极简主义方法”，利用量子计算机生成认证随机性：我们摒弃所有在叠加态中进行的密码学操作，只考察随机或伪随机量子电路的输出分布。选择这条路线，我们放弃了高效验证，但换来了在当前硬件上的可行性，并在概念上将认证随机性与基于采样的量子霸权本身统一起来。

近期，Bassirian、Bouland、Fefferman、Gunn 和 Tal 在基于我们其中一位作者（SA）此前未发表的、现于本文报告的研究成果所作宣布的基础上， [14] 迈出了分析如何利用基于采样的量子霸权实验实现认证随机性的第一步。他们的第一个结果表明，相对于随机预言机，任何用于傅里叶采样的高效量子算法，都必须在运行过程中产生 $\Omega(n)$ 比特的最小熵作为副产物。他们的第二个结果表明，长列表量子霸权验证（LLQSV）——我们困难性归约所针对的问题——相对于随机预言机，既不属于 BQP，也不属于多项式层级。为证明该问题不包含于多项式层级，他们基于 Raz 和 Tal [55]关于 BQP 与多项式层级之间突破性预言机分离的工作。

当然，这些结果与我们的工作密切相关，但尚未对我们的认证随机性协议进行可靠性分析。我们在至少四个方面超越了 [14]：

1. 我们证明，一个关于 LLQSV 的合理困难性假设意味着可以生成认证随机比特。该归约不依赖随机预言机。2. 我们为这一困难性假设提供黑盒证据。 ([14], 关于黑盒 LLQSV 不属于多项式层级 PH 的结果很有意思，也是新的，但对我们而言既非必要条件，也非充分条件。正如我们将要解释的，我们需要证明它不属于 QCAM/qpoly 类。）3. 我们证明了熵在多轮之间的累积。
4. 在黑盒设定下，我们证明了对纠缠对手的安全性。

我们的证明技巧也独立于[14]中的技巧。

最后，值得一提的是，Brandão 和 Peralta [22]已经报告了数值计算，以寻找适用于本文所述协议的恰当参数设置。

1.4 本文的历史

我们之一（SA）于2018年2月构想了认证随机性协议，以及其可靠性分析的基本要素（例如，LLQSV $\notin$ QCAM/qpoly 困难性假设）。随后，SA 就该提议进行了多次公开演讲（例如，[2]），尽管当时仅概述了该分析。这些演讲影响了后续关于量子霸权的工作：例如，谷歌团队在其2019年宣布其53量子比特 Sycamore 实验的论文中，将这些演讲列为动机 [12]。

遗憾的是，可靠性分析最终变得过于复杂，SA 无法独自完成。由于这一点及其他因素，本文的撰写工作被推迟了四年多。在本文中，我们不仅完成了 SA 于 2018年宣布的分析，还在随机预言机模型下证明了安全性，即使对手与量子计算机存在任意纠缠。这超出了 SA 在 2018年所声称的结果，也确实解决了当时提出的一个核心未解问题。

1.5 未来方向

仍有许多重要问题有待解决：

- 如前所述，也许最大的问题是设计一种基于采样的量子霸权实验，它既能在含噪中等规模量子设备上运行，也能进行高效的经典验证。如果能开发出这样的实验，那么根据我们在本文中的结果，我们预计，只需稍加改造，就能将其用于构建一种安全且可高效验证、能在现有设备上运行的可认证随机性方案。

- 除此之外，将我们的随机性协议从随机线路采样（RCS）改编到其他已知的量子霸权方案也很有意思，例如玻色子采样[4] 和瞬时量子多项式（IQP） [23]。对于玻色子采样，问题在于，我们目前缺少一个明确、定量的猜想，来描述多项式时间经典算法伪造线性交叉熵基准（LXEB）等测试所能达到的最佳水平。从 Aaronson 和 Arkhipov 于 2013年的研究 [5], 中我们知道，与我们对 RCS 的猜想不同，高效经典算法在玻色子采样中能够获得某种与深度无关的 Ω(1) LXEB 优势，但具体能达到多少？回答这个问题似乎是设计可认证随机性协议的先决条件，因为这将为玻色子采样实验在用于此类协议之前必须达到的表现设定下界。

- 当然，若能更多地了解作为我们协议安全性基础的核心困难性猜想究竟成立与否，那将非常理想——例如，“长列表量子霸权验证”（LLQSV）不存在 QCAM/qpoly 协议。若能在更弱的假设下证明我们协议的安全性，也将非常理想。我们至少能否去除指数长度的电路列表，并使用涉及单个量子线路的困难性假设?

- 在存在纠缠对手的情形下，我们目前只能在随机预言机模型中证明安全性。我们能否提出一个足以适用于该情形的合理困难性假设?

- 在某个合理的困难性假设下，我们能否收紧每个样本生成的最小熵数量的下界——甚至达到 $n - O(\log n)$ 的最大值? [4]

[4] $n - O(\log n)$ 是最大值，因为量子计算机总可以（例如）从正确分布中生成 $n^{O(1)}$ 个样本，直到找到一个其前 $O(\log n)$ 位全为 0 的样本。

• 同样地，即使我们反复使用同一个电路 C 进行采样，我们能否证明生成的最小熵仍会不断增加？显然，这里存在一个极限：一旦经过足够长的时间，使得欺骗者能够明确计算出 C 的整个输出分布，甚至可能将其存储在一个巨大的查找表中， C 就不再安全，需要替换为新的电路。但我们至少能达到这个极限吗？在我们能够达到的程度内，我们的协议在实践中将变得高效得多——尤其是考虑到（例如）在新电路上校准超导量子计算机所需的时间之后 C。

• 我们从 Haar 随机近似和大量数值证据中得知，给定一个随机量子电路 作为输入，理想诚实的量子计算机以压倒性的概率通过线性交叉熵基准 C 。在某种意义上，由于我们的安全性分析从未需要这一事实，经验性证据足以支持它！尽管如此，至少对于“自然”的量子电路系综而言，这一事实至今仍缺乏严格证明，实在令人诧异。在第 3.4.2 节中，我们在随机预言机模型下证明了这一事实，但能否直接证明它呢？近期研究表明，随机量子电路可以构成t设计[21, 33] ，这让我们向前迈进了一步，但似乎还需要一个额外的想法。

2 技术概述

2.1 我们的基本结果（无纠缠对手）

在本文中，我们始终令 C 表示作用于 n 个量子比特上的量子电路，并令 $N = 2^n$ 表示希尔伯特空间维数。令 P_C 表示由 $p_C(z) = |\langle z|C|0^n\rangle|^2$ 定义的概率分布。众所周知，当 $C \sim \text{Haar}(N)$ 为酉矩阵上的 Haar 测度时，我们有

$$\mathop{\mathbb{E}}_{C} \mathop{\mathbb{E}}_{z\sim P_C} [p_C(z)] = \frac{2}{N+1}. \tag{1}$$

2019年，Google [12] 宣布进行一项实验，以展示在以下任务上的量子优势，该任务称为线性交叉熵基准测试（LXEB）。

问题 1 （线性交叉熵基准测试 $\text{LXEB}_{b,\ k}(\mathcal{D})$ ）。 令 $\mathcal{D}$ 为定义在 n 个量子比特上的量子电路的概率分布。那么，$\text{LXEB}_{b,\ k}(\mathcal{D})$ 问题如下：给定从 $\mathcal{D}$ 中抽取的 C ，输出样本 z_1，.....， $z_k \in \{0,1\}^n$，使得

$$\frac{1}{k}\sum_{i=1}^{k} p_C(z_i) \geq \frac{b}{N}. \tag{2}$$

我们有时会省略参数 $\mathcal{D}$。

直观而言，我们预计，对于任意 $\text{LXEB}_{b,\ k}$ $\Omega(1)$，多项式时间经典算法都无法求解。相比之下，如果理想量子计算机只需在初始态 C 上反复运行 $|0^n\rangle$，在计算基下进行测量并返回结果，那么通过随机酉矩阵近似 C ，根据 (1) 我们预计，对于任意常数 $b < 2$，量子计算机都能以$1 - 1/\exp(k)$ 的成功概率求解 $\text{LXEB}_{b,\ k}$ 。与此同时，我们预计含噪量子计算机能够求解 $\text{LXEB}_{b,\ k}$ 其中 b 大于 1 但小于 2——事实上，经验观察到的结果正是如此，例如谷歌2019年实验达到了 $b \sim 1.002$。

本文的目标不仅是证明，在求解 $\text{LXEB}_{b,k}$ 时，量子相较于经典方法具有优势；还要证明量子采样相较于任何高效算法——无论是量子算法还是经典算法—— s_i在给定相同电路时，频繁返回相同结果 C。

为此，我们将采用一种新的、诚然并不常见的困难性假设，但我们认为它极有可能成立。我们的假设涉及以下问题：

问题 2（长列表量子霸权验证 LLQSV($\mathcal{U}$)）。给定对 $M = O(2^{3n})$ 量子电路 $C_1, \ldots, C_M$ 的预言机访问，每个电路作用于 n 个量子比特，并承诺它们是从分布 $\mathcal{U}$ 中独立抽取的。我们还获得了对 M 个字符串 $s_1, , \ldots, s_M \in \{0,1\}^n$ 的预言机访问。接下来，任务是区分以下两种情况：

1. **否例**：每个 s_i 都是从 $\{0,1\}^n$ 中均匀抽取的。
2. **是例**：每个 s_i 都是从 p_{C_i} 中抽取的，且 p_{C_i} 是 C_i 的输出分布。

我们称之为长列表困难性假设（LLHA$_B(\mathcal{U})$）的困难性假设如下，其中参数 $B < n$ 满足某些条件：

$$\text{LLQSV}(\mathcal{U}) \notin \mathsf{QCAMTIME}(2^B)/\mathsf{q}(2^B n^{O(1)}). \tag{3}$$

这里，QCAM（即量子经典亚瑟—梅林）是指这样一类问题：它们允许采用经典通信和量子验证者的 AM 协议。QCAMTIME(T) 是 QCAM 的推广，其中验证者可以使用运行时间 T（通信仍限制为多项式）。QCAMTIME(T)/q(A) 也相同，但验证者现在会接收 A 比特的量子辅助信息，且这些信息仅依赖于 n。

因此，我们的第一个主要结果如下。

定理 2.1（单轮分析，无旁信息，非正式表述）。设 $\mathcal{U}$ 是一个n量子比特量子电路上的分布，并假设 LLHA$_B(\mathcal{U})$ 成立。此外，设 $\mathcal{A}$ 是一个解决 LXEB$_{b,k}(\mathcal{U})$ 的多项式时间量子算法，其成功概率至少为 q。那么， $\mathcal{A}$的输出 $s_1, \ldots, s_k$ 满足

$$\Pr_{C' \sim \mathcal{U}}\left[H_{\min}(s_1 \ldots s_k | C = C') \geq B/2\right] \geq \left(\frac{bq-1}{b-1} - o(1)\right), \tag{4}$$

其中 $H_{\min}(\{p_i\}) :=$ 最小$_i$对数$_2 \frac{1}{p_i}$ 是最小熵。

举例来说，假设我们设定 $B := 0.49n$——我们所知的最佳上界， $B < n/2$来自 Grover 算法。再假设 $b = 1.002$，如 Google 的实验中那样 [12], 并且 k选择得足够大，使得 $q \geq 0.9990$ 根据大偏差不等式成立。那么 定理 2.1 告诉我们， $\mathcal{A}$的输出必须至少包含 $(0.12 - o(1))n$ 个随机比特。

有趣的是，尽管定理 2.1 是以最小熵来表述的，而且我们最终得到的多轮结果也将以最小熵来表述，但作为中间步骤，改用香农熵会更方便，因为熵累积定理使用的正是香农熵。当然，由于 $H_{\min}(\mathcal{D}) \leq H(\mathcal{D})$ 对每个分布 $\mathcal{D}$，定理 2.1 立即推出香农熵具有相同的下界。事实上，由于香农熵关于期望呈线性，定理 2.1 推出

$$H(s_1, \ldots, s_k | C) \geq \frac{B}{2} \cdot \left(\frac{bq-1}{b-1} - o(1)\right). \tag{5}$$

尽管 LLHA$_B(\mathcal{U})$ 确实是一个很强的假设，但我们的下一个结果证明它在随机预言机模型中成立，从而为该假设提供了依据：

定理 2.2 (LLQSV($\mathcal{U}$)的困难性，非正式表述)。给定一个随机预言机 $\mathcal{O}$，令 $\mathcal{U}$ 为以下 $M = 2^{O(n)}$ 量子电路 $C_1, \ldots, C_M$上的均匀分布；这些电路分别对互不相交的布尔函数 $f_1, \ldots, f_M$进行傅里叶采样： $\{0,1\}^n \to \{-1,+1\}$ 它们分别由 A定义。则 $\mathrm{LLHA}_B(\mathcal{U})$ 相对于 $\mathcal{O}$，对 B =Ω(n)成立。

这里我们概述证明。首先，我们将 LLQSV 归约到另一个称为布尔函数偏差检测（BFBD）的问题。在后一个问题中，算法可以访问M 个函数，这些函数从某个分布 $\mathcal{D}$ 或均匀分布中采样得到。分布$\mathcal{D}$可通过以下过程描述：首先，以概率 $N(1-2r/N)^2 \cdot \binom{N}{r} 2^{-N}$采样一个整数 $r \in \{0,1,\ldots,N\}$，然后采样一个大小为 r的随机子集 $R \subseteq \{0,1\}^n$，最后当且仅当 $x \in R$时，设定$f(x) = -1$ 。由于这两种分布都集中在 $r = N/2$附近，一个简单的混合论证便得出 BQP 的基本下界。随后，我们用类似的论证将困难性结果推广到交互式证明系统，具体来说，是双消息量子交互式证明类 QIP[2]：请回想，证明者的目标始终是说服验证者相信给定函数是从 $\mathcal{D}$中采样得到的。根据上述观察，我们可以在少数几个点上修改函数$f \sim \mathcal{D}$，从而得到一个随机函数。因此，若证明者能说服验证者接受 $f \sim \mathcal{D}$，也就能说服验证者接受一个随机函数。再由包含关系 QCAM ⊆QIP[2], ，可知 LLQSV 对 QCAM 是困难的。

为了证明非一致类 QCAM/qpoly （或将其推广为使用更多查询和更多辅助信息的情形）具有我们所需的困难性，我们注意到，根据 Aaronson 和 Drucker 的交换定理[8], QCAM/qpoly ⊆ QMA/poly，只需证明相对于后一个类的困难性。接着，我们改变预言机模型（而不改变问题本身），如下所示：预言机 $\mathcal{O}$ 包含 N 个区段，每个区段由一个 n 位字符串 x索引。获得预言机 $\mathcal{O}$访问权限、输入 x以及所有样本（也由 x索引）的非一致协议，需要判断样本 s_x 是否采样自 $\mathcal{O}_x$ 还是均匀分布（见 问题 2）。

显然，任何 LLQSV 求解器都能判断 s_x 是否采样自 $\mathcal{O}_x$，对每个 $x \in \{0,1\}^n$均成立。通过用随机猜测取代经典辅助信息，我们证明，任何能够解决该问题的 QMA/poly验证者，都意味着存在一个 $Nn^{O(1)}$查询的 QMA 验证者，能够以概率 N 解决 $2^{-\mathrm{poly}(n)}$个问题。接着，我们援引 Sherstov 的 强直接积定理，他证明了即使要达到成功概率 [58], ，计算 $2^{-\Omega(N)}$个 N 独立问题也需要Ω(Nd) 次查询，其中 d 是利用多项式方法得到的单个问题的查询下界。最后，我们通过证明单个问题具有指数级下界，导出矛盾。

基于上述单轮分析，下一步是证明熵在多轮中的累积。我们给出一个简单的 m 轮熵累积过程，使用 $\mathrm{LXEB}_{1+\delta,k}$ 作为 $m = n^{O(1)}$[5] 的验证，并采用常数 $0 < \delta < 1$。在每一轮中，对于 $\gamma = O(\log n/m)$，验证者以概率 $1-\gamma$ 发送与上一轮相同的电路，或以概率 γ 抽取一个新的随机电路。我们将连续发送同一电路的一段轮次定义为一个时期。[6] 以压倒性概率，时期数至多为 $O(\log n)$。验证者为每个电路选择 k 个随机样本，并检查验证者是否对 99% 的给定电路通过 $\mathrm{LXEB}_{1+\delta,k}$。应用熵累积定理（EAT，详见区段 2.4），我们证明以下结论。

定理 2.3 （熵累积，无旁信息，非正式表述）。对于 $\beta \in [0,1]$，如果 $\mathrm{LLHA}^{\beta n}$成立，那么对于整数 $k = \Omega(n^2)$ 和 $m = \Omega(\log n)$，存在一个 m-轮熵累积

[5]可能 m 会呈指数级增长，但我们在此不作进一步探讨。[6]Brakerski、Christiano、Mahadev、Vazirani 和 Vidick [20] 在分析其认证随机性协议时也使用了“时期”这一概念。

pro协议，使用 $k \cdot m$ 个样本，使得在以未中止事件 Ω 为条件时，

$$H_{\min}(Z|C)_{\rho|\Omega} \geq n\left(\left(0.99 - \frac{0.01}{\delta}\right)\frac{\beta}{2}m - O(\sqrt{m})\right) \tag{6}$$

对于每个求解 $\mathrm{LXEB}_{1+\delta}$ 的k设备，其中 ρ 是输出态，Z 是从设备接收的响应，C 是每一轮中的电路。

2.2 纠缠对手与理想测量

在上一节中，我们假设试图预测量子计算机输出的攻击者 Eve 与量子计算机之间没有预共享纠缠。现在我们放宽这一假设。

为了建立直觉，我们从一个特殊情况入手：量子计算机执行理想测量——也就是说，它“只是”对 n 个量子比特施加 C，然后在标准基下进行测量。唯一的问题是，这些量子比特的初始态可能不是所需的 $|0^n\rangle$，而是某个与 Eve 的量子比特纠缠的任意态。

我们定义以下理想化得分，称为 b-XHOG($\mathcal{U}$)。

问题 3 (b-XHOG($\mathcal{D}$)[39]). 对于分布 $\mathcal{D}$ 关于 n 个量子比特上的量子电路，若算法$\mathcal{A}$ 可以访问 $C \sim \mathcal{D}$，则称其求解了 b-XHOG，如果它输出一个样本 z，使得

$$\mathop{\mathbb{E}}_{C\sim\mathcal{D}}\left[\mathop{\mathbb{E}}_{z\sim\mathcal{A}^C}[p_C(z)]\right] \geq \frac{b}{N}. \tag{7}$$

对于一个能够访问 C 并输出 z的算法 $\mathcal{A}$，我们将$\mathcal{A}$的“XHOG 得分”定义为值 $\mathbb{E}_C[\mathbb{E}_{z\sim\mathcal{A}^C}[p_C(z)]]$。Kretschmer 最先考虑了这一得分，并用它在预言机模型 [39]中证明了随机线路采样的 Tsirelson 界。回想一下，在 CHSH 博弈中，违反经典界 $3/4$ 意味着可以获得认证随机性。有趣的是，我们的结果可以解释为：违反经典 XHOG 得分界所带来的认证随机性。

我们将首先分析 b-XHOG，并证明当设备解决$(1+\delta)$-XHOG 时，其冯·诺依曼熵下界为 $\Omega(\delta n)$。首先，该问题本身关于设备的输出分布是线性的：也就是说，对于得分分别为 $s_{\mathcal{A}}$ 和 $s_{\mathcal{B}}$的两个设备 $\mathcal{A}$，若第三个设备以概率 p 运行 $\mathcal{A}$，并以概率$(1-p)$运行 $\mathcal{B}$，那么它的得分为 $p \cdot s_{\mathcal{A}} + (1-p) \cdot s_{\mathcal{B}}$。这一线性条件与违反贝尔不等式时的得分计算一致。

更具体地说，回顾一下，为了从对贝尔不等式的违反中确立认证随机性，可以要求两个设备 $\mathcal{A}$ 和 $\mathcal{B}$ 进行例如 CHSH 博弈：验证者向设备发送两个问题 x、y，并收集响应 a、b。若 $x \wedge y = a \oplus b$，验证者将得分设为 1，否则设为 0；得分的期望定义为

$$\omega = \mathop{\mathbb{E}}_{x,y\sim\{0,1\}}\left[\mathop{\mathbb{E}}_{a,b\sim\mathcal{A}^x\otimes\mathcal{B}^y(\rho)}[\mathbb{I}[x \wedge y = a \oplus b]]\right]. \tag{8}$$

众所周知，可达到的最佳期望为 $\omega = \cos^2(\pi/8)$。对于认证随机性，进一步的研究表明，当期望为 $\omega \geq \cos^2(\pi/8+\varepsilon)$ 时，$\mathcal{A}$的输出具有以下界定的冯·诺依曼熵：$1 - h(\sin 4\varepsilon) \approx 1 - O(\varepsilon)$，其中 $h(x) := -x\log x - (1-x)\log(1-x)$ 是二元熵函数 [11]。与 XHOG得分 类似，这里的得分 ω 只有通过从相同设备获取无限多个样本才能精确计算。样本数量有限时，我们只能近似计算该得分。

在 m 轮序贯过程中，根据样本统计证明条件最小熵下界，归结为熵累积问题。认证随机性的熵累积定理（EAT）通常表述如下：在 m 轮序贯过程中，验证者随机选择 $O(\log m)$ 轮，以获得得分的近似值。如果该近似值足够接近 $\cos^2(\pi/8)$，则可提取随机比特的数量至少为 $\Omega(m)$ 乘以单轮分析中确定的冯·诺依曼熵下界。

不失一般性地，设设备与 Eve 共享的纠缠为纯态 $|\psi\rangle$。对于每个在 Z 上为经典的量子态 ρ_{ZE}，我们证明条件冯·诺依曼熵$H(Z|CE)_\rho \geq H(Z|C)_\rho - \chi(Z:CE)_\rho$，其中 χ 是 Holevo量。为说明为什么它们必须使用弱纠缠，我们可以将其写为 $|\psi\rangle := \sum_x \alpha_x |\psi_x\rangle|\phi_x\rangle$，其中 $\{|\psi_x\rangle\}$ 和 $\{|\phi_x\rangle\}$ 是施密特分解中的标准正交基。我们证明，对于求解 b-XHOG 的设备，当 $b \geq 1+\delta$ 时，振幅 α_x 必须集中于单个分量上，例如 x^*，使得 $|\alpha_{x^*}|^2 \geq \delta$。根据 Holevo量等于纠缠熵这一观察，我们在 Holevo量上建立上界$O((1-\delta)n)$。

在这个简化的设置中，我们已经看到，如果设备的 XHOG得分很高，那么它们必须使用弱纠缠才能通过验证。然而，整个分析都依赖于这样一个假设：设备必须执行理想测量。

2.3 完全通用设备

接下来，我们考虑对手可能与 Eve 共享任意纠缠的设置。我们在随机预言机模型中，为认证随机性给出无条件证明。

不同于第 2.1 节中为每个问答对设置二元得分的做法，对于问题 C 和响应 z，得分设为 $p_C(z)$。然后，在单轮分析中，我们首先证明，如果设备通过了$(1+\delta)$-XHOG 得分测试，那么联合态的冯·诺依曼熵至少为$\Omega(n)$。

定理 2.4 (单轮分析，非正式表述)。 每个设备 $\mathcal{A}$ 在输入双部态 ρ_{DE} 的第一系统并获得对 *Haar* 随机 C的预言机访问后，进行 $T \leq 2^{n/7}$ 次查询并解决$(1+\delta)$-XHOG 时，都必须输出一个与量子态 ψ_{ZE} 相距至多 $2^{-\Omega(n)}$ 的量子态，该量子态在系统 Z 上是经典的，使得

$$H(Z|CE)_\psi \geq 0.99\delta n - O(\log T). \tag{9}$$

此外，存在一种只需一次查询就能解决 $(2-2^{-n})$-XHOG 的设备。

为证明定理 2.4，关键观察在于：任意进行 T 次查询的设备 $\mathcal{A}$，若查询的是 Haar 随机 C，都可以用另一个不进行任何查询、但获得 k 个样本 z_1、.....、$z_k \sim P_C$（针对 $k = T^2 \cdot 2^{O(n)}$）的设备 $\mathcal{F}$ 来近似，菱形距离为 $2^{-\Omega(n)}$。对于每个 $\mathcal{A}$，我们将相应的设备 $\mathcal{F}$ 称为简化设备。以概率 $1-O(k^2/N)$，这些样本中不会出现任何碰撞。在此事件（即没有发生碰撞）下，若 $\mathcal{F}$ 能以至少 $\delta - o(1)$ 的概率输出 $z \in S = \{z_1, \ldots, z_k\}$，则意味着 $\mathcal{F}$ 能解决 $(1+\delta)$-XHOG。直观地说，这就稳健地证实了 $\mathcal{A}$ 的输出必定与这样一种策略相距不超过 ε：从 C 中采样 k 次，并从中选取一个样本来生成输出。

从这一角度来看，解决（$1+\delta$）-XHOG 的简化设备，等价于以至少 $\delta - o(1)$ 的概率赢得以下博弈：给定来自 P_C 的 k个独立样本 S，输出一个字符串 $z \in S$。尽管该博弈看起来相当简单，但它给出了冯·诺依曼最小熵的一个紧下界。根据无通信定理，即使 Eve 获知 P_C，她也无法获得提供给 $\mathcal{F}$ 的样本的信息，但当设备看到一组特定样本时，Eve 可能控制输出分布

由于以高概率，对 C 而言， P_C 的最小熵为 $n - O(\log\ n)$，我们证明，对支撑集为这些样本的任意分布取平均后，所得分布的冯·诺依曼熵至少为 $0.99\delta n - O(\log\ T)$。

我们在定理 2.4 中给出的下界接近最优。考虑一种设备，它以概率 P_C从 δ 中采样，并以概率 $1-\delta$ 输出一个均匀分布的字符串；该字符串是通过对与 Eve 共享的 EPR 对进行标准基测量得到的。在前一种b事件中，该设备以 $b \approx 2$解决1-XHOG；而在后一种情况下，输出是一个均匀随机字符串，可解决1-XHOG。因此，根据线性性，该设备可解决 $(1+\delta)$-XHOG。该设备输出的联合经典-量子态是这两种量子态的概率混合。此外，对于 C的选择，以压倒性概率， P_C 的香农熵为 $n - O(\log n)$。由冯·诺依曼熵的凹性可知，输出的条件冯·诺依曼熵为 $\delta n - o(n)$。

为了累积熵，我们给出一个与第 2.1 节中介绍的过程非常相似的序贯过程：验证者采样 $t = O(\log n)$ 个不同的电路，并要求每个电路至少提供 k个样本。收到这些样本后，验证者为每个电路选取 k 个随机样本，并检查设备是否对常数 δ 通过 $\mathrm{LXEB}_{1+\delta,\ k}$，且适用于 99% 的电路。我们证明，该累积过程可认证 $\Omega(\delta mn)$ 比特。

定理 2.5 （来自一般设备的熵累积，非正式表述）。 对于整数 $k = \Omega(n^2)$、 $m = \Omega(k \log n)$，存在一个熵累积协议，使用 m 个样本，使得在未中止事件 Ω 的条件下，

$$H_{\min}(Z|CE)_{\rho|\Omega} \geq n\big(0.99\delta m - O(\sqrt{m})\big) \tag{10}$$

对于求解 $\mathrm{LXEB}_{1+\delta的k}$设备，其中 ρ 是输出态， Z 是设备提供的样本， C 是电路， E 是 *Eve* 持有的信息。

更具体地说，取 $\delta = 0.1$，该界为 $n \cdot (0.099m - O(\sqrt{m}))$，使用设备提供的 m 个样本即可得到。我们注意到，该界表面上弱于 定理 2.3中的界，但样本数量为 m （而非 km，如 定理 2.3 中所示）。这两个协议所需的最小样本复杂度并无不同——对于完美设备，要以压倒性概率通过验证，所需样本数均为 $\Omega(n^2 \log n)$。出于技术原因，在后一个协议中，每次验证所用的 k 个样本会从设备针对同一挑战电路发送的所有样本中随机选取，并依次接收。相比之下，在前一个协议中，设备每轮都要发送 k 个样本，验证者则针对每个电路检查一轮。

我们还要指出，定理 2.3 和 定理 2.5 是不可比较的结果。特别是，定理 2.5 的安全性分析高度依赖这样一种模型：设备可以访问电路以及电路上的分布（Haar 测度）。相比之下，基于 LLHA 的安全性分析在设备能够访问从其他分布中采样得到的电路描述时，仍可能成立。我们将以下问题留作开放问题：是否存在一种困难性假设，使得线性交叉熵基准测试能够在普通模型下针对纠缠对手证明最小熵。

2.4 熵累积

定理 2.5 的证明基于 Dupuis、Fawzi 和 Renner 提出的熵累积定理（EAT） [28], ，并作如下修改。设 f 为一个仿射函数，称为最小权衡函数，使得在单轮分析中可以证明 $H(Z|E)_\rho \geq f(q)$对于分布 $q = (p, 1-p)$ 以及任意量子态 ρ，其接受概率为 p。在一个 m轮的序贯过程中，验证者通过计算决策来检查 γm 轮（称为测试轮次）

比特，并根据样本计算近似分布 $\tilde{q} = (\tilde{p}, 1-\tilde{p})$。随后，跨越 m 轮的最小熵为 $m \cdot f(\tilde{q}) - O(\sqrt{m})$。因此，熵累积定理将多轮分析简化为对单轮冯·诺依曼熵下界的求取。

由于我们采用 b-XHOG 得分来界定单轮分析中的冯·诺依曼熵，因此从测试轮次中获得的得分不再由二元随机变量计算。于是我们定义一个新的最小权衡函数 f'，它将得分映射为冯·诺依曼熵的下界。随后我们证明，如果定义为 $p_{C_i}(z_i)$ 平均值的得分近似值大于 s，那么累积熵至少为 $m \cdot f'(s) - O(\sqrt{m})$。

熵累积过程允许进行抽查，也就是说，在 m 轮过程中，验证者不再对每一轮 $i \in [m]$ 都计算 $p_{C_i}(z_i)$，而只对大小为 $O(n^2 \log n)$ 的索引子集 i 计算 $p_{C_i}(z_i)$。更具体地说，验证者会改变 O 的电路 n 次（log 次），并在每个时期计算 $k = O(n^2)$ 个样本的平均值。测试轮次的数量是为设备设定的，使其在每个电路 C 上从 p_C 中独立同分布地抽取样本，并以压倒性概率通过验证。根据霍夫丁不等式，一个从 p_C 输出中抽取 k 个样本的设备，其平均得分以压倒性概率集中在典型 C 的 $2 - O(1)$ 之上。如果验证者通过 $\mathrm{LXEB}_{b,\,k}$ 个时期（其比例足够大，为 $\Omega(1)$），则平均值以压倒性概率高于 $1 + \Omega(1)$；根据熵累积定理，条件最小熵为 $\Omega(nm)$。

2.5 伪随机性与统计零知识

认证随机性协议依赖于完美随机性来生成挑战电路。然而，通过计数论证可知，挑战空间是双指数规模的，要计算真正随机的电路，需要指数数量的随机比特。为了获得随机性净增益，我们必须依赖一种可高效计算的函数：它使用多项式数量的随机比特，并生成安全级别足以满足我们目的的伪随机性。

然而，针对量子多项式时间对手的伪随机函数（PRF）的标准概念似乎并不充分，因为它只能保证设备的输出是伪随机的！因此，对于认证随机性，我们需要一种更强的伪随机函数：用它替代真正随机的函数后，输出仍与均匀分布在统计上不可区分。

为了提供这样的安全保证，我们构造了一种伪随机函数，使其对于任意 QSZK 协议都与真正随机的函数不可区分。为理解为何这样的安全级别足够，我们回顾一下 QSZK 类的相关事实：该类由能够构造量子统计零知识协议的承诺问题组成。QSZK 协议包含一个证明系统，即一个量子多项式时间验证者和一个无界证明者，以及一个高效的量子模拟器；后者无需访问见证即可模拟证明系统的交互。

Watrous 证明了量子统计零知识有一个自然的完全问题，称为量子态可区分性问题（QSD）[61]。在这个问题中，实例是由两个可高效计算的量子电路组成的元组 Q_0，Q_1。对于 $\alpha \in (0, 1]$，验证者需要判断迹距离 $\|\rho_0 - \rho_1\|_{\mathrm{tr}}$ 至少为 α，还是至多为 α^2，其中 ρ_b 是通过计算 Q_b 得到的边缘态，适用于 $b \in \{0, 1\}$。已知该类问题存在放大过程，因此可以将间隙缩小到指数级接近 1 [61]。最近，Menda 和 Watrous 证明，相对于随机预言机，$\mathsf{UP} \not\subset$ 量子统计零知识 [44]。Ben-David 和 Kothari 为统计零知识证明定义了一种查询度量，并证明正权对手方法对于某些问题只能给出次优下界 [16]。

关于经认证的随机性 随机性，我们定义两个分布之间的 QSZK 可区分性 r

fun，并且可以将类似的定义扩展到酉算子上的分布。

定义 2.6 (QSZK-可区分性，非正式)。 若存在一对算法 $\mathcal{D}_0, \mathcal{D}_1$ ，使得 $\mathcal{A}^F$ 与 $\mathcal{B}^F$ 的输出态之间的平均迹距离在 $F \sim \mathcal{D}_0$ 和 $F \sim \mathcal{D}_1$ 之间存在非可忽略差异，则称两个关于函数的分布 $\mathcal{D}_0, \mathcal{D}_1$ 是 QSZK- 可区分的。若不存在这样的算法，则称这些分布是 QSZK 不可区分的。

QSZK 安全伪随机函数定义为与随机函数 QSZK 不可区分的函数。我们提出一个称为伪随机函数假设（PRFA）的假设，即存在 QSZK 安全伪随机函数。我们通过给出一种构造来证明该假设成立，该构造适用于可访问该函数预言机的算法。

定理 2.7 (伪随机函数，非正式)。 相对于随机预言机，存在一个密钥长度为 $O(n)$ 的QSZK 安全伪随机函数。

类似地，如果伪随机酉算子与随机酉矩阵 QSZK 不可区分，我们就称它是 QSZK 安全的。我们提出一个类似的假设，称为伪随机酉算子假设（PRUA）：存在一个 QSZK 安全的伪随机酉算子，并证明相对于一个密钥长度为 $O(n)$ 的预言机，该假设成立。

在这些假设下，用伪随机电路替换随机电路时，输出在给定 Eve 的侧信息的条件下，仍与均匀分布在统计上不可区分。要理解其中的原因，请回想 De、Portmann、Vidick 和 Renner [26] 证明了 Trivesan 随机性提取器 [59] 是量子安全的。也就是说，随机性提取器的输出与 Eve 的侧信息构成的量子态 ρ 在统计上与 $\sigma \otimes \rho_E$ 不可区分，其中 σ 是最大混态，而 ρ_E 是 Eve 持有的边缘态。如果接收伪随机电路的设备输出某个量子态，使得该态与 $\sigma \otimes \rho_E$ 之间的距离变化达到非忽略量级，那么这样的设备就意味着存在一个 量子统计零知识 协议，可以区分伪随机电路和随机电路。

为了看出随机性确有净增益，该协议会采样 $O(\log n)$ 个伪随机电路，每个电路使用 $O(n)$ 个随机比特作为伪随机函数的密钥，最终产生 $\Omega(mn)$ 个随机比特。对于 $m = \text{poly}(n)$，我们有多项式扩展。

虽然我们不知道更弱的假设能否用于认证随机性，但面对纠缠对手时，这一安全级别似乎是必要的。确实，如果不存在量子侧信息，那么我们只需使用能够抵御求解与均匀分布的统计差异问题的对手的伪随机电路。在纯经典情形下，该问题已知是 NISZK 完全的；NISZK 是 SZK 的一个子类，由那些允许非交互式统计零知识协议的问题组成 [31]。然而，在存在量子侧信息时，无界的 Eve 可以制备任意 ρ_E，因此似乎有必要确保对 QSZK 的安全性。

3 预备知识

如前所述，电路 C 作用于 n 个量子比特，且 $N = 2^n$。二元熵函数 $h : [0,1] \to \mathbb{R}$ 定义为 $h(x) := -x \log x - (1-x)\log(1-x)$，并且 $h(0) = h(1) = 0$。对于矩阵 A，我们用 $\|A\|_p := \text{tr}(|A|^p)^{1/p}$ 表示其 Schatten p-范数。此外，我们用 $\|A\|_{\text{op}}$ 表示算子范数，用 $\|A\|_F := \left(\sum_{i=1}^n \sum_{j=1}^n |A_{ij}|^2\right)^{1/2}$ 表示 $n \times n$ 矩阵 A 的 Frobenius范数。两个量子态 ρ, σ 之间的迹距离定义为 $\|\rho - \sigma\|_{\text{tr}} := \frac{1}{2}\|\rho - \sigma\|_1$。两个量子态 ρ, σ 之间的保真度 $F(\rho, \sigma)$ 定义为 $\|\rho^{1/2}\sigma^{1/2}\|_1$。函数 F 是对称的，即 $F(\rho, \sigma) = F(\sigma, \rho)$。如果 ρ 是一个纯态 $|\psi\rangle$，那么保真度 $F(\rho, \sigma) = \langle\psi|\sigma|\psi\rangle$。

量子过程是完全正迹保持（CPTP）映射。对于整数 $n, m > 0$，令 $\Phi\colon M_n(\mathbb{C}) \to M_m(\mathbb{C})$ 表示从复值 $n \times n$ 矩阵 $M_n(\mathbb{C})$ 到 $M_m(\mathbb{C})$ 的线性变换。Φ 的菱形范数定义为 $\|\Phi\|_\diamond := \max_{X \in M_n(\mathbb{C}):\, \|X\|_1 \le 1} \|\Phi \otimes \mathbb{I}_n(X)\|_1$。两个量子过程 Φ 和 Ψ 之间的菱形距离定义为 $\|\Phi - \Psi\|_\diamond$。

对于希尔伯特空间 A，我们将 $A(A)$ 记为 A 中归一化量子态的集合。对于希尔伯特空间 A、B，我们将 $\mathrm{CPTP}(A, B)$ 记为从 A 上的线性算子映射到 B 上的线性算子的完全正迹保持映射集合。A 上的酉算子集合记为 $\mathbb{U}(A)$。

3.1 复杂性类

我们假设读者熟悉标准经典复杂性类和 BQP 类。下面我们简要介绍与本文工作相关的量子复杂性类。QMA 类（即“量子 Merlin–Arthur”）是 MA 的量子类比，定义如下。

定义 3.1（QMA）。复杂性类 QMA由满足以下条件的语言 L 组成：存在一个量子多项式时间算法 V，使得以下条件成立。

- 如果 $x \in L$，则存在一个作用于 $\mathrm{poly}(|x|)$ 个量子比特上的量子态 ρ，使得 $\Pr[V(x, \rho) \text{ 接受}] \ge 2/3$.
- 如果 $x \notin L$，则对于每个作用于 $\mathrm{poly}(|x|)$ 个量子比特上的量子态 ρ，$\Pr[V(x, \rho) \text{ 接受}] \le 1/3$。

量子多项式时间算法 V 也称为 QMA 验证器，而量子态 ρ 可以被视为由拥有无限能力的 QMA“证明者”发送的量子态。QCMA 也是 MA 的量子类比，其定义方式与 QMA 类似，不同之处在于见证态 ρ 被限制为经典字符串。为了明确 QMA 验证器的运行时间或查询复杂度，我们将 $\mathrm{QMA}(T)$记作在相对化世界中运行时间为 T 或进行 T 次查询的 QMA 验证器。相同的记法也适用于其他类。

QCAM 类（代表“量子-经典 Arthur–Merlin”）是 AM 的量子类比，可以用两消息协议来定义。在第一条消息中，量子多项式时间验证者向证明者 Merlin 发送一个随机字符串 r，其长度关于实例的大小是多项式级的。随后 Merlin 发送响应 w（也称为见证），其长度关于实例的大小同样是多项式级的。注意，见证 w 可以任意依赖于实例和随机字符串 r。如果存在一个 Arthur，使其对每个实例都以至少 $2/3$的概率输出正确答案，则称语言属于 QCAM。

定义 3.2 (QCAM)。复杂性类QCAM由满足以下条件的语言 L 组成：存在一个量子多项式时间算法 V（也称为 *Arthur*）和一个多项式 p。

- 如果 $x \in L$，则存在一个多项式 q 和一个经典字符串 $w \in \{0,1\}^{q(|x|)}$，使得

$$\Pr_{r \in \{0,1\}^{p(|x|)}}[V(x, r, w) \ \textit{accepts}] \ge 2/3. \tag{11}$$

- 如果 $x \notin L$，那么对于每个多项式 q 和每个字符串 $w \in \{0,1\}^{q(|x|)}$，

$$\Pr_{r \in \{0,1\}^{p(|x|)}}[V(x, r, w) \ \textit{accepts}] \le 1/3. \tag{12}$$

一个包含 k 条消息的交互式证明系统由两个算法组成：计算能力无界的证明者 P和多项式时间验证者 V； V与 P之间进行 k 次消息交换。我们还将这种协议称为长度为 k 的验证者。QIP 是一种交互式证明系统，其中验证者以量子多项式时间运行，并且每条消息都可以是量子态。这种协议也称为量子交互式证明系统。

定义 3.3 (量子交互式证明$[k]$)。 复杂性类 量子交互式证明$[k]$ 由满足以下条件的语言 L 构成：存在一个量子多项式时间算法 V （也称为验证者），其长度为 k 。

- 若 $x \in L$，则存在一个证明者 P，使验证者以概率 2 /3.
- 若 $x \notin L$，则对于任意证明者 P，验证者 V接受的概率至多为 $1/3$。

复杂性类 量子统计零知识（QSZK 是“量子统计零知识”的缩写）由能够进行 Watrous 定义的量子统计零知识协议的语言构成 [61]。

定义 3.4 (量子统计零知识)。 语言 L 的量子统计零知识证明系统由一个无界的 P （称为诚实证明者）以及一个量子多项式时间验证者 V 组成，并满足以下条件。

- 完备性和可靠性：$(V,\ P)$ 是针对 L的证明系统。
- 零知识：存在一个可忽略函数 η 和一个可制备态集合 $\{\sigma_{x,i}\}$ ，使得如果 $x \in L_1$, $\|\sigma_{x,\ i} -$ 视图$_{V,\ P}(x,\ i)\|_{\mathrm{tr}} \leq \eta(|x|)$。这里，视图$_{V,\ P}(x,\ i)$ 是验证者在第 i 轮之后的验证者视图，即在以 x 为输入执行证明系统的过程中发送第 i 条消息后，验证者与消息量子比特的混合态。

Watrous 证明，量子统计零知识具有一个自然的完全问题，称为量子态可区分性（QSD） [61], ，定义如下。

定义 3.5 ($(\alpha,\ \beta)$-QSD)。 承诺问题 $(\alpha,\ \beta)$-QSD $=(\mathrm{QSD}_1, \mathrm{QSD}_0)$ 对于 $0 \leq \alpha < \beta^2 \leq 1$ ，由一对量子电路 $(Q_0,\ Q_1)$ 组成，使得

- 如果$(Q_0,\ Q_1) \in \mathrm{QSD}_1$，则 $\|\rho_0 - \rho_1\|_{\mathrm{tr}} \geq \beta$，并且
- 若$(Q_0,\ Q_1) \in \mathrm{QSD}_0$，则 $\|\rho_0 - \rho_1\|_{\mathrm{tr}} \leq \alpha$,

其中 ρ_b 由在零态上应用 Q_b ，再对部分量子比特取部分迹得到。

Watrous 证明了，通过给出一个从 Q_b 到某个电路的变换，该电路的规模关于 n 和 $|Q_b|$ 为多项式（对于$b \in \{0,1\}$ [61]），可以将完备性和可靠性参数（α，β）放大为（2^{-n}，$1–2^{-n}$）。由于对于这个问题而言这些参数并不重要，我们将具有常数间隔的同一问题记为 QSD。

该问题有一个非常简单的 QSZK 协议：验证者抛掷一枚随机硬币 b，并将 ρ_b 发送给证明者。证明者执行使迹距离达到饱和的最优测量，并输出一位比特 b'。若 $b = b'$，验证者便接受。完备性源于这样一个事实：这些量子态的迹距离与 1 的差距可忽略不计，这意味着存在一种能够完美区分这些量子态的测量。对于可靠性，由于这些量子态在迹距离上仅有可忽略的差异，证明者无法比随机猜测取得不可忽略的优势。为了证明

该协议是零知识的，量子模拟器会先应用验证者的量子操作。收到证明者的回复 b' 后，它将 $b' = b$设为相应的值。

The QSZK-完备性 QSD可以相对化。特别是，Menda 和 Watrous [44] 证明了，对于预言机 A，问题 L_A 属于 QSZK^A 当且仅当存在一个从 L_A 到 QSD^A的归约。

定理 3.6 ([44, 定理 1])**.** 对于字母表 Σ, Γ，设 $L \subseteq \Gamma^*$ 为一个语言， $A \subseteq \Sigma^*$ 为一个预言机。语言 L_A 属于 QSZK^A ，当且仅当存在一个由成对的相对化量子电路组成的多项式时间一致族 (Q_0^A, Q_1^A)，满足以下性质：

- 如果 $x \in L_A$，那么 $(Q_0^A, Q_1^A) \in \mathrm{QSD}_1^A$。
- 如果 $x \notin L_A$，那么 $(Q_0^A, Q_1^A) \in \mathrm{QSD}_0^A$。

Ben-David 和 Kothari [16] 独立地研究了所谓的函数 f 的 QSZK 复杂度，记作 QSZK(f)。它定义为一对查询算法$\mathcal{A}$、$\mathcal{B}$在获得对 x 的预言机访问时所进行的最小查询次数 k，使得对于每个 x，满足：(i) 若 $f(x) = 1$，则 $\|\mathcal{A}^x - \mathcal{B}^x\|_{\mathrm{tr}} \geq 2/3$；(ii) 若 $f(x) = 0$，则 $\|\mathcal{A}^x - \mathcal{B}^x\|_{\mathrm{tr}} \leq 1/3$。

3.2 多项式方法

Beals、Buhrman、Cleve、Mosca 和 de Wolf 提出的量子多项式方法，是证明查询问题量子下界的标准技术[15]。具体而言，我们将使用 Markov 给出的次数下界，以及 Sherstov 给出的强直接积定理 [58]。

引理 3.7。令 $p: \mathbb{R} \to \mathbb{R}$ 为一个多项式。对于实数 a，b，若

$$\max_{a \leq x \leq b} |p(x) - p(y)| \leq H, \tag{13}$$

then

$$|p'(x)| \leq \frac{H}{b-a} \deg(p)^2, \tag{14}$$

其中 p' 是 p 的一阶导数，而$\deg(p)$ 是 p的次数。

定理 3.8 （强直接积定理[58, 定理 1。5]）。固定函数 f_1、……、f_k：$\{-1,+1\}^m \to \{-1,+1\}$。以最坏情况概率 $2^{-\Omega(k)}$ 求解 （f_1、……、f_k） 需要

$$\Omega\left(\min_{S \subseteq [k]: |S| = 0.99k} \left(\sum_{i \in S} \deg_{1/5}(f_i)\right)\right), \tag{15}$$

其中 $\deg_\varepsilon(f)$ 是 实多项式近似 f 且逐点误差不超过 ε 时的最小次数 .

3.3 量子信息理论

可提取随机性的数量即为条件最小熵 $H_{\min}(Z|E)$，它描述了在给定 Eve 的信息 E的条件下，系统 Z 所具有的随机性数量。平滑最小熵的正式定义如下：

$$H_{\min}(Z|E)_\rho = \sup_{\sigma_E} \left\{ -\inf_{\lambda} \left\{ \lambda : \rho_{ZE} \leq 2^{-\lambda} \mathbb{I}_Z \otimes \sigma_E \right\} \right\}. \tag{16}$$

当 Z 和 E 都是经典的时，它们被正式定义为随机变量，并且 ρ_{ZE} 和 σ_E 都在同一基底下是对角的。

我们还将考察条件最小熵的平滑版本。该版本通过考虑一对全变差距离小于 ε 的随机变量，放宽了上述定义：

$$H_{\min}^{\varepsilon}(Z|E)_\rho = \sup_{\tilde{\rho}:\|\tilde{\rho}_{ZE}-\rho_{ZE}\|_{\mathrm{tr}}\leq\varepsilon} H_{\min}(Z|E)_\rho. \tag{17}$$

量子Rényi熵这一类熵中另一个有用的量是冯·诺依曼熵。量子态 ρ_A 的冯·诺依曼熵定义为 $H(A)_\rho := -\mathrm{tr}(\rho\log\rho)$。双部态 ρ_{AB} 的条件冯·诺依曼熵定义为 $H(A|B)_\rho = H(AB)_\rho - H(B)_\rho$。

对于按照分布 P 分布的经典随机变量 X，我们用 $H(X)$ 或 $H(P)$ 表示 X 的冯·诺依曼熵，并用 $H_{\min}(X)$ 或 $H_{\min}(P)$ 表示 X 的最小熵。

以下关于冯·诺依曼熵的不等式将会很有用。

引理3.9。对于有限维希尔伯特空间 A，B，C 以及定义在 $A\otimes B\otimes C$ 上的三体态 ρ_{ABC}，有

$$H(A|B)_\rho + H(B|C)_\rho \geq H(A|C)_\rho. \tag{18}$$

证明。根据强次可加性，$H(A|BC)_\rho \leq H(A|B)_\rho$ 因此

$$\begin{aligned} H(B|C)_\rho &= H(AB|C)_\rho - H(A|BC)_\rho \\ &\geq H(A|C)_\rho - H(A|B)_\rho. \end{aligned} \tag{19}$$

□

引理 3.10。设有限维希尔伯特空间为 A，ρ,σ 是定义在其上的两个归一化量子态。对于 $\lambda\in[0,1]$，

$$H(A)_{(1-\lambda)\rho+\lambda\sigma} \leq (1-\lambda)H(A)_\rho + \lambda H(A)_\sigma + h(\lambda) \tag{20}$$

其中 h是二元熵函数。

证明。定义量子态

$$\psi_{BA} = (1-\lambda)|0\rangle\langle 0|_B\otimes\rho_A + \lambda|1\rangle\langle 1|_B\otimes\sigma_A. \tag{21}$$

根据定义，ψ 的冯·诺依曼熵为

$$\begin{aligned} H(BA)_\psi &= -\mathrm{tr}((1-\lambda)\rho\log(1-\lambda)\rho)) - \mathrm{tr}(\lambda\sigma\log\lambda\sigma)) \\ &= -(1-\lambda)\log(1-\lambda) - (1-\lambda)\mathrm{tr}(\rho\log\rho) - \lambda\log\lambda - \lambda\mathrm{tr}(\sigma\log\sigma) \\ &= H(A)_\rho + H(A)_\sigma + h(\lambda). \end{aligned} \tag{22}$$

此外，由于 $\mathrm{tr}_B(\psi) = (1-\lambda)\rho+\lambda\sigma$, $H(A)_\psi = H(A)_{(1-\lambda)\rho+\lambda\sigma}$。由于条件冯·诺依曼熵总是非负的，$H(BA)_\psi \geq H(A)_\psi$，由此得证。 □

引理3.11 ([48, 定理 11。9])。对于希尔伯特空间 A，设 ρ 是定义在 A 上的量子态，且 $\{P_i\}$是定义在 A 上的一组完备投影测量。那么，测量后态$\sigma = \sum_i P_i\rho P_i$ 的熵至少与原始熵相等，即 $H(A)_\sigma \geq H(A)_\rho$。

根据 引理3.10 以及冯·诺依曼熵的凹性，我们可以用各个分量互信息的凸组合，给出状态概率混合的互信息下界。回顾一下，根据定义，对于希尔伯特空间 A，B 以及双部态 ρ_{AB}，$I(A:B)_\rho = H(A) + H(B) - H(AB)$。

引理 3.12。对于有限维希尔伯特空间 A 和 B，令 ρ_{AB}，σ_{AB} 为一个双体量子态。对于$\lambda \in [0,1]$,

$$I(A:B)_{(1-\lambda)\rho+\lambda\sigma} \geq (1-\lambda)I(A:B)_\rho + \lambda I(A:B)_\sigma - h(\lambda).$$

证明。根据冯·诺依曼熵的凸性，对于 $X \in \{A, B\}$,

$$H(X)_{(1-\lambda)\rho+\lambda\sigma} \geq (1-\lambda)H(X)_\rho + \lambda H(X)_\sigma. \tag{23}$$

然后根据引理 3.10,

$$\begin{aligned} I(A:B)_{(1-\lambda)\rho+\lambda\sigma} &= H(A)_{(1-\lambda)\rho+\lambda\sigma} + H(B)_{(1-\lambda)\rho+\lambda\sigma} - H(AB)_{(1-\lambda)\rho+\lambda\sigma} \\ &\geq (1-\lambda)I(A:B)_\rho + \lambda I(A:B)_\sigma - h(\lambda). \end{aligned} \tag{24}$$

□

3.4 Haar 随机酉矩阵

我们将依赖以下事实。对于 Haar 随机酉矩阵 $C \in \mathbb{C}^{N\times N}$，对于每个 $i \in \{0,1\}^n$，密度 P 的分布 $P_z = p_C(z) := |\langle z|C|0\rangle|^2$ 服从概率单纯形 [27, 39]上的狄利克雷分布 狄利克雷分布(1^N) 。

3.4.1 狄利克雷分布

令 Dir(α) 表示浓度超参数为 α 的狄利克雷分布。关于 $(X_1, \ldots, X_N) \sim$Dir(α) 对于 $\alpha = (\alpha_1, \ldots, \alpha_N)$ 的矩已有深入研究。首先，每个随机变量的均值为 $\mathbb{E}[X_i] = \frac{\alpha_i}{\alpha_0}$，其中 $\alpha_0 = \sum_{i=1}^N \alpha_i$。此外，

$$\mathbb{E}\left[\prod_{i=1}^N X_i^{\beta_i}\right] = \frac{B(\alpha+\beta)}{B(\alpha)}, \tag{25}$$

其中 $B(\alpha) := \frac{1}{\Gamma(\alpha_0)}\prod_{i=1}^N \Gamma(\alpha_i)$。

狄利克雷分布是类别分布和多项分布 [30] 的共轭先验分布。如果先验分布按照狄利克雷分布进行采样，则后验也服从具有不同超参数的狄利克雷分布。具体而言，设数据点为 z_1、...、$z_k \sim P$，其中 $P \sim$Dir(α)。那么后验分布 $P|(z_1, \ldots, z_k) \sim$Dir$(\alpha + m)$，其中 m 是各类别中数据点出现次数所组成的向量。

我们可以通过以下过程，从狄利克雷分布 Dir(α) 中抽取一个概率分布：首先，对 $i \in [N]$ 独立地抽取 $Q_i \sim \Gamma(\alpha_i, 1)$，其中 $\Gamma(\alpha_i, 1)$ 是参数为 $\alpha_i, 1$ 的伽马分布。然后计算 $\bar{Q} = \sum_{i=1}^N Q_i$ 并为每个 $i \in [N]$ 设置 $P_i = Q_i/\bar{Q}$。因此，简要介绍一些关于伽马函数的性质会很有帮助。回顾一下，伽马分布 $\Gamma(\alpha, \beta)$ 的概率密度函数为

$$f(x;\alpha,\beta) = \frac{\beta^\alpha e^{-\beta x} x^{\alpha-1}}{\Gamma(\alpha)}. \tag{26}$$

特别地，对于 $\alpha = \beta = 1$，概率密度函数为 $f(x; 1, 1) = e^{-x}$。这意味着 $\Gamma(1, 1)$ 的累积分布函数为

$$F(x; 1, 1) = 1 - e^{-x}. \tag{27}$$

利用这些事实，我们证明几个后续会用到的引理。首先， $P \sim \mathrm{Dir}(1^N)$ 的最大值的期望为 $O(n)/N$。

引理 3.13。设 $P \sim \mathrm{Dir}(1^N)$。则

$$\mathop{\mathbb{E}}_{P\sim\mathrm{Dir}(1^N)}\left[\max_z P_z\right] \le \frac{2\ln N + 7}{N}. \tag{28}$$

and

$$\mathop{\mathbb{E}}_{P\sim\mathrm{Dir}(1^N)}[H_{\min}(P)] \ge n - \log n - O(1). \tag{29}$$

证明。设 $F(x) = 1 - e^{-x}$ 是 $\Gamma(1, 1)$ 和 $Q_1, \ldots, Q_N \sim \Gamma(1, 1)$ 的累积分布函数。再设 $Q = (Q_1, \ldots, Q_N)$。$\max_z Q_z$ 的累积分布函数为

$$G(x) = \Pr[\forall z, Q_z \le x] = (1 - e^{-x})^N. \tag{30}$$

因此，期望

$$\begin{aligned}
\mathop{\mathbb{E}}_{Q\sim\Gamma(1,1)^N}\left[\max_z Q_z\right] &= \int_0^\infty \mathrm{d}x(1 - (1 - e^{-x})^N) \\
&= \int_0^1 \mathrm{d}y \frac{1 - y^N}{1 - y} \\
&= \int_0^1 \mathrm{d}y(1 + y + y^2 + \ldots y^{N-1}) \\
&= 1 + \frac{1}{2} + \ldots + \frac{1}{N} \\
&\le \ln N + 1.
\end{aligned} \tag{31}$$

如 引理 3.14 的证明 $Q = \sum_z Q_z$ 所示，它是集中的：

$$\Pr_Q[|\bar{Q} - N| \le N/2] \ge 1 - \frac{4}{N}. \tag{32}$$

设 $\Omega := \{Q : Q \ge N/2\}$。由 (32)， $\Pr_{Q\sim\Gamma(1,1)^N}[Q \in \Omega] \ge 1 - 4/N$。这意味着

$$\begin{aligned}
\mathop{\mathbb{E}}_{Q\sim\Gamma(1,1)^N}\left[\frac{\max_z Q_z}{\bar{Q}}\right] &\le \mathop{\mathbb{E}}_{Q}\left[\frac{\max_z Q_z}{\bar{Q}}\middle| Q \in \Omega\right] + \Pr[Q \notin \Omega] \\
&\le \frac{2}{N}\mathop{\mathbb{E}}_{Q}\left[\max_z Q_z \middle| Q \in \Omega\right] + \frac{4}{N} \\
&\le \frac{2}{N}\frac{1}{\Pr[Q \in \Omega]}\mathop{\mathbb{E}}_{Q}\left[\max_z Q_z\right] + \frac{4}{N} \\
&\le \frac{2\ln N + 7}{N}.
\end{aligned} \tag{33}$$

这表明(28) 是正确的。对于(29)，根据詹森不等式，

$$\mathop{\mathbb{E}}_{P\sim\mathrm{Dir}(1^N)}[H_{\min}(P)] \ge -\log \mathop{\mathbb{E}}_{P\sim\mathrm{Dir}(1^N)}\left[\max_z P_z\right] \ge n - \log n - O(1). \tag{34}$$

□

$P \sim$狄利克雷分布 1^N 的最大值集中在 $O(n)/N$ 附近。

引理 3.14。有

$$\Pr_{P\sim \mathrm{Dir}(1^N)}\left[\max_z P_z \le \frac{4\ln N}{N}\right] \ge 1 - \frac{6}{N}. \tag{35}$$

证明。令 $F(x) = (1 - e^{-x})$ 为 $\Gamma(1, 1)$ 的累积分布函数。因此，转而考虑

$$\begin{aligned}\Pr_{Q\sim\Gamma(1,1)^N}\left[\max_z Q_z \le 2\ln N\right] &= \Pr_{Q\sim\Gamma(1,1)^N}[\forall z, Q_z \le 2\ln N] \\ &= F(2(\ln 2)n)^N \\ &= (1 - N^{-2})^N \\ &\ge 1 - 2/N. \end{aligned} \tag{36}$$

此外，$\bar{Q} = \sum_z Q_z$ 是集中的，因为均值 $\mathbb{E}[\bar{Q}] = N$ 和方差 $\sigma^2 = \mathbb{E}[\bar{Q}^2] - \mathbb{E}[\bar{Q}]^2 = N($ $\mathbb{E}[\bar{Q}_0^2] - \mathbb{E}[\bar{Q}_0]^2) = N$。根据切比雪夫不等式，

$$\Pr_Q[|\bar{Q} - N| \le N/2] \ge 1 - \frac{4}{N}. \tag{37}$$

结合 (36)和 (37)，

$$\Pr_Q\left[\frac{\max_z Q_z}{\bar{Q}} \le \frac{4\ln N}{N}\right] \ge 1 - \frac{6}{N}. \tag{38}$$

□

3.4.2 完美装置的性能

在本文中，我们将完美装置定义为：给定 C，输出一个样本 $z \sim p_C$，其中p_C 是由 $p_C(z)$: $= |\langle z|C|0^n\rangle|^2$定义的分布。第一个结果是众所周知的，并且已使用不同的数学工具得到证明：对于 $b \approx 2$，完美装置可以解决 b-XHOG。在此，我们利用狄利克雷分布的性质证明该结果。

引理 3.15. 从 $z \sim P_C$ 对 *Haar* 随机 C 进行采样，可得

$$\mathop{\mathbb{E}}_{C\sim\mathrm{Haar}(N), z\sim P_C}[p_C(z)] = \frac{2}{N+1}. \tag{39}$$

证明. 算法 $\mathcal{A}$ 输出给定的样本 z。对于 $z \in \{0,1\}^n$，令 $P_z = |\langle z|C|0\rangle|^2$ 为 Haar 随机 C 的随机变量，并令 $P = (P_0, \ldots, P_{N-1})$ 为一个取值于概率单纯形上的随机变量向量。由于 $P \sim \mathrm{Dir}(1^N)$、$P|z \sim \mathrm{Dir}(m + 1^N)$，其中 $m = (0, \ldots, 0, m_z = 1, 0, \ldots, 0)$。得分可计算如下：

$$\mathop{\mathbb{E}}_{P\sim\mathrm{Dir}(1^N)}[P_z|m] = \mathop{\mathbb{E}}_{P\sim\mathrm{Dir}(m+1^N)}[P_z] = \frac{m_z + 1}{N+1}. \tag{40}$$

因此，对于满足 $m_z = 1$ 的 z，期望为 $\frac{2}{N+1}$。 □

事实上，$C \sim \mathrm{Haar}(N)$ 的得分集中在 $\frac{2}{N+1}$ 附近。因此，从 $C \sim \mathrm{Haar}(N)$ 中采样时，完美装置以压倒性概率给出的样本，其得分接近 $\frac{2}{N+1}$。

引理 3.16 (碰撞概率的集中性)。 设 $S_C := \mathbb{E}_{z\sim p_C}[p_C(z)]$。则 S_C 按如下意义集中：

$$\Pr_C\left[\left|S_C - \frac{2}{N+1}\right| \le \frac{\varepsilon}{N+1}\right] \ge 1 - O\left(\frac{1}{\varepsilon^2 N}\right). \tag{41}$$

证明。 我们考察随机变量 $S_C = \sum_z p_C(z)^2$ 对于 Haar 随机 C的各阶矩。根据引理 3.15，$\mu = \mathbb{E}_C[S_C] = \frac{2}{N+1}$。

$$\begin{aligned}
\mathop{\mathbb{E}}_C[S_C^2] &= \mathop{\mathbb{E}}_C\left[\sum_{z,z'} p_C(z)^2 p_C(z')^2\right] \\
&= N \mathop{\mathbb{E}}_C[p_C(0)^4] + N(N-1)\mathop{\mathbb{E}}_C[p_C(0)^2 p_C(1)^2] \\
&= \frac{N!4!}{(N+3)!} + N(N-1)\frac{(N-1)!2!2!}{(N+3)!} \\
&= \frac{20+4N}{(N+1)(N+2)(N+3)}
\end{aligned} \tag{42}$$

因此，方差为

$$\begin{aligned}
\mathop{\mathbb{E}}_C[S_C^2] - \mathop{\mathbb{E}}_C[S_C]^2 &= \frac{(4N+20)(N+1) - 4(N+2)(N+3)}{(N+1)^2(N+2)(N+3)} \\
&= \frac{4(N-1)}{(N+1)^2(N+2)(N+3)} = O\left(\frac{1}{N^3}\right).
\end{aligned} \tag{43}$$

根据切比雪夫不等式，

$$\begin{aligned}
\Pr_C\left[\frac{2+\varepsilon}{N+1} \ge S_C \ge \frac{2-\varepsilon}{N+1}\right] &= \Pr_C\left[|S_C - \mu| \le \frac{\varepsilon}{N+1}\right] \\
&\ge 1 - \frac{4(N-1)}{\varepsilon^2(N+2)(N+3)} = 1 - O\left(\frac{1}{\varepsilon^2 N}\right).
\end{aligned} \tag{44}$$

这意味着，对于 C，以概率 $1 - O(\frac{1}{\varepsilon^2 N})$，当 $S_C \ge (2-\varepsilon)/N$ 时。 □

该引理表明， P_C 的碰撞概率高度集中在其均值附近。也就是说，对于几乎所有的 C，如果设备从 P_C 中采样，那么 $p_C(z)$ 的期望非常接近 $\frac{2}{N+1}$。这意味着，从 P_C 采样的设备以常数概率解决 LXEB$_{b,\ k}$ 其中$k = \Omega(n^2)$，且 $b \ge 1.98$。

引理 3.17。 对于整数 k，以概率 $1 - O(1/N)$ 取自 $C \sim \mathrm{Haar}(N)$，采样 z_1、……、$z_k \sim P_C$，

$$\Pr_{z_1,\ldots,z_k\sim P_C}\left[\frac{1}{k}\sum_{i=1}^{k} p_C(z_i) \ge \frac{1.98}{N+1}\right] \ge 1 - 2^{-\Omega(k/n^2)}. \tag{45}$$

证明。根据引理 3.16，结合 $\varepsilon = 0.01$，

$$\Pr_{C\sim\mathrm{Haar}(N)}\left[S_C \ge \frac{1.99}{N+1}\right] \ge 1 - O(1/N). \tag{46}$$

此外，根据引理 3.14，以概率 $1-O(1/N)$，最大值$_z\, p_C(z) \le 4n/N$。对于 C满足$S_C \ge 1.99/(N+1)$ 且 最大值$_z\, p_C(z) \le 4n/N$，根据霍夫丁不等式，

$$\begin{aligned}\Pr_{z_1,\ldots,z_k\sim P_C}\left[\frac{1}{k}\sum_{i=1}^{k} p_C(z_i) \le \frac{1.98}{N+1}\right] &\le \Pr_{z_1,\ldots,z_k\sim P_C}\left[\left|\frac{1}{k}\sum_{i=1}^{k} p_C(z_i) - S_C\right| \ge \frac{0.01}{N+1}\right] \\ &\le 2e^{-0.01k/(16n^2)} = 2e^{-k/(1600n^2)}. \end{aligned} \tag{47}$$

□

因　　此，只需从不同的电路中各取 $O(n^2)$ 个独立样本，共取 $O(\log n)$ 个　　s.

引理 3.18. 对于整数 k、电路 C以及由 $\{0,1\}^n$中的 k个字符串组成的元组 d，令 $V_k(C,\ d)$ 定义为

$$V_k(C,d) := \mathbb{I}\left[\frac{1}{k}\sum_{i=1}^{k} p_C(z_i) \ge \frac{1.98}{N+1}\right] \tag{48}$$

对于 $d=(z_1,\ldots,z_k)$。那么，对于 $k=O(n^2)$ 且 $m=\Omega(\log\ n)$，对完美装置进行 $\mathcal{A}$ mk次采样可得到 $d_1,\ldots,d_m$，满足

$$\Pr_{C_1,\ldots,C_m\sim\mathrm{Haar}(N),\{d_i\sim\mathcal{A}(C_i)\}_{i=1}^m}\left[\sum_{i=1}^{m} V_k(C_i,d_i) \ge 0.99m\right] \ge 1-1/n. \tag{49}$$

证明。根据 引理 3.17，对于 $k=cn^2$ 当常数 c足够大时，

$$\mu := \Pr_{C\sim\mathrm{Haar}(N),d\sim\mathcal{A}(C)}[V(C,d)=1] \ge 0.995. \tag{50}$$

由霍夫丁不等式可得，

$$\begin{aligned}&\Pr_{C_1,\ldots,C_m\sim\mathrm{Haar}(N),\{d_i\sim\mathcal{A}(C_i)\}_{i=1}^m}\left[\sum_{i=1}^{m} V_k(C_i,d_i) \le 0.99m\right] \\ &\quad\le \Pr_{C_1,\ldots,C_m\sim\mathrm{Haar}(N),\{d_i\sim\mathcal{A}(C_i)\}_{i=1}^m}\left[\left|\frac{1}{m}\sum_{i=1}^{m} V_k(C_i,d_i) - \mu\right| \ge 0.005\right] \\ &\quad\le 2^{-2\cdot 0.005^2 m} \\ &\quad\le 1/n \end{aligned} \tag{51}$$

当 c' 足够大时，$m=c'\log n$。□

这意味着，从完美装置中采样 mk 次，即可得到与 $1.94/(N+1)$ 接近的 XHOG 得分近似值。对于任意小的常数 $c>0$，该界可改进为 $2-c$。

推论 3.19. 对于 $k=O(n^2)$ 且 $m=\Omega(\log n)$，从完美装置中采样 $\mathcal{A}$ 次，对从 *Haar* 测度中采样得到的 m 个独立电路进行操作，其概率为 $1-1/n$，

$$\frac{1}{mk}\sum_{i=1}^{m}\sum_{j=1}^{k} p_{C_i}(z_{ij}) \ge \frac{1.94}{N+1}, \tag{52}$$

其中 z_{ij} 表示来自 C_i的第 j个样本。

证明。该推论由引理 3.18 以及以下蕴含关系

$$\frac{1}{m}\sum_{i=1}^{m} V_k(C_i, d_i) \geq 0.98 \implies \frac{1}{mk}\sum_{i=1}^{m}\sum_{j=1}^{k} p_{C_i}(z_{ij}) \geq \frac{1.94}{N+1}, \tag{53}$$

对于 $d_i = (z_{i1}, \ldots, z_{ik})$. □

4 熵累积定理

在本区段中，我们对 Dupuis、Fawzi 和 Renner 提出的熵累积定理（EAT）作了修改 [28]。我们的证明与 [28] 的证明基本相同，仅有以下细微改动：在[28], 中，最小权衡函数 f： $\mathbb{P} \to \mathbb{R}$ 定义在概率分布集合 $\mathbb{P}$上。这里，我们的最小权衡函数 f： $\mathbb{R}^{\geq 0} \to \mathbb{R}$，其中输入对应于设备的得分。为了说明这一修改确实能提供一种有效工具，将多轮熵累积过程的分析简化为冯·诺依曼熵的单轮分析，我们从头开始正式证明该定理。

回顾一下，根据冯·诺依曼熵的定义，链式法则成立：

$$H(A_1A_2|B)_\rho = H(A_1|B)_\rho + H(A_2|A_1B)_\rho \tag{54}$$

对于每个三体态 $\rho_{A_1A_2B}$，这一点都成立。然而，同样的等式对其他 Rényi 熵并不成立。相反，Dupuis、Fawzi 和 Renner [28]证明了以下结论。

定理 4.1 ([28, 定理 3。2])。 令 $\rho_{A_1A_2B}$ 为一个密度算子，且 $\alpha \in (0, \infty)$。该 n

$$H_\alpha(A_1A_2|B)_\rho = H_\alpha(A_1|B)_\rho + H_\alpha(A_2|A_1B)_\nu, \tag{55}$$

其中

$$\nu_{A_1A_2B} = \nu_{A_1B}^{1/2}\rho_{A_2|A_1B}\nu_{A_1B}^{1/2} \qquad with \qquad \nu_{A_1B} = \frac{\left(\rho_{A_1B}^{1/2}\rho_B^{\frac{1-\alpha}{\alpha}}\rho_{A_1B}^{1/2}\right)^\alpha}{\mathrm{tr}\left(\rho_{A_1B}^{1/2}\rho_B^{\frac{1-\alpha}{\alpha}}\rho_{A_1B}^{1/2}\right)^\alpha}. \tag{56}$$

注意， $\nu_{A_1A_2B}$ 是归一化的，而 ν_{A_1B} 是 $\nu_{A_1A_2B}$ 对系统取迹后得到的边缘分布 A_2。尽管存在一个量子态 ν 使得(55) 中的等式成立，但就我们的目的而言，我们只关心某个能够导出不等式的量子态族。具体来说，下面的不等式将很有用。

定理 4.2 ([28, 定理 3。3])。 令 $\rho_{A_1B_1A_2B_2}$ 为一个密度算子，且 $\alpha \in (0, \infty)$ 满足马尔可夫链条件。那么

$$\inf_\nu H_\alpha(A_2|B_2A_1B_1)_\nu \leq H_\alpha(A_1A_2|B_1B_2)_\rho - H_\alpha(A_1|B_1)_\rho \leq \inf_\nu H_\alpha(A_2|B_2A_1B_1)_\nu \tag{57}$$

定理 4.2 可通过证明马尔可夫链条件蕴含 $H_\alpha(A_1|B_1B_2)_\rho = H_\alpha(A_1|B_1)_\rho$，并利用 定理 4.1 得出。我们还可以用量子信道来表示 定理 4.2 。

定理 4.3 ([28, 推论 3.5])。 设 $\rho_{RA_1B_1}$ 是定义在 $R \otimes A_1 \otimes B_1$ 上的密度算子， $\mathcal{M}$ ∈完全正迹保持$(R,\ A_2B_2)$ 且 $\alpha \in (0,\ \infty)$。若 $\mathcal{M}(\rho_{RA_1B_1})$ 满足马尔可夫链条件 $A_1 \leftrightarrow B_1 \leftrightarrow B_2$，则

$$\inf_{\omega} H_\alpha(A_2|B_2A_1B_1)_{\mathcal{M}(\omega)} \leq H_\alpha(A_1A_2|B_1B_2)_{\mathcal{M}(\rho)} - H_\alpha(A_1|B_1)_\rho \leq \sup_{\omega} H_\alpha(A_2|B_2A_1B_1)_{\mathcal{M}(\omega)}, \tag{58}$$

其中，上确界和下确界取遍 $R\otimes A_1 \otimes A_2$ 上的密度算子。此外，如果 $\rho_{RA_1B_1}$ 是纯态，则只需在纯态 $\omega_{RA_1B_1}$ 上进行优化。

定理 4.3 可通过应用 定理 4.2 并给出一个使不等式取等的量子态 ω 来得到。在本例中，马尔可夫链条件显然成立，因为系统 B_i 为空。

˜设 E_{i-1} 是与 $R_{i-1}E$ 同构的系统，并令 $\mathbb{P}$ 表示分布集合。添加一个˜系统 R_{i-1}，是为了将 $R_{i-1}E$ 上的量子态纯化，使得量子态 $^{\omega}{}_{R_{i-1}E\tilde{R}_{i-1}}$ 为纯态，且其边缘分布是输入到 $\mathcal{M}_i$ 的 R_{i-1} 上任意一个量子态。

我们修改最小权衡函数的定义，使其适用于[28], ，具体如下。

定义 4.4。 f 上的实值函数： $\mathbb{R}^{\geq 0} \to \mathbb{R}$ ，称为 $\mathcal{M}_i$ 的最小权衡函数，若其满足

$$f(s) \leq \inf_{\nu \in \Sigma_i(G,s)} H(A_i|E\tilde{E}_{i-1})_\nu \tag{59}$$

其中 $\Sigma_i\ (G,\ s)\ :=\{\rho_{A_iR_iE\tilde{E}_{i-1}} = (\mathcal{M}_i \otimes \mathbb{I}_{E\tilde{R}_{i-1}})\ (^{\omega}{}_{R_{i-1}E\tilde{R}_{i-1}})\ :\ \mathrm{tr}\ (G\rho_{A_i}) = s\}$，即其在 A_i 上的边缘分布得分为 s的量子态集合，该得分使用对角半正定矩阵 G进行评估。

虽然 f 的定义域是非负实数集合，但出于归一化的目的，我们将注意力限制在区间 $[0,2]$ 内的 f的性质上。令 $\|\nabla f\|_\infty$ 为限制在 $[0,2],$和 $g_{\max}$上的 ∇f的无穷范数， $g_{\min}$ 为 f在 $[0,2],$上的最大值和最小值，即:

$$g_{\max} := \max_{s\in[0,2]} f(s), \qquad g_{\min} = \min_{s\in[0,2]} f(s) \tag{60}$$

特别地，通过将 $[0,2]$中的定义域设定为……，可得 $\frac{1}{2}|g_{\max} - g_{\min}| \leq \|\nabla f\|_\infty$，其中 $\|\nabla f\|_\infty$是 f的无穷范数。注意，这一限制不失一般性：给定一个得分位于 $[0,a]$ 内且具有某个对角 G'的博弈，我们可以设定 $G = 2G'/a$。

为了确定下确界，只需考虑纯态 $^{\omega}{}_{R_{i-1}\tilde{R}_{i-1}}$ ，因为根据强˜次可加性，添加一个纯化系统不会增加 $H(A_i|ER_{i-1})$。对于事件 $\Omega \subseteq \mathcal{A}^m$，我们记作

$$\Pr_\rho[\Omega] := \sum_{(a_1,\ldots,a_m)\in\Omega} \mathrm{tr}(\rho_{E,a_1,\ldots,a_m}) \tag{61}$$

对于在 A^m 上为经典的经典-量子态 ρ ，将该量子态投影到由 $|w_1$、…、$w_m\rangle$ 张成的子空间上所得的迹，适用于 $(w_1$、…、$w_m)$ $\in\Omega$。对于在 $A_1^mB_1^m$ 上为经典的任意量子态 $\rho_{A_1^mB_1^mE}$，我们记条件态为

$$\rho_{A^mE|\Omega} := \frac{1}{\Pr_\rho[\Omega]} \sum_{(a_1,\ldots,a_m)\in\Omega} |a_1,\ldots,a_m\rangle\langle a_1,\ldots,a_m| \otimes \rho_{E,a_1,\ldots,a_m}. \tag{62}$$

显然，该量子态已归一化。

以下　下述定理指出，只需对 $H_\alpha^{\uparrow}(Z^m|E)_{\mathcal{M}_m\circ\ldots\circ\mathcal{M}_1(\rho)|\Omega}$ 给出一个下界　　.

命题 4.5 ([28, 引理 B.10]). 对于任意密度算子 ρ和非负算子 σ 任意$\alpha \in (1,2]$, 以及任意 $\varepsilon \in (0,1)$,

$$H_{\min}^{\varepsilon}(Z^m|E)_{\mathcal{M}_m\circ\ldots\circ\mathcal{M}_1(\rho)|\Omega} \geq H_{\alpha}^{\uparrow}(Z^m|E)_{\mathcal{M}_m\circ\ldots\circ\mathcal{M}_1(\rho)|\Omega} - \frac{\log(2/\varepsilon^2)}{\alpha-1}. \tag{63}$$

为计入事件 Ω，我们遵循 [28]中的思路：首先，引入系统D_1、……、 D_m 以及归一化态 $\{\tau(z)\colon z \in \mathcal{Z}\}$，使得

$$H(D_i)_{\tau(z)} = \bar{g} - f(G_z), \tag{64}$$

其中 $G_z\colon = \langle z|G|z\rangle$，以及完全正迹保持映射 $\mathcal{D}_i\colon$ CPTP(Z_i, Z_iD_i)，其中

$$\mathcal{D}_i(|z\rangle\langle z|) := |z\rangle\langle z| \otimes \tau(z)_{D_i}. \tag{65}$$

此外，我们定义 $\mathcal{M}_i\colon = \mathcal{D}_i \circ \mathcal{M}_i$。这使我们能够应用 Metger、Fawzi、Sutter 和 Renner [45] 提出的以下命题。

命题 4.6 ([45, 引理 4.5])。 对于 $\alpha > 1$ 和归一化态 ρ,

$$H_{\alpha}^{\uparrow}(Z^m|E)_{\mathcal{M}_m\circ\ldots\circ\mathcal{M}_1(\rho)|\Omega} \geq H_{\alpha}^{\uparrow}(Z^mD^m|E)_{\mathcal{M}_m\circ\ldots\circ\mathcal{M}_1(\rho)|\Omega} - \max_{z\in\Omega} H_{\alpha}(D^m)_{\bar{\mathcal{M}}_m\circ\ldots\circ\bar{\mathcal{M}}_1(\rho)_z}. \tag{66}$$

令 $g_{\min}$ 和 $g_{\max}$ 分别表示 f值域的最大值和最小值。此外，令$\bar{g}\colon = \frac{1}{2}(g_{\min} + g_{\max})$。如果分布 q由样本 z_1、……、 z_m 诱导，则称其为

$$q(z) = \frac{1}{m}|\{i : z_i = z\}|. \tag{67}$$

对于仿射 f以及由样本 z_1、……、 z_m诱导的分布 q，

$$\left|\bar{g} - f\left(\mathop{\mathbb{E}}_{z\sim q} G_z\right)\right| \leq \frac{1}{2}|g_{\max} - g_{\min}| \leq \|\nabla f\|_{\infty}. \tag{68}$$

接下来，我们分别对(66) 右侧的每一项给出界。

命题 4.7. 对于 $\alpha > 1$ 以及任意 $z = (z_1,\ldots,z_m) \in \mathcal{Z}^m$,

$$H_{\alpha}(D^m)_{\bar{\mathcal{M}}_m\circ\ldots\circ\bar{\mathcal{M}}_1(\rho)_{D,z}} \leq m\|\nabla f\|_{\infty}, \tag{69}$$

证明。 由于每个 $\tau(z_i)_{D_i}$ 都由 z_i 决定，因此边缘态是乘积态，即:

$$\bar{\mathcal{M}}_m \circ \ldots \circ \bar{\mathcal{M}}_1(\rho)_{D_1\ldots D_m} = \tau(z_1)_{D_1} \otimes \ldots \otimes \tau(z_m)_{D_m}. \tag{70}$$

Thus

$$\begin{aligned}
\frac{1}{m}H_{\alpha}(D^m)_{\bar{\mathcal{M}}_m\circ\ldots\circ\bar{\mathcal{M}}_1(\rho)} &= \frac{1}{m}\sum_{i=1}^{m} H_{\alpha}(D_i)_{\tau(z_i)} \\
&\leq \frac{1}{m}\sum_{i=1}^{m} H(D_i)_{\tau(z_i)} \\
&= \frac{1}{m}\sum_{i=1}^{m} \bar{g} - f(G_{z_i}) \\
&= \bar{g} - f\left(\mathop{\mathbb{E}}_{z\sim q} G_z\right) \\
&\leq \|\nabla f\|_{\infty}.
\end{aligned} \tag{71}$$

第一个等式由 (70) 得出。第一个不等式依据 Rényi 熵关于 α 的单调性得出。第二个等式由 (64) 得出。第三个等式成立是因为 f 是仿射函数。最后一个不等式由 (68) 得出。

□

式 (66) 中的第一项可以利用链式法则进一步化简 定理 4.3。注意，马尔可夫链显然成立，因为本文只考虑每个系统 B_i 在定理 4.3 中均为空的情形 $i \in [m]$。

命题 4.8。对于 $\alpha \in (1, \infty)$,

$$\begin{aligned} &H_\alpha^\uparrow(Z^m D^m|E)_{\sigma|\Omega} \\ &\quad \geq \sum_{i=1}^m \inf_{\omega_{i-1} \in \mathrm{S}(R_{i-1}E\tilde{E}_{i-1})} H_\alpha(Z_i D_i|E\tilde{E}_{i-1})_{\bar{\mathcal{M}}_i(\omega_{i-1})} - \frac{\alpha}{\alpha-1}\log\left(\frac{1}{\Pr_\sigma[\Omega]}\right), \end{aligned} \tag{72}$$

˜其中 $\sigma := \mathcal{M}_m \circ \cdots \circ \mathcal{M}_1(\rho)$ 且 E_{i-1} 是与 $R_{i-1}E$ 同构的系统（见 定义 4.4）。

证明。 直接计算可得,

$$\begin{aligned} H_\alpha^\uparrow(Z^m D^m|E)_{\mathcal{M}_m \circ \ldots \circ \mathcal{M}_1(\rho)|\Omega} &\geq H_\alpha(Z^m D^m|E)_{\mathcal{M}_m \circ \ldots \circ \mathcal{M}_1(\rho)|\Omega} \\ &\geq H_\alpha(Z^m D^m|E)_{\mathcal{M}_m \circ \ldots \circ \mathcal{M}_1(\rho)} - \frac{\alpha}{\alpha-1}\log\left(\frac{1}{\Pr_\sigma[\Omega]}\right). \end{aligned} \tag{73}$$

第一个不等式 $H_\alpha^\uparrow(A|B)_\rho \geq H_\alpha(A|B)_\rho$ 对任意有限维希尔伯特空间 A、B以及双部态 ρ均成立。第二个不等式由 [28, 引理 B5]可得。

接下来，我们对第一项应用链式法则 定理 4.3 ，得到

$$H_\alpha(Z^m D^m|E)_{\mathcal{M}_m \circ \ldots \circ \mathcal{M}_1(\rho)} \geq \sum_{i=1}^m \inf_{\omega_{i-1} \in \mathrm{S}(R_{i-1}E\tilde{E}_{i-1})} H_\alpha(Z_i D_i|E\tilde{E}_{i-1})_{\bar{\mathcal{M}}_i(\omega_{i-1})}, \tag{74}$$

˜ ˜其中，我们为每个 i 引入一个净化系统 E_i ，使得 $\omega_{i-1} \in \mathrm{S}(R_{i-1}EE_{i-1})$ 是一个纯态。 □

现在我们对(72)中的每一项进行界定。实际上，这个界取决于 D_i的维数。回想一下，每个 D_i 的引入都是出于分析目的，因此我们可以选择一个足够大的维数$d_{D_i} = d_D := \lceil 2^{\|\nabla f\|_\infty} \rceil$ 使得(64)对每个 $i \in [m]$都成立。这意味着以下命题成立。

命题 4.9。对于 $\alpha \in (1, 1 + \log(2d_Z d_D + 1))$,

$$H_\alpha(Z_i D_i|E\tilde{E}_i)_{\bar{\mathcal{M}}_i(\omega_{i-1})} \geq H(Z_i D_i|E\tilde{E}_i)_{\bar{\mathcal{M}}_i(\omega_{i-1})} - (\alpha-1)(\|\nabla f\|_\infty + \log(2d_Z+1))^2. \tag{75}$$

证明。 根据 [28, 引理 B。9],

$$\begin{aligned} H_\alpha(Z_i D_i|E\tilde{E}_i)_{\bar{\mathcal{M}}_i(\omega_{i-1})} &\geq H(Z_i D_i|E\tilde{E}_i)_{\bar{\mathcal{M}}_i(\omega_{i-1})} - (\alpha-1)\log^2(2d_Z d_D + 1) \\ &\geq H(Z_i D_i|E\tilde{E}_i)_{\bar{\mathcal{M}}_i(\omega_{i-1})} - (\alpha-1)(\|\nabla f\|_\infty + \log(2d_Z+1))^2. \end{aligned} \tag{76}$$

□

结合命题 4.8 和命题 4.9，我们得到以下推论 .

推论 4.10。 对于 $\alpha \in (1,\ 1+2/V)$,

$$
\begin{aligned}
&H_\alpha^{\uparrow}(Z^m D^m|E)_{\mathcal{M}_m\circ\ldots\circ\mathcal{M}_1(\rho)|\Omega} \\
&\quad \geq \sum_{i=1}^{m} \inf_{\omega_{i-1}\in \mathrm{S}(R_{i-1}E\tilde{E}_{i-1})} H(Z_iD_i|E\tilde{E}_i)_{\bar{\mathcal{M}}_i(\omega_{i-1})} - m\left(\frac{\alpha-1}{4}\right)V^2 - \frac{\alpha}{\alpha-1}\log\left(\frac{1}{\Pr_\sigma[\Omega]}\right), \quad (77)
\end{aligned}
$$

其中 $V = 2(\log(2d_Z+1) + \|\nabla f\|_\infty)$。

证明。 直接计算可得,

$$
\begin{aligned}
&H_\alpha^{\uparrow}(Z^m D^m|E)_{\sigma|\Omega} \\
&\quad \geq \sum_{i=1}^{m} \inf_{\omega_{i-1}\in \mathrm{S}(R_{i-1}E\tilde{E}_{i-1})} H_\alpha(Z_iD_i|E\tilde{E}_{i-1})_{\bar{\mathcal{M}}_i(\omega_{i-1})} - \frac{\alpha}{\alpha-1}\log\left(\frac{1}{\Pr_\sigma[\Omega]}\right) \\
&\quad \geq \sum_{i=1}^{m} \inf_{\omega_{i-1}\in \mathrm{S}(R_{i-1}E\tilde{E}_{i-1})} H(Z_iD_i|E\tilde{E}_i)_{\bar{\mathcal{M}}_i(\omega_{i-1})} - m\left(\frac{\alpha-1}{4}\right)V^2 - \frac{\alpha}{\alpha-1}\log\left(\frac{1}{\Pr_\sigma[\Omega]}\right). \quad (78)
\end{aligned}
$$

第一个不等式由 命题 4.8 得出。第二个不等式由 命题4.9 得出。

□

接下来，我们简化 推论 4.10 中的第一项。

命题 4.11。

$$
H(Z_iD_i|E\tilde{E}_i)_{\bar{\mathcal{M}}_i(\omega_{i-1})} \geq \bar{g}. \quad (79)
$$

证明。 直接计算可得,

$$
\begin{aligned}
H(Z_iD_i|E\tilde{E}_{i-1})_{\bar{\mathcal{M}}_i(\omega_{i-1})} &= H(Z_i|E\tilde{E}_{i-1})_{\bar{\mathcal{M}}_i(\omega_{i-1})} + H(D_i|Z_iE\tilde{E}_{i-1})_{\bar{\mathcal{M}}_i(\omega_{i-1})} \\
&= H(Z_i|E\tilde{E}_{i-1})_{\bar{\mathcal{M}}_i(\omega_{i-1})} + H(D_i|Z_i)_{\bar{\mathcal{M}}_i(\omega_{i-1})} \\
&= H(Z_i|E\tilde{E}_{i-1})_{\bar{\mathcal{M}}_i(\omega_{i-1})} + \mathop{\mathbb{E}}_{z\sim r} H(D_i)_{\tau(z)} \\
&= H(Z_i|E\tilde{E}_{i-1})_{\bar{\mathcal{M}}_i(\omega_{i-1})} + \bar{g} - \mathop{\mathbb{E}}_{z\sim r} f(G_z) \\
&= H(Z_i|E\tilde{E}_{i-1})_{\bar{\mathcal{M}}_i(\omega_{i-1})} + \bar{g} - f\left(\mathop{\mathbb{E}}_{z\sim r} G_z\right) \\
&\geq \bar{g}, \quad (80)
\end{aligned}
$$

其中， r 是将 $\mathcal{M}_i(\omega_{i-1})$对 Z_i取边缘分布得到的分布。第一个等式由冯·诺依曼熵链式法则得出。第二个等式成立是因为边缘态 $\mathcal{M}_i(\omega_{i-1})_{D_iZ_i} = \sum_z \tau_i(z)_{D_i} \otimes r(z)|z\rangle\langle z|_{Z_i}$。第三个等式由条件冯·诺依曼熵及 r的定义得出。第四个等式由(64)得出。第五个等式成立是因为 f 是仿射的。不等式成立是因为根据定义， $H(Z_i|EE_{i-1})_{\bar{\mathcal{M}}_i(\omega_{i-1})} \geq f(\mathbb{E}_{z\sim r} G_z)$，其中 $r = \mathcal{M}_i(\omega_{i-1})_{Z_i}$。

□

结合命题 4.6、命题 4.7、推论 4.10和命题 4.11，我们得到以下推论。

推论 4.12。对于 $\alpha \in (1,\ 1+2/V)$,

$$H_\alpha^\uparrow(Z^m|E)_{\mathcal{M}_m\circ\ldots\circ\mathcal{M}_1(\rho)|\Omega} \geq mf(s) - m\left(\frac{\alpha-1}{4}\right)V^2 - \frac{\alpha}{\alpha-1}\log\left(\frac{1}{\Pr_\sigma[\Omega]}\right), \tag{81}$$

其中 $\sigma :=\mathcal{M}_m\circ\cdots\circ\mathcal{M}_1(\rho)$，而 $s :=\frac{1}{m}\sum_{i=1}^m G_{z_i}$ 是通过对每一轮 $i\in[m]$ 的G_{z_i} 取平均值得到的得分。

证明。直接计算可得,

$$\begin{aligned} H_\alpha^\uparrow(Z^m|E)_{\mathcal{M}_m\circ\ldots\circ\mathcal{M}_1(\rho)|\Omega} &\geq H_\alpha^\uparrow(Z^mD^m|E)_{\mathcal{M}_m\circ\ldots\circ\mathcal{M}_1(\rho)|\Omega} - m\|\nabla f\|_\infty \\ &\geq m\bar{g} - m\left(\frac{\alpha-1}{4}\right)V^2 - \frac{\alpha}{\alpha-1}\log\left(\frac{1}{\Pr_\sigma[\Omega]}\right) - m\|\nabla f\|_\infty \\ &\geq mf(s) - m\left(\frac{\alpha-1}{4}\right)V^2 - \frac{\alpha}{\alpha-1}\log\left(\frac{1}{\Pr_\sigma[\Omega]}\right). \end{aligned} \tag{82}$$

第一个不等式由 命题 4.6 和 命题 4.7 得出。第二个不等式由推论 4.10 得出。第三个不等式成立是因为 $f(s)\ \leq \bar{g} - \|\nabla f\|_\infty$。 □

最后，由 命题 4.5 和 推论 4.12，我们得到以下推论 .

推论 4.13。对于 $\alpha \in (1,\ 1+2/V)$,

$$H_{\min}^\varepsilon(Z^m|E)_{\mathcal{M}_m\circ\ldots\circ\mathcal{M}_1(\rho)|\Omega} \geq mf(s) - m\left(\frac{\alpha-1}{4}\right)V^2 - \frac{1}{\alpha-1}\log\left(\frac{2}{\varepsilon^2\Pr_\sigma(\Omega)^2}\right). \tag{83}$$

注意，推论 4.13 对任意 $\alpha \in (1,\ 1+2/V)$ 均成立。因此，我们通过寻找一个合适的 α 来优化这个界。

推论 4.14。对于 $V = 2(\log(2d_Z+1)\ + \|\nabla f\|_\infty)$,

$$H_{\min}^\varepsilon(Z^m|E)_{\mathcal{M}_m\circ\ldots\circ\mathcal{M}_1(\rho)|\Omega} \geq mf(s) - \sqrt{m}V\sqrt{\log\frac{2}{\Pr_\sigma[\Omega]^2\varepsilon^2}} \tag{84}$$

证明。 为了优化参数 α，我们令

$$m\left(\frac{\alpha-1}{4}\right)V^2 = \frac{1}{\alpha-1}\log\left(\frac{2}{\varepsilon^2\Pr_\sigma[\Omega]^2}\right), \tag{85}$$

由此可得

$$\alpha = 1 + \left(\frac{4}{mV^2}\log\left(\frac{2}{\varepsilon^2\Pr_\sigma[\Omega]^2}\right)\right)^{1/2}. \tag{86}$$

这意味着

$$m\left(\frac{\alpha-1}{4}\right)V^2 = \frac{\sqrt{m}V}{2}\sqrt{\log\left(\frac{2}{\varepsilon^2\Pr_\sigma[\Omega]^2}\right)}. \tag{87}$$

□

在抽查协议中，验证者在每一轮以概率 $\gamma \in [0,1]$ 抛掷一枚偏置硬币 T_i ~伯努利分布(γ)。如果 $T_i = 1$，则协议进入测试轮次，此时验证者会统计得分。否则，如果 $T_i = 0$，则协议进入生成轮次，此时验证者不会计算得分。实际上，这相当于将得分设置为零。

为了了解经过我们修改的抽样检查如何运作，我们沿用了 [28]中的思路。具体而言，我们将 G 乘以因子 γ，也就是说，我们考虑新的线性算子 $G' = \gamma G$。此外，我们选择新的最小权衡函数 $f' = \frac{1}{\gamma} f$。采用新的选择 G'和 f'后，上述分析得出了相同的平滑条件最小熵下界。

抽样检查的这一变化似乎确实允许我们选择任意小的 γ。然而，任意小的 γ 应该行不通，因为取 $\gamma \to 0$ 就意味着熵累积协议不需要任何验证。相反，我们希望选择足够大的 γ ，使得良好的设备满足 Ω 的概率渐近地接近一。例如，在基于贝尔不等式违背的熵累积协议中，得分是 $[\omega_c, \omega_q]$ 中的一个值，其中 ω_c 和ω_q 分别是经典设备和量子设备能够达到的最佳得分的常数。根据霍夫丁不等式，对于完美装置，只需取 $\gamma = O((\log m)/m)$，即可使其以 $1 - O(1/m)$的概率成功。

在本文接下来的章节中，我们旨在证明基于 LXEB 的累积协议中条件最小熵的一个下界。在第 3.4.2 节中，我们已经证明，对于 C 的各种取值，碰撞概率的集中性 $O(\log\ n)$ 个电路足以让完美装置以概率 $1 - O(1/n)$ 成功，推理过程相同。

5 无侧信息的一般设备

在本节中，我们考虑以下情形：设备与对手不共享纠缠，但可以学习电路。在这种设定下，我们给出一个协议：在通过 LXEB$_{1+\delta、k}$这一事件 Ω 的条件下，当$\delta =$足够大时，熵会累积，且$\delta =$为 Ω(1)。更正式地说，我们旨在证明 $H^{\varepsilon}_{\min}(Z_1 \dots Z_m | C_1 \dots C_m)_{\rho|\Omega}$ 具有 Ω(nm) 的下界。

在第5.1节中，我们定义了一个称为长列表量子霸权验证（LLQSV）问题的问题，即判定字符串 s 是从随机电路 C 中采样得到，还是根据均匀分布独立采样得到。我们的困难性假设称为长列表困难性假设（LLHA），其指出，对于能够访问量子建议态的 QCAM 协议而言，LLQSV 是困难的。在第5.2节中，我们证明，若 LLHA 成立，则对于 C 的选择，任何设备都必须以 Ω(1) 的概率生成 Ω(n) 的最小熵。由于条件冯·诺依曼熵是通过取期望计算的，这意味着每个通过 LXEB$_{1+\delta,\ k}$ 的设备，都必须在输入电路上建立 Ω(n) 的条件冯诺依曼熵下界。

我们在图 1中陈述了我们的协议。具体而言，验证者随机选择Ω(log n) 个测试轮次，方法是以概率 $\gamma = \Omega((\log n)/m)$选择每一轮进行验证；在这些轮次中，验证者会判定设备是否通过LXEB$_{1+\delta,\ k}$。根据第5.1节中建立的条件冯诺依曼熵下界，以及第4节中给出的熵累积定理，我们在第5.3节中建立了平滑条件最小熵的Ω(nm)下界。

由于 LLHA 是一个看似很强的假设，我们必须为其提供依据。在第5.4节中，我们证明，相对于随机预言机，LLQSV 对具有量子辅助信息的 QCAM 协议而言是困难的。这意味着存在一种电路分布，使得 LXEB$_{1+\delta,\ k}$ 如果设备可以访问随机

电路的预
言机。

5.1 长列表量子霸权验证问题

本节将正式定义问题 LLQSV，如下所示。

问题 4 (长列表量子霸权验证（LLQSV）**).** 给定一个包含 $M = O(N^3)$个电路-字符串元组 $\{(C_i, s_i) : i \in [M]\}$ 的列表，区分以下情况：

- **是例**：对于每个 $i \in [M]$，$C_i \sim \mathcal{D}$ 和 s_i 均从 C_i 中抽样，即 $s_i \sim p_{C_i}$。
- **否例**：对于每个 $i \in [M]$，$C_i \sim \mathcal{D}$ 和 s_i 均匀分布抽样（因此独立于 C_i）。

我们将证明，如果

$$\mathrm{LLQSV}(\mathcal{D}) \notin \mathsf{QCAMTIME}(2^B n^{O(1)})/\mathsf{q}(2^B n^{O(1)}), \tag{88}$$

那么，任何在 $n^{O(1)}$ 时间内运行并以概率 q解决 LXEB$_{b,\ k}$ 的量子算法，都必须以至少 $\frac{bq-1}{b-1}$的概率（对 C的选择而言）输出最小熵至少为 B的 s_1、.....、s_k。因此，参数 B 决定了最小熵下界。我们在所谓的长列表困难性假设（LLHA）下证明这一点。

假设 5.1 ($\mathrm{LLHA}_B(\mathcal{D})$)。 不存在这样的QCAM 协议：量子 *Arthur* 在获得长度为 $2^B n^{O(1)}$的量子辅助信息后，能在 $2^B n^{O(1)}$ 时间内解决 $\mathrm{LLQSV}(\mathcal{D}, V)$。换言之，$\mathrm{LLQSV}(\mathcal{D}) \notin \mathsf{QCAMTIME}(2^B n^{O(1)})/\mathsf{q}(2^B n^{O(1)})$。

5.2 LLHA 蕴含认证随机性

本节中，我们证明 $\mathrm{LLHA}_B(\mathcal{D})$ 蕴含：任何通过 LXEB$_{b,k}$ 的设备，在给定 $C \sim \mathcal{D}$的情况下，都必须输出最小熵为 $\Omega(n)$ 的样本。我们的归约依赖于用于近似计数的 Goldwasser-Sipser 协议 [32], ，其说明如下。回顾一下，实例由 M 个元组 (C_i, s_i) 构成，其中 $i \in [M]$，而 $C_i \sim \mathcal{D}$和 s_i则是从 p_{C_i}或均匀分布 $\mathcal{U}$中采样得到的。设 V 是一个运行时间为 $2^B n^{O(1)}$ 的量子-经典 Merlin-Arthur 协议，使得对于是实例，它至少接受 κ 个元组；对于否实例，它至多接受 $(1 - \Omega(\varepsilon))\kappa$ 个元组，且两种情况下的概率均为 $1 - 2^{-\Omega(n)}$。那么这立即导出一个量子-经典 Arthur–Merlin 协议：

输入：Arthur 和 Merlin 都接收一个实例 $(C_1, s_1) \ldots, (C_M, s_M)$。

1. Arthur 对 R（事后确定的）上的 $[M] \to [R]$ 采样一个随机哈希函数 h r.
2. Merlin 发送 $i \in [M]$ 和一个证明 π。
3. 如果 V接受带有见证 π 的 (C_i, s_i)，且 $h(i) = y$，Arthur 就接受。

该协议的间隙为 $\Omega(\varepsilon^2/\alpha)$，证明如下。

引理 5.2. 对于实数 $\alpha > 1$ 和整数 κ，存在一个 *Arthur-Merlin* 协议，该协议以集合 S 的描述为输入，使用值域大小为 $R = 2\alpha\kappa/\varepsilon$ 的哈希函数，以至少 $\frac{\varepsilon^2}{4\alpha}$ 的间隔判定 $\alpha\kappa \geq |S| \geq \kappa$ 还是 $|S| \leq (1 - \varepsilon)\kappa$。

证明。只需得到该概率的紧上界和下界

$$\Pr_{h,y}[\exists x \in S, h(x) = y] \tag{89}$$

对于一个值域大小为 R 的随机哈希函数 h。根据并集界，上界为 $\sum_{x\in S} \Pr_{h,\ y}[h(x) = y] = \frac{|S|}{R}$。对于下界，根据容斥原理[7]

$$\begin{aligned}
\Pr_{h,y}[\exists x \in S, h(x) = y] &\geq \frac{|S|}{R} - \sum_{x\leq x', x, x' \in S} \Pr_{h,y}[h(x) = h(x') = y] \\
&= \frac{|S|}{R} - \binom{|S|}{2}\frac{1}{R^2} \\
&= \frac{|S|}{R}\left(1 - \frac{|S|-1}{2R}\right) > \frac{|S|}{R}\left(1 - \frac{|S|}{R}\right)
\end{aligned} \tag{90}$$

在是情况下，$\alpha\kappa \geq |S| \geq \kappa$ 和 $R = 2\alpha\kappa/\varepsilon$，并且

$$\begin{aligned}
\Pr_{h,y}[\exists x \in S, h(x) = y] &\geq \frac{|S|}{R}\left(1 - \frac{|S|}{R}\right) \\
&\geq \frac{\kappa}{R}\left(1 - \frac{\alpha\kappa}{R}\right) \\
&\geq \frac{\kappa}{R}\left(1 - \frac{\varepsilon}{2}\right),
\end{aligned} \tag{91}$$

而在否情况下，$|S| \leq (1-\varepsilon)\kappa$，并且

$$\Pr_{h,y}[\exists x \in S, h(x) = y] \leq \frac{|S|}{R} \leq \frac{\kappa}{R}(1-\varepsilon). \tag{92}$$

间隙至少为 $\frac{\kappa\varepsilon}{2R} = \frac{\varepsilon^2}{4\alpha}$。 □

假设存在一个量子设备 $\mathcal{A}$，它以概率 q（对 C 的选择而言）求解 $\mathrm{LXEB}_{b,\ k}$，并以概率 p 输出 k 个元组 $(s_1, \ldots, s_k)$，其最小熵至多为 $B/2$，且 p 和 q 满足

$$p > \frac{b}{b-1}(1-q) + \varepsilon. \tag{93}$$

为了破解 $\mathrm{LLHA}_B(\mathcal{D})$，我们考虑以下关于 $\tau \in [0,1]$ 的随机变量 $Y_\tau(C, s)$:

$$Y_\tau(C,s) := \begin{cases} 1 & \text{if } \exists d = (z_1, \ldots, z_k),\ \Pr[\mathcal{A}(C) = d] \geq \frac{\tau}{2^{B/2}} \text{ and } s \in \mathcal{A}(C) \\ 0 & \text{otherwise.} \end{cases} \tag{94}$$

这里 $s \in \mathcal{A}(C)$ 表示样本 $s \in \{z_1, \ldots, z_k\}$ 针对样本 $(z_1, \ldots, z_k) \sim \mathcal{A}(C)$。定义

$$\mu_1(\tau) = \mathop{\mathbb{E}}_{C\sim\mathcal{D}, s\sim p_C}[Y_\tau(C,s)], \qquad \mu_0(\tau) = \mathop{\mathbb{E}}_{C\sim\mathcal{D}, s\sim\mathcal{U}}[Y_\tau(C,s)], \tag{95}$$

其中 $\mathcal{U}$ 是 $\{0,1\}^n$上的均匀分布。

令 $p(\tau)$ 表示　对于 $C \sim \mathcal{D}$，$\mathcal{A}(C)$ 的最大概率至少为 $\tau/2^{B/2}$ 的概率，即 .,

$$p(\tau) := \Pr_{C\sim\mathcal{D}}\left[\max_d \Pr[\mathcal{A}(C) = d] \geq \frac{\tau}{2^{B/2}}\right]. \tag{96}$$

以下引理表明，比值 $\mu_1(\tau)/\mu_0(\tau)$ 的界为 $b \cdot (p(\tau) + q - 1)/p(\tau)$。

[7] The principle states that $\Pr[\bigvee_i E_i] \geq \sum_i \Pr[E_i] - \sum_{i<j} \Pr[E_i \wedge E_j]$.

引理 5.3。对于 $\tau \in [0,1]$，令 Y_τ 如 *(94)* 中所定义，$\mu_1(\tau)$ $\mu_0(\tau)$ 如 *(95)* 中所定义，以及 $p(\tau)$ 如 *(96)* 中所定义。则

$$\frac{\mu_1(\tau)}{\mu_0(\tau)} \geq b \cdot \frac{p(\tau)+q-1}{p(\tau)}. \tag{97}$$

证明。注意，在每种情况下，我们都在界定

$$\mathop{\mathbb{E}}_{C\sim\mathcal{D},s}[Y_\tau(C,s)] = \Pr_{C\sim\mathcal{D},(z_1,\ldots,z_k)\sim\mathcal{A}(C),s}\left[\exists d, \Pr[\mathcal{A}(C)=d] \geq \frac{\tau}{2^{B/2}} \wedge s \in \{z_1,\ldots,z_k\}\right], \tag{98}$$

其中，在是情况下为 $s \sim p_C$，或在否情况下为 $s \sim \mathcal{U}$。定义

$$G_\tau(C) := \mathbb{I}\left[\max_d \Pr[\mathcal{A}(C)=d] \geq \frac{\tau}{2^{B/2}}\right]. \tag{99}$$

根据 (96)，$p(\tau) = \mathbb{E}_{C\sim\mathcal{D}}[G_\tau(C)]$。

- 对于是情况，

$$\begin{aligned}\mu_1(\tau) &= \mathop{\mathbb{E}}_{C\sim\mathcal{D},s\sim p_C}[Y_\tau(C,s)] \\ &= \Pr_{C\sim\mathcal{D},O\sim\mathcal{A}(C),s\sim p_C}[G_\tau(C) \wedge s \in O] \\ &\geq \Pr_{C\sim\mathcal{D},O\sim\mathcal{A}(C),s\sim p_C}[G_\tau(C) \wedge s \in O \wedge V(C,O)],\end{aligned} \tag{100}$$

其中，如果 $\mathrm{LXEB}_{b,\ k}$ 接受 $O=(z_1,\ldots,z_k)$，即，$V(C,O)=1$

$$\sum_{i=1}^{k} p_C(z_i) \geq \frac{bk}{N} \tag{101}$$

否则为 0。根据并集界，

$$\begin{aligned}\Pr_{C\sim\mathcal{D},O\sim\mathcal{A}(C),s\sim p_C}[G_\tau(C) \wedge V(C,O)=1] &\geq \Pr_{C\sim\mathcal{D}}[G_\tau(C)] + \Pr_{C\sim\mathcal{D},O\sim\mathcal{A}(C)}[V(C,O)] - 1 \\ &= p(\tau)+q-1.\end{aligned} \tag{102}$$

此外，条件概率

$$\Pr_{C\sim\mathcal{D},O\sim\mathcal{A}(C),s\sim p_C}[s \in O | G_\tau(C) \wedge V(C,O)] \geq \frac{bk}{N} \tag{103}$$

因为若 $V(C,\ O)=1$，则 $\Pr_{s\sim p_C}[s \in O] = \sum_{z\in O} p_C(z) \geq bk/N$ 由 (101)。结合 (102)和 (103)，

$$\mu_1(\tau) = \frac{bk}{N}(p(\tau)+q-1). \tag{104}$$

- 对于否情况，由于 s 是独立抽取的，

$$\begin{aligned}\mu_0(\tau) &= \Pr_{C\sim\mathcal{D},O\sim\mathcal{A}(C),s\sim\mathcal{U}}[G_\tau(C) \wedge s \in O] \\ &= \frac{k}{N}\Pr_{C\sim\mathcal{D}}[G_\tau(C)] = \frac{k}{N}\cdot p(\tau).\end{aligned} \tag{105}$$

根据 (104) 和 (105)，我们得出证明。 □

此外，我们证明下界是单调非增的

引理 5.　4. 比值 $(p(\tau)+q-1)/p(\tau)$ 对于 $\tau\in[0,1]$ 单调非增。

证明。 对于 $1\geq\alpha\geq\beta\geq 0$, $p(\alpha)\leq p(\beta)$, 且

$$\frac{p(\beta)+q-1}{p(\alpha)+q-1}\geq\frac{p(\beta)}{p(\alpha)} \tag{106}$$

这意味着 $p_{(\tau)p}{}^{+q-1}{}_{\tau}{}^{()}$ 对于 $\tau\in[0,1]$ 单调非增。 □

引理 5.3 和 引理 5.4推出

$$\frac{\mu_1(\tau)}{\mu_0(\tau)}\geq\frac{\mu_1(1)}{\mu_0(1)}\geq b\cdot\frac{p+q-1}{p}\geq 1+\varepsilon. \tag{107}$$

虽然这看起来为应用 Goldwasser-Sipser 协议提供了一个充分条件，但有一点需要注意：我们不知道如何在时间 $2^B n^{O(1)}$ 内验证 Y_τ 是否接受 (C,s)（尤其是 Y_1）。原因是，即使给定见证 d, 也无法高效验证 $\mathcal{A}(C)$ 以大于 $\tau/2^B$ 的概率输出字符串 d 这一条件。下一步将证明，对于足够大的 T，存在 $j\in[T]$，使得对于 $\tau=1/2+j/T$, $\mu_1(\tau)\geq(1+\varepsilon/2)\mu_0(\tau-1/T)$。

引理 5.5。 令 μ_1 和 μ_0 按 *(95)*中的定义。假设 *(93)* 成立。那么对于 $T\geq\frac{8}{\varepsilon}\log(\frac{N}{\varepsilon})$，存在 $j\in[T]$ 使得

$$\mu_1(1/2+j/T)\geq(1+\varepsilon/2)\mu_0(1/2+(j-1)/T). \tag{108}$$

证明。 我们通过逆否命题证明该引理。假设对于每个 $j\in[T]$,

$$\mu_1(1/2+j/T)<(1+\varepsilon/2)\mu_0(1/2+(j-1)/T). \tag{109}$$

然后将这个比值展开为一个望远镜乘积,

$$\begin{aligned}\frac{\mu_1(1/2)}{\mu_1(1)}&=\prod_{j=1}^{T}\frac{\mu_1(1/2+j/T)}{\mu_1(1/2+(j+1)/T)}\\&\geq(1+\varepsilon/2)^{-T}\prod_{j=1}^{T}\frac{\mu_1(1/2+j/T)}{\mu_0(1/2+j/T)}\\&\geq\left(\frac{1+\varepsilon}{1+\varepsilon/2}\right)^{T}\\&\geq(1+\varepsilon/4)^{T}.\end{aligned} \tag{110}$$

第一个不等式由 (109) 得出。第二个不等式由 (107) 得出。第三个不等式由以下不等式得出: $1+\varepsilon-(1+\varepsilon/2)(1+\varepsilon/4)=\varepsilon/4\cdot(1-\varepsilon/2)\geq 0$，对于 $\varepsilon\leq 2$。取 $T\geq\frac{8}{\varepsilon}\log(n/\varepsilon)$,

$$\begin{aligned}\mu_1(1/2)&>(1+\varepsilon/4)^{T}\cdot\mu_1(1)\\&\geq\frac{k}{N}\cdot\varepsilon(1+\varepsilon/4)^{T}\\&\geq\frac{k}{N}\cdot\varepsilon e^{\varepsilon T/8}\\&\geq k.\end{aligned} \tag{111}$$

这与 $\mu_1(1/2)\leq 1$ 这一事实相矛盾。 □

有了这个间隙，我们可以考虑以下 Merlin-Arthur 协议，该协议可在 $2^B \cdot T^2 \cdot n^{O(1)}$ 时间内验证 $s \sim p_C$:

Arthur 和 Merlin 都可以访问电路 C 以及字符串 $s \in \{0,1\}^n$。

1. Merlin 发送 $d = (z_1, \ldots, z_k)$。

2. Arthur 获取 $K+1$ 个样本 d_1、...、d_K、$O \sim \mathcal{A}(C)$，其中整数 K 稍后确定。Arthur 接受当且仅当

$$\frac{1}{K}|\{\ell : d_\ell = d\}| \geq \left(\tau - \frac{1}{2T}\right)2^{-B/2}, \tag{112}$$

且 $s \in O$，否则拒绝。

该量子-经典 Merlin-Arthur 协议解决了这样的问题：(C, s) 要么被 Y_τ接受，要么被 $Y_{\tau-1/T}$拒绝。

引理 5.6。对于 $\tau \in [1/2, 1]$、$\eta = O(1/N^2)$ 和 $K \geq 4T^2 2^B n$，上述过程满足以下条件：

1. 如果 Y_τ 接受（C， s），那么 *Arthur* 以概率 $1-\eta$ 接受，并且

2. 如果 $Y_{\tau-1/T}$ 拒绝（C， s），那么 *Arthur* 以概率 $1-\eta$ 拒绝。

证明。如果 Y_τ接受（C， s），那么存在 $d = (z_1, \ldots, z_k)$ 使得 $\Pr[\mathcal{A}(C) = d] \geq \tau/2^B$，并且 $s \in \{z_1, \ldots, z_k\}$。根据霍夫丁不等式，式 $\tilde{\nu}$ 在 （112）中出现的比例$\tau - \frac{1}{2T}$）$2^{-B/2}$不超过以下概率

$$\Pr\left[|\tilde{\nu} - \Pr[\mathcal{A}(C) = d]| > \frac{1}{2T}2^{-B/2}\right] \leq 2e^{-2\frac{K}{4T^2 2^B}} \leq 2e^{-2n}. \tag{113}$$

如果 $Y_{\tau-1/T}$ 拒绝（C， s），那么对于每个 d 满足 s 包含于 d中的 $\Pr[\mathcal{A}(C) = d] <$（$\tau - 1/T$）$/2^{B/2}$。同样根据霍夫丁不等式，式 （112）出现的概率至多为 $2e^{-2n}$。 □

对于 $M \geq N^3$，量子-经典 Merlin-Arthur 协议在是实例中接受的元组数量多于在否实例中接受的元组数量，且该结论以压倒性概率成立。

引理 5.7。对于 $M \geq N^3$ 和 $\eta' = 2^{-\Omega(N)}$，存在一个整数 $\kappa \in [M]$，使得以至少 $1-\eta'$ 的概率，*Arthur* 在是实例中接受至少 κ 个元组，并且在否实例中接受至多$\kappa' = (1 - \varepsilon/5 + O(\varepsilon^2))\kappa$ 个元组。

证明。回忆一下，$\mu_1(\tau) = \mathbb{E}_{C\sim\mathcal{D}, s\sim p_C}[Y_\tau(C, s)]$。由于在是实例和否实例中，每个元组均被独立地采样，根据引理 5.6，Authur 接受每个样本的概率至多为 $\mu_0(\tau) + \eta$。因此，根据霍夫丁不等式，对于 $\kappa' = (\mu_0(\tau) + \eta)(1 + \varepsilon/8)M$，

$$\begin{aligned}\Pr_{C_1,\ldots,C_M\sim\mathcal{D}, s_1,\ldots,s_M\sim\mathcal{U}}[\text{Arthur accepts more than } \kappa' \text{ tuples}] &\leq 2e^{-M\varepsilon^2(\mu_0(\tau)+\eta)^2/32} \\ &= 2e^{-\Omega(M\varepsilon^2 k^2 p^2/N^2)} \\ &\leq 2e^{-\Omega(M\varepsilon^4 k^2/N^2)}, \end{aligned} \tag{114}$$

因为根据 (93)，$\mu_0(\tau) = p(\tau)k/N \geq pk/N \geq \varepsilon k/N$。取 $M \geq N^3$，上界为 $2e^{-\Omega(N)}$.

类似地，对于 $\kappa = (\mu_1(\tau) - \eta)(1-\varepsilon/8)M$，

$$\Pr_{C_1,\ldots,C_M\sim\mathcal{D}, s_i\sim p_{C_i}}[\text{Arthur accepts fewer than } \kappa \text{ tuples}] \le 2e^{-M\varepsilon^2(\mu_1(\tau)-\eta)^2/32} \le 2e^{-\Omega(M\varepsilon^2 p^2 k^2/N^2)}, \tag{115}$$

由于 $\eta = O(1/N^2)$ 且 $\mu_1(\tau) - \eta = \Omega(\mu_1(\tau)) = \Omega(\mu_0(\tau)) = \Omega(pk/N)$。

接下来需要给出该比值的上界：由于 $\eta = o(\varepsilon)$，

$$\begin{aligned}
\frac{\kappa'}{\kappa} &\le \frac{\mu_0(\tau)+\eta}{\mu_1(\tau)-\eta}\frac{1+\varepsilon/8}{1-\varepsilon/8} \\
&\le \frac{\mu_0(\tau)+\eta}{\mu_1(\tau)-\eta}\frac{1}{1-\varepsilon/4} \\
&\le \frac{1}{1+\varepsilon/4-O(\eta)} \\
&\le \frac{1}{1+\varepsilon/5} \\
&\le 1-\varepsilon/5+O(\varepsilon^2).
\end{aligned} \tag{116}$$

□

我们已经证明了本区段中证明主定理所需的全部陈述。现在我们描述量子-经典 Arthur–Merlin 协议。

Merlin 和 Arthur 都可以访问 $(C_1, s_1)\ldots,(C_M, s_M)$，并获得包含整数 T、$j \in [T]$ 和 R 的辅助字符串。

1. Arthur 选择一个随机哈希函数 $h: [M] \to [R]$ 和 y 均匀分布于 $[R]$。
2. Merlin 发送 i 和 $d = (z_1, \ldots, z_k)$。
3. 对于 $K \ge 4T^2 2^B n$，Arthur 取 $K+1$ 个样本 $d_1, \ldots, d_K, O \sim \mathcal{A}(C_i)$。若
   (a) $\frac{1}{K}|\{\ell: d_\ell = d\}| \ge (\tau - \frac{1}{2T})2^{-B/2}$，其中 $\tau = 1/2 + j/T$；
   (b) $s_i \in O$；以及 (c) $h(i) = y$，则接受。

我们在本节中证明主要定理。

定理 5.8. 如果存在一个设备 $\mathcal{A}$，它以量子多项式时间运行并满足 *(93)*，那么就存在一个量子-经典 *Arthur–Merlin* 协议，其在输入一个 $O(n)$ 位辅助字符串时，可以解决 $\mathrm{LLQSV}_B(\mathcal{D})$。换言之，$\mathrm{LLQSV}_B(\mathcal{D}) \in \mathsf{QCAMTIME}(2^B n^{O(1)})/O(n)$。

证明。我们证明上述协议以常数间隔求解 $\mathrm{LLQSV}_B(\mathcal{D})$。根据引理 5.7，$\kappa' \le (1-\varepsilon/6)\kappa$ 的概率为 $1-2^{-\Omega(N)}$。再由引理 5.2，对于 $R = 12\alpha\kappa/\varepsilon$，由于 $\alpha = 1+O(\varepsilon)$，间隔为 $\Omega(\varepsilon)$。因此，对上述协议进行 $(1/\varepsilon)^{O(1)}$ 重并行重复，即可得到常数间隔。对于辅助字符串的长度，由于 $1/\varepsilon = n^{O(1)}$，$T = n^{O(1)}$ 且 $R \le M$，只需选择 $M = N^3$，总长度为 $O(n)$。

□

作为推论，如果 $\mathrm{LLHA}_B(\mathcal{D})$ 为真，那么

$$p \leq \frac{b}{b-1}(1-q) + n^{-\omega(1)}. \tag{117}$$

推论 5.9。 对于整数 n，假设分布 $\mathcal{D}$ 上的$\mathrm{LLHA}_B(\mathcal{D})$ 成立，该分布作用于具有 n 个量子比特的电路。则对于每个通过$\mathrm{LXEB}_{b,k}$ 的设备 $\mathcal{A}$，在 $C \sim \mathcal{D}$ 的选择下以概率 q，

$$\Pr_{C\sim\mathcal{D}}[H_{\min}(\mathcal{A}(C)) \geq B/2] \geq \frac{bq-1}{b-1} - n^{-\omega(1)}. \tag{118}$$

由于最小熵是 Rényi 熵这一族中最小的量，因此我们建立了冯·诺依曼熵的下界。

定理 5.10。 对于整数 n，假设分布 $\mathcal{D}$ 上的$\mathrm{LLHA}_B(\mathcal{D})$ 成立，该分布作用于具有 n 个量子比特的电路。则对于任何设备，若其输入为电路 C，输出为 $\{0,1\}^{nk}$上的经典态 ψ，并以概率 q求解$\mathrm{LXEB}_{b,k}$，则有

$$H(Z|C)_\psi \geq \frac{B}{2}\left(\frac{bq-1}{b-1} - n^{-\omega(1)}\right). \tag{119}$$

证明。 根据推论 5.9，由于最小熵是 Rényi 熵这一族中最小的量，

$$\Pr_{C\sim\mathcal{D}}\left[H(Z)_{\psi^C} \geq B/2\right] \geq \frac{bq-1}{b-1} - n^{-\omega(1)}$$

其中 ψ^C 是设备在给定 C 条件下输出的分布。由于对每个 C，冯·诺依曼熵均非负，根据条件冯·诺依曼熵的定义，我们得证。

□

5.3 熵累积

为了应用我们在第4节中证明的熵累积定理（EAT），我们必须给出一个最小权衡函数 f，使得对于输出经典态 ψ 且以$\mathrm{LXEB}_{b\text{成功求解}k}$ 的设备，成功概率为 q，$H(Z|C)_\psi \geq f(q)$。根据定理 5.10，仿射函数可定义为

$$f(q) := \frac{bq-1}{b-1}\frac{B}{2} - c, \tag{120}$$

对于与 q 无关的 $c = n^{-\omega(1)}$。

对于抽查，根据引理 3.18，我们将电路$\Omega(\log n)$ 次，以便完美装置能够以压倒性概率通过验证。结合这些参数，我们可以在图 1中给出我们的协议。

我们证明熵会累积。在下述定理中，令 $D = D_1 \ldots D_m$ 表示从设备接收到的响应，令 $C = C_1 \ldots C_m$ 表示发送给设备的电路，并令$T = T_1 \ldots T_m$ 表示指示是否执行测试轮次的标志（见图 1）。

定理 5.11。 假设 $\mathrm{LLHA}_B(\mathcal{D})$ 对分布 $\mathcal{D}$成立。在事件 Ω（即验证者未在 图 1所示协议中中止）的条件下，

$$H^\varepsilon_{\min}(D|CT)_{\rho|\Omega} \geq n\left((0.99 - 0.01/\delta)\beta m - O\left(\sqrt{m}\right)\cdot\sqrt{\log\frac{2}{p^2\varepsilon^2}}\right), \tag{123}$$

其中，$\beta = \frac{B}{2n}$ ρ 是输出态，p 是不中止概率。此外，存在一种设备，对于 $k = O(n^2)$，能够以概率 $1 - o(1)$求解 $\mathrm{LXEB}_{2,k}$。

输入：安全参数 n、 n个量子比特上电路的分布 $\mathcal{D}$ 、阈值常数$b \in [1,2]$、每次迭代的样本数 $k = O$（n^2）、轮数 m，以及电路更新的比例$\gamma = O$（(log n)$/m$）。

该协议：

1. 对于 $i = 1, \ldots, m$，执行以下步骤：

   (a) 验证者以伯努利分布(γ)进行采样，得到 $T_i \sim$ 。如果 $T_{i-1} = 1$ （当 $i > 1$时）或 $i = 1$，设备就采样 $C_i \sim \mathcal{D}$。否则，设备设置 $C_i = C_{i-1}$。验证者将 C_i 发送给设备（并对 T_i 保密）。

   (b) 设备返回 k 个样本 $d_i =$ （$z_1, \ldots, z_k$）。(c) 如果 $T_i = 1$，验证者设置

$$W_i = \mathbb{I}\left[\frac{1}{k}\sum_{i=1}^{k} p_C(z_i) \geq \frac{b}{N} \wedge E_i\right]. \tag{121}$$

   其中，如果存在不同的 ℓ、$\ell' \in \{j$ ，使得 $C_j = C_i\}$ 成立，则 $E_i = 0$ ；此时样本 $d_\ell = (z_{\ell 1}, \ldots, z_{\ell k})$ 与 $d_{\ell'} = (z_{\ell' 1}, \ldots, z_{\ell' k})$ 并非全部互不相同。（此项检查用于防止设备在任意两轮中使用相同的挑战电路重复响应。）如果$T_i = 0$，验证者设置 $W_i = \perp$。

2. 令 $t = |\{i : T_i = 1\}|$ 表示测试轮次的数量。验证者计算

$$W = \sum_{i:T_i=1} W_i. \tag{122}$$

若 $W \geq 0.99t$，则验证者接受，并将 (d_1,... , d_m) 输出给量子安全随机性提取器。

图 1：基于 LLHA 的熵累积协议。

证明。令 f 如 (120) 中所定义。为应用 推论 4.14，令 $d_Z = N$ 且 $\|\nabla f\|_\infty = \frac{b}{b-1}\frac{B}{2}$，因此 $V \leq (n+1) + \frac{b}{b-1}\frac{B}{2}$。对于 $b = 1+\delta$ 和 $q \geq 0.99$,

$$\frac{bq}{b-1} \geq \frac{(1+\delta)0.99 - 1}{\delta} \geq 0.99 - 0.01/\delta. \tag{124}$$

这意味着存在一个下界

$$\begin{aligned}
&(0.99 - 0.01/\delta)Bm/2 - \sqrt{m}((n+1) + (1/\delta+1)B/2)\sqrt{\frac{2}{p^2\varepsilon^2}} \\
&= n\left((0.99 - 0.01/\delta)\beta m - \sqrt{m}\cdot(1 + 1/n + (1/\delta+1)\beta)\sqrt{\frac{2}{p^2\varepsilon^2}}\right) \\
&\geq n\left((0.99 - 0.01/\delta)\beta m - O(\sqrt{m})\cdot\sqrt{\frac{2}{p^2\varepsilon^2}}\right),
\end{aligned} \tag{125}$$

其中 $\beta = \frac{B}{2n}$。 □

5.4 相对于随机预言机的 LLHA

现在，我们转而证明假设 5.1 相对于随机预言机成立。给定对随机函数 f 的访问：$\{0,1\}^n \to \{+1,-1\}$，存在一种简单的算法，可从傅里叶谱中采样：

$$|0^n\rangle \overset{H^{\otimes n}}{\longmapsto} \sum_{x\in\{0,1\}^n} |x\rangle \overset{O_f}{\longmapsto} \sum_{x\in\{0,1\}^n} f(x)|x\rangle \overset{H^{\otimes n}}{\longmapsto} \sum_{y\in\{0,1\}^n} \hat{f}(x)|x\rangle, \tag{126}$$

其中 $\hat{f}(x) := \frac{1}{N}\sum_{y\in\{0,1\}^n}(-1)^{x\cdot y} f(y)$ 是 f 的傅里叶系数。给定对 M 随机布尔函数的预言机访问以及这些样本，我们定义了 LLQSV 问题的黑盒版本。具体而言，算法可访问酉算子 $\mathcal{O}$：$|i, x\rangle \mapsto f_i(x)|i, x\rangle$，其中 i 的取值范围为 1 到 M，而 $f_1,\ldots,f_M$ 是从 n-位布尔函数的均匀分布 $\mathcal{F}_n$ 中采样得到的随机函数。LLQSV 的黑盒版本正式定义如下。

问题 5 (黑盒 LLQSV)。对于 $M = 2^{O(n)}$，给定通过酉算子 $\mathcal{O}$：$|i,x\rangle \mapsto f_i(x)|i,x\rangle$ 访问字符串 $s_1,\ldots,s_M \in \{0,1\}^n$ 以及函数 $f_1,\ldots,f_M \sim \mathcal{F}_n$，判断在是情况下是否有 $s_i \sim |\hat{f}_i|^2$；或者在否情况下，每个 s_i 是否均从均匀分布中采样（因此与 f_i 独立）。

证明分为以下几个步骤。我们证明 LLQSV 不属于 QIP[2], ，即不属于那些存在双消息量子交互证明系统的问题类，即使相对于随机预言机也是如此。该证明与 Bassirian、Bouland、Fefferman、Gunn 和 Tal 关于 BQP 的黑盒 LLQSV 下界密切相关 [14], ，后者也使用了混合论证, [17], 但我们在此将困难性加强到了 QIP[2]。因此，该问题不属于 QCAM。

然而，混合论证并不能直接推出 QCAM/qpoly 的困难性。根据 Aaronson 和 Drucker 的交换定理，QCAM/qpoly $\subseteq$QMA/poly，因此只需证明后者具有困难性。接着，我们利用多项式方法给出查询下界，并借助 Sherstov [58] 的强直接积定理。

5.4.1 双消息量子交互式证明

为了证明 LLHA 相对于 $\mathcal{O}$ 成立，我们先给出直观解释。如果算法无法访问$\mathcal{O}$，那么在两种情况下，s_1、.....、s_M都服从均匀分布。因此，我们也可以将 $\mathcal{O}$ 视为一种分布，它可能依赖于均匀分布的 s_1、.....、s_M，也可能不依赖。以下引理陈述了这一事实。

引理 5.12。设 $\mathcal{F}_n$ 是 n 位布尔函数 $\{0,1\}^n \to \{+1,-1\}$ 上的均匀分布，$\mathcal{U}_n$ 是 n 位字符串上的均匀分布。以下两个采样过程等价，即它们的输出分布相同：

- 采样 $f \sim \mathcal{F}_n$，然后采样 $s \sim |\hat{f}|^2$。输出 $(f,\ s)$。
- 采样 $s \sim \mathcal{U}_n$，然后采样 $f \sim \mathcal{G}_{n,\ s}$，其中 $\mathcal{G}_{n,\ s}(f) = \mathcal{F}_n(f) \cdot |\hat{f}(s)|^2 \cdot N$。输出 $(f,\ s)$。

证明。设第一个分布的概率密度为 $\mu(f,s) = \mathcal{F}_n(f) \cdot |\hat{f}(s)|^2$。边缘分布

$$\begin{aligned}\mu(s) &= \sum_f \mathcal{F}_n(f) \cdot |\hat{f}(s)|^2 \\ &= \mathop{\mathbb{E}}_f[|\hat{f}(s)|^2] \\ &= \frac{1}{N}.\end{aligned} \tag{127}$$

接下来只需计算 $\mu(f|s)$：

$$\begin{aligned}\mu(f|s) &= \frac{\mu(f,s)}{\mu(s)} \\ &= \mathcal{F}_n(f) \cdot |\hat{f}(s)|^2 \cdot N.\end{aligned} \tag{128}$$

□

接下来我们定义 以下承诺问题，称为布尔函数偏差检测（BFBD ）.

定义 5.13 (布尔函数偏差检测（BFBD）**)**。布尔函数偏差检测问题要求区分以下情形：

- **是例**：对于每个 $i \in [M]$，抽取样本 $f \sim \mathcal{G}_n$，其中 $\mathcal{G}_n$ 是密度为$\mathcal{G}_n(f) := N(1-2\Delta(f))^2\mathcal{F}_n(f)$的概率分布，其中 $\Delta(f)$ 是取值为 -1 的元素比例，即 $\Delta(f) := \frac{1}{N}|\{x :\ f(x) = -1\}|$。
- **否例**：对于每个 $i \in [M]$，抽取分布 $f \sim \mathcal{F}_n$。

对于函数 f，我们也将 $\Delta(f)$ 称为 f 的距离。现在我们证明 BFBD 可归约到 LLQSV，因此只需证明 BFBD 的下界。

引理 5.14. BFBD 可归约为LLQSV。

证明。归约如下进行：从均匀分布中采样 $s_1, \ldots, s_M$，并模拟预言机 $\mathcal{Q}: |i,x\rangle \mapsto (-1)^{s_i \cdot x}|i,x\rangle$。使用预言机 $\mathcal{Q}\mathcal{O}$运行 LLQSV 协议，实际上该协议获得了对函数 $g_i = \chi_{s_i} \cdot f$ 的预言机访问，其中 $\chi_{s_i}(x) := (-1)^{s_i \cdot x}$ 对每个 $i \in [M]$ 都成立。要说明归约为何有效，只需证明每个预言机都与

LLQSV 的相应情况具有相同的分布。在否情况下，对于均匀分布的 s 和 f， $\chi_s \cdot f$ 的分布均匀且独立于 s。在是情况下，令 $g = \chi_s \cdot f$: g 的密度 μ 可按如下方式计算:

$$\begin{aligned}\mu(g|s) &= N(1-2\Delta(g\cdot\chi_s))^2 \cdot \mathcal{F}_n(g\cdot\chi_s)\\ &= N(1-2\Delta(g\cdot\chi_s))^2 \cdot \mathcal{F}_n(g).\end{aligned} \tag{129}$$

第二个等 式成立，因为 $\mathcal{F}_n$ 是均匀分布。剩下要证明 $\hat{g}(s) = 1-2\Delta(g\cdot\chi_s)$:

$$\begin{aligned}\hat{g}(s) &= \frac{1}{N}\sum_x \chi_s(x)f(x)\\ &= \frac{1}{N}\sum_{x:\chi_s(x)f(x)=1}\chi_s(x)f(x) - \frac{1}{N}\sum_{x:\chi_s(x)f(x)=-1}\chi_s(x)f(x)\\ &= 1-2\Delta(g\cdot\chi_s).\end{aligned} \tag{130}$$

□

尽管我们的目的是证明 LLQSV，或等价地 BFBD，不属于 QCAM，但这里我们证明一个更强的结果：BFBD 不属于 QIP[2]。首先注意到，每个分布都可以通过先选取距离 Δ，再从所有距离为 Δ的函数中按照均匀分布采样一个函数 f 来生成。更正式地说，BFBD 等价于以下问题:

- **否例**: 对于每个 $i \in [M]$，采样 $D_i \sim \text{Binomial}(N, 1/2)$，即具有 N次试验和偏置 $1/2$的二项分布，并设定 $\Delta_i = D_i/N$，也就是说，密度为

$$p_0(\Delta_i) = \binom{N}{N\Delta_i}2^{-N}. \tag{131}$$

  然后采样 $f_i \sim \mathcal{H}_{\Delta_i}$，即在所有距离为 $\Delta(g) = \Delta_i$的函数 g 上的均匀分布。

- **是例**: 对于每个 $i \in [M]$，根据密度为 p_1 的分布对 Δ_i 进行采样

$$p_1(\Delta_i) := p_0(\Delta_i)\cdot N(1-2\Delta_i)^2. \tag{132}$$

  然后对 $f_i \sim \mathcal{H}_{\Delta_i}$ 进行采样。

然后我们证明，对于每个分布， Δ 都集中在 $1/2$ 附近，这使我们只需考虑 Δ 与 $1/2$ 足够接近的事件。

引理 5.15。对于 $b \in \{0,1\}$ 和 $\alpha > 0$,

$$\Pr_{\Delta_1,\ldots,\Delta_M\sim p_b}\left[\exists i, |\Delta_i - 1/2| \geq \frac{\alpha}{\sqrt{N}}\right] \leq 2MNe^{-2\alpha^2}. \tag{133}$$

证明。 在否情况中，由于 f 中的每个元素都是一枚公平硬币，根据霍夫丁不等式和并集界,

$$\Pr_{\Delta_1,\ldots,\Delta_M\sim p_0}\left[\exists i, |\Delta_i - 1/2| \geq \frac{\alpha}{\sqrt{N}}\right] \leq 2Me^{-2\alpha^2}. \tag{134}$$

在是情况中，

$$\Pr_{\Delta_1,\ldots,\Delta_M\sim p_1}\left[\exists i, |\Delta_i - 1/2| \geq \frac{\alpha}{\sqrt{N}}\right] \leq M \Pr_{\Delta\sim p_1}\left[|\Delta - 1/2| \geq \frac{\alpha}{\sqrt{N}}\right] \leq 2MNe^{-2\alpha^2}. \tag{135}$$

第二个不等式成立，因为对于 $p_1(\Delta) \leq N \cdot p_0(\Delta)$，根据霍夫丁不等式可得。 □

对于每个分布，考虑事件 Ω，其中 $|\Delta - 1/2| \leq t$，且 $t = ((\ln MN^2)/N)^{1/2} = O((n/N)^{1/2})$。根据引理 5.15，在给定 Ω 的条件下，间隙至多减少 $O(1/N)$。于是，对于 $(\Delta_1, \ldots, \Delta_M) \in \Omega$，我们处理的是对每个 i均从 H_{Δ_i} 分布中抽取的函数。由于 $\mathcal{H}_\Delta$可以通过翻转 $f \sim \mathcal{H}_{1/2}$的 $|\Delta - 1/2|N$ 位得到，因此我们可以利用 BBBV 给出查询下界。

在给出证明之前，我们先刻画双消息量子交互证明系统在区分两个分布 $\mathcal{D}_1$ 和 $\mathcal{D}_0$时的行为。在两消息协议中，验证者首先向 f 进行 T_1 次查询，其中 f 从 $\mathcal{D}_1$ 或 $\mathcal{D}_0$ 中抽样，然后计算一个二分量子态σ_{AB}。验证者将第一系统 A 发送给（不受限的）证明者，证明者执行任意量子过程 $\mathcal{P} \in$ 完全正迹保持(A, A')，并返回第二条量子消息 $\tau_{A'}$。令所得量子态为 $\tau_{A'B} := \mathcal{P} \otimes \mathbb{I}_B(\sigma_{AB})$。随后，验证者继续在输入 $\tau_{A'B}$ 上进行 T_2 次查询，并输出一个判定位。一个 T-查询协议定义为进行 $T = T_1 + T_2$ 次查询的协议。如果验证者在给定 $\mathcal{D}_b$ 时以至少 $2/3$的概率输出 b，则称该协议解决了这个问题。

我们的目标是确定 b，给定对 M 个样本 Δ_1、.....、$\Delta_M \sim p_b$ 的访问权限，这些样本编码为预言机 $\mathcal{O}$。为了证明不存在能够解决该问题的协议，我们从任意一个在是实例上以至少 $2/3$ 的概率输出 1 的验证者开始。我们证明，当给定否实例时，存在一个证明者，能以至少 $2/3 - \eta$ 的概率说服验证者，其中 η 可忽略。更具体地说，我们通过以下步骤对一个是实例进行随机修改，使其变为否实例：

1. 给定 f_1、.....、f_M，对于 $i \in [M]$，计算 $\Delta_i = \Delta(f_i)$ 和 $S_i = \{x : f_i(x) = -1\}$。另外令 $\bar{S}_i = \{0,1\}^n \backslash S_i$。

2. 对 Δ'_1、.....、$\Delta'_M \sim p_0$ 进行采样。对于 $i \in [M]$，若 $\Delta'_i \geq \Delta_i$，则选择 S_i 的一个随机子集 R，使得 $|R| = \Delta'_i - \Delta_i$。令 $g_i(x) = f_i(x) \cdot (-1)^{\mathbb{I}_R(x)}$，其中 $\mathbb{I}_R$ 是集合 $R \subseteq \{0,1\}^n$ 的示性函数；否则，选择 $\bar{S}_i$ 的一个随机子集 R，使得 $|R| = \Delta_i - \Delta'_i$。令 $g_i(x) = f_i(x) \cdot (-1)^{\mathbb{I}_R(x)}$。

3. 输出 $g_1, \ldots, g_M$。

接下来我们证明，该修改会产生一个否实例。

引理 5.16. 以下两个过程是等价的，也就是说，它们的输出分布相同：

1. 输出 $g_1,\ldots, g_M \sim \mathcal{F}_n$。 *2.* 抽取样本 $f_1, \ldots, f_M \sim \mathcal{G}_n$ 并执行上述修改。输出 $g_1, \ldots, g_M$。

证明。 只需证明，对于每个 $\Delta_1, \ldots, \Delta_M$，对乘积分布 $\mathcal{H}_{\Delta_1} \times \ldots \times \mathcal{H}_{\Delta_M}$ 进行修改后会得到分布 $\mathcal{F}_n$，因为 $\mathcal{G}_n$ 是 $\Delta_1, \ldots, \Delta_M \sim p_0$对应的 $\mathcal{H}_{\Delta_1} \times \ldots \times \mathcal{H}_{\Delta_M}$的概率混合。对于每个 $i \in [M]$，回顾一下，$f_i \sim \mathcal{H}_{\Delta_i}$是大小为 $\Delta_i N$的随机子集。如果 $\Delta'_i \geq \Delta_i$，从 S_i 中移除 $\Delta'_i - \Delta_i$ 个元素后，会得到一个大小为 Δ'_i的随机子集。另一种情况的证明类似。 □

我们直观地说明，为什么对于每个 $o((N/n)^{1/4})$ 次查询的量子交互式证明协议 [2]，都存在一个作弊证明者。根据引理 5.15，以概率 $O(1/N)$，对于从 $\mathcal{G}_n$中抽取的函数的选择，$|\Delta_i - 1/2| \leq O((n/N)^{1/2})$ 对每个 $i \in [M]$都成立。再次根据引理 5.15，以概率 $O(1/N^{1/2})$，抽取 $\Delta'_1, \ldots, \Delta'_M \sim p_0$后，$|\Delta'_i - 1/2| \leq O((n/N)^{1/2})$。这意味着，从一个至少含有 $NM(1/2 - o(1))$ 个元素的集合中随机翻转$\sum_{i=1}^{M} |\Delta'_i - \Delta_i|N = O(\sqrt{nNM})$ 个元素，会得到一个否实例。根据 BBBV 的混合论证 [17],，求解 BFBD 必须进行 $O((N/n)^{1/4})$ 次查询。

Theo定理 5.17. 任何求解 量子交互式证明[2] 协议的 BFBD 都必须进行 $\Omega((N/n)^{1/4})$ 次查询 s.

证明。令 $\mathcal{V}$ 为任意一个验证者，它在是实例上以概率 $p \geq 2/3$输出 1。从是实例 $f_1, \ldots, f_M \sim \mathcal{G}_n$ 出发，根据引理 5.16，我们执行随机修改，得到函数 $g_1, \ldots, g_M$。令 $\Delta_i = \Delta(f_i)$ 和 $\Delta'_i = \Delta(g_i)$。根据引理 5.15，以概率 $O(1/N)$，$|\Delta_i - 1/2|$ 和 $|\Delta'_i - 1/2|$ 均以 $O((n/N)^{1/2})$ 为界。在此事件发生的条件下，$|\Delta_i - \Delta'_i| \leq O((n/N)^{1/2})$。

对于任意函数 $F = (f_1, \ldots, f_M)$，令证明者为一个量子信道 $\mathcal{P}_F \in$完全正迹保持(A, A')。给定对 $\mathcal{O} = \mathcal{O}(F)$ 的访问权限，其中编码了 F，令 $\mathcal{V}_{\mathcal{O}}^{(1)}$ 和 $\mathcal{V}_{\mathcal{O}}^{(2)}$ 分别为验证者在协议第一步和第二步中执行的酉信道。对于 $c \in \{1, 2\}$，不失一般性，我们可以写成

$$V_{\mathcal{O}}^{(c)} = U_{T_c}^{(c)} \mathcal{O} \ldots U_1^{(c)} \mathcal{O} U_0^{(c)}, \tag{136}$$

和 $\mathcal{V}_{\mathcal{O}}(\rho) = V_{\mathcal{O}} \rho V_{\mathcal{O}}^{\dagger}$。作弊证明者向验证者证明，自己获得了对 f_1、……、$f_M \sim \mathcal{G}_n$ 的预言机访问；但验证者获得的访问权限是 $\mathcal{O}(G)$，它编码了通过上述修改得到的 $G = (g_1$、……、$g_M)$。随机修改下的整体量子信道 $\mathcal{T}_F$ 定义为 $\mathcal{V}_{\mathcal{O}}^{(2)}{}_{(G)} \circ \mathcal{P}_F \circ \mathcal{V}_{\mathcal{O}}^{(1)}{}_{(G)}$。不失一般性，通过引入验证者无法访问的净化系统 E，我们可以假设，对于某个验证者也无法访问的系统 E'，$\mathcal{P}_F \in$ 完全正迹保持$(AE, A'E')$ 是一个酉信道。

我们的目标是证明 $\mathcal{V}_{\mathcal{O}}^{(2)}{}_{(F)} \circ \mathcal{P}_F \circ \mathcal{V}_{\mathcal{O}}^{(1)}{}_{(F)}$ 与 $\mathcal{T}_F$ 接近。根据三角不等式，

$$\begin{aligned}
\eta &:= \left\| \mathop{\mathbb{E}}_{G} \mathcal{V}^{(2)}_{\mathcal{O}(G)} \circ \mathcal{P}_F \circ \mathcal{V}^{(1)}_{\mathcal{O}(G)}(|0\rangle\langle 0|) - \mathcal{V}^{(2)}_{\mathcal{O}(F)} \circ \mathcal{P}_F \circ \mathcal{V}^{(1)}_{\mathcal{O}(F)}(|0\rangle\langle 0|) \right\|_{\mathrm{tr}} \\
&\leq \mathop{\mathbb{E}}_{G} \left\| \mathcal{V}^{(2)}_{\mathcal{O}(G)} \circ \mathcal{P}_F \circ \mathcal{V}^{(1)}_{\mathcal{O}(G)}(|0\rangle\langle 0|) - \mathcal{V}^{(2)}_{\mathcal{O}(G)} \circ \mathcal{P}_F \circ \mathcal{V}^{(1)}_{\mathcal{O}(F)}(|0\rangle\langle 0|) \right\|_{\mathrm{tr}} \\
&\quad + \mathop{\mathbb{E}}_{G} \left\| \mathcal{V}^{(2)}_{\mathcal{O}(G)} \circ \mathcal{P}_F \circ \mathcal{V}^{(1)}_{\mathcal{O}(F)}(|0\rangle\langle 0|) - \mathcal{V}^{(2)}_{\mathcal{O}(F)} \circ \mathcal{P}_F \circ \mathcal{V}^{(1)}_{\mathcal{O}(F)}(|0\rangle\langle 0|) \right\|_{\mathrm{tr}} \\
&\leq \mathop{\mathbb{E}}_{G} \left\| \mathcal{V}^{(1)}_{\mathcal{O}(G)}(|0\rangle\langle 0|) - \mathcal{V}^{(1)}_{\mathcal{O}(F)}(|0\rangle\langle 0|) \right\|_{\mathrm{tr}} + \mathop{\mathbb{E}}_{G} \left\| \mathcal{V}^{(2)}_{\mathcal{O}(G)}(\rho_F) - \mathcal{V}^{(2)}_{\mathcal{O}(F)}(\rho_F) \right\|_{\mathrm{tr}},
\end{aligned} \tag{137}$$

其中 $\rho_F := \mathcal{P}_F \circ \mathcal{V}_{\mathcal{O}}^{(1)}{}_{(F)}(|0\rangle\langle 0|)$ 是一个独立于随机修改的量子态。因此，只需给出第二项的一个上界；对于第一项，使用类似的论证即可得到一个上界，因为零态也独立于随机修改。

令 $|\psi_F\rangle$ 为任意不受随机修改影响的量子态 ρ_F 的纯化。

对于 $c \in \{1,2\}$，考虑以下量子态序列：

$$
\begin{aligned}
|\phi_{T_c}^G\rangle &= U_{T_2}^{(c)}\mathcal{O}(F)U_{T_2-1}^{(c)}\mathcal{O}(F)\dots U_1^{(c)}\mathcal{O}(F)U_0^{(c)}|\psi_F\rangle,\\
|\phi_{T_c-1}^G\rangle &= U_{T_2}^{(c)}\mathcal{O}(G)U_{T_2-1}^{(c)}\mathcal{O}(F)\dots \mathcal{O}(F)U_1^{(c)}\mathcal{O}(F)U_0^{(c)}|\psi_F\rangle,\\
&\vdots\\
|\phi_1^G\rangle &= U_{T_2}^{(c)}\mathcal{O}(G)U_{T_2-1}^{(c)}\mathcal{O}(G)\dots \mathcal{O}(G)U_1^{(c)}\mathcal{O}(F)U_0^{(c)}|\psi_F\rangle,\\
|\phi_0^G\rangle &= U_{T_2}^{(c)}\mathcal{O}(G)U_{T_2-1}^{(c)}\mathcal{O}(G)\dots \mathcal{O}(G)U_1^{(c)}\mathcal{O}(G)U_0^{(c)}|\psi_F\rangle. \qquad (138)
\end{aligned}
$$

第一个混合实验与最后一个混合实验之间的欧几里得距离，可以通过界定两个相邻混合实验之间的距离来界定：

$$
\||\phi_{T_1}^G\rangle - |\phi_0^G\rangle\| \le 2\sum_{i=0}^{T-1} \|_{\mathbb{I}} W|\psi_t\rangle\|, \qquad (139)
$$

其中，$|\psi_t\rangle := U_t\mathcal{O}(F)U_{t-1}\dots U_1\mathcal{O}(F)U_0|\psi_F\rangle$ 是经过 t 次查询后的中间态，而集合 $W := \{(i,x) : g_i(x) \neq f_i(x)\}$。注意，$|\psi^t\rangle$ 与 W 独立。回想一下，我们固定 F，并通过翻转随机元素来生成 G。根据（139），对 W 取期望可得

$$
\begin{aligned}
\mathop{\mathbb{E}}_W \|\mathcal{V}_{\mathcal{O}(G)}^{(2)}(\rho_F) - \mathcal{V}_{\mathcal{O}(F)}^{(1)}(\rho_F)\|_{\mathrm{tr}} &\le 2\mathop{\mathbb{E}}_W \||\phi_{T_1}^G\rangle - |\phi_0^G\rangle\|\\
&\le 4T_1\|Q\|_{\mathrm{op}}^{1/2}, \qquad (140)
\end{aligned}
$$

其中，$Q = \mathbb{E}_W \mathbb{I}_W$ $|W| = \sum_{i=1}^M |\Delta_i -:$。$\Delta_i'|N = O\ M\ nN^{1/2}$ $M\ N/2 - O\ \ nN^{1/2}$ $\|Q\| \le O\ \ n/N^{1/2}$

由于该修改从大小至少为（(( ))）的集合中随机选取大小为（( )）的子集，因此（（ ））。因此$\eta \le O(T($ $n/N)^{1/4})$。所以，验证者接受否情况的概率至少为 $p-\eta-O(1/N)$ $>1/3$。 □

定理定理 5.17 中的结论可以进一步加强为 QIP $=$ QIP[3]，方法是采用类似的混合论证。不过，由于我们不会用到这个结果，因此不再进一步探讨。根据 BFBD 和 LLQSV 之间的等价性（见引理 5.14 和 定理 5.17），我们立即得到以下推论。

推论 5.18。 存在一个常数 $c > 0$，使得 LLQSV $\notin$ QIP[2]$(c(N/n)^{1/4})$ 相对于随机预言机成立。

5.4.2 加强困难性

最后一步是将针对均匀复杂性类（如 QIP[2] 或其子类 QMA）的下界“提升”为针对非一致复杂性类 QCAM/qpoly 的下界（或推广到使用更多时间和更多辅助信息的情形）。

首先注意到，QCAM $=$ BP $\cdot$ QCMA，且BP$\cdot$ 算子可以通过多项式规模的经典辅助信息，利用 Adleman 技巧进行模拟。因此 QCAM/poly $=$QCMA/poly 以及 QCAM/qpoly $=$QCMA/qpoly。其次，Aaronson 和 Drucker [8] 证明了 QCMA/qpoly $\subseteq$QMA/poly。此外，所有这些结果都可以相对化。

我们应用 Sherstov [58] 提出的强直接积定理（SDPT），将困难性提升至 QMA/poly。回顾一下，Sherstov 证明了：当单个实例的查询下界是通过多项式方法 [15]得出的时，查询复杂度满足强直接积定理。

首先，我们给出一个预言机分离 coNP $\not\subset$QMA/poly；稍作修改后，LLQSV $\not\in$QMA/poly 的证明基本上也会遵循相同思路。

预热： coNP $\not\subset$ QMA/poly。为了给出一个预言机分离，预言机 F 编码 $N = 2^n$了该问题的实例。预言机 F 包含 N 个区段，每个区段 $F_x \in \{0,1\}^N$ 由一个 n位字符串 x索引。令是实例为全一函数，即对于每个 $x \in \{0,1\}^n$， $f_0(x) = 1$ 。否实例是通过翻转 εN个点得到的，其中 $\varepsilon \geq \eta$且 $\eta = 100/N$。每个区段 F_x 以 1/2 的概率为是情况或否情况。任务是：输入 x后，判定 F_x 属于哪种情况。该问题显然属于 coNP，因此下面定理的证明旨在说明该问题不属于 QMA/poly。

定理 5.19。存在一个预言机，使得 coNP $\not\subset$QMA/poly。

证明。令 $\mathcal{D}_x$ 表示对每个 $x \in \{0,1\}^n$的「是」情况和「否」情况的等权混合。对于$x \in \{0,1\}^n$，令 F_{-x} 表示除 F_x 以外的所有区段， $\mathcal{D}_{-x}$也同理。令 $f_0 = 1^N$ 表示是实例，并令 $\rho_{F,x}$表示在预言机访问 F并输入 x时给出的见证态。对于足够小的常数 c， $\eta = 100/N$、 $T = o((1/\eta)^{1/2}/n)$ 和 $S = cN$，我们的想法是证明：一组见证态 $\{\rho_x : x \in \{0,1\}^n\}$，若能使任何 QMA($T$)/$S$验证者 V在 $F_x = f_0$ 时以至少2/3 的概率信服，那么对于某个$x \in \{0,1\}^n$，也能使同一验证者以大于 1/3的概率接受一个否实例。因此， V无法解决这个问题。

反设结论不成立。那么，当 $F_x = f_0$ 时， V 以至少 2/3 的概率接受，即

$$\Pr_{F_x=f_0, F_{-x}\sim\mathcal{D}_{-x}}\left[V^F(w_F, x, \rho_x) = 1\right] \geq 2/3, \tag{141}$$

其中， $w_F \in \{0,1\}^S$是依赖于 F的经典辅助信息。此外，对 F_x应用该修改时，验证者可以借助辅助信息检测出变化。更具体地说，对于 $y \in \{0,1\}^n$，令 M_y 表示一个概率算法，它对 F 进行修改，将 $F_y = f_0$ 变为一个否实例；也就是说，若 $x = y$，则 $M_y(F)_x$属于否情况；否则， $M_y(F)_x = F_x$。根据我们的假设，应用该修改后，对每个 $x \in \{0,1\}^n$，

$$\Pr_{F_x=f_0, F_{-x}\sim\mathcal{D}_{-x}, M_x(F)=G}\left[V^G(w_G, x, \rho_x) = 0\right] \geq 2/3. \tag{142}$$

注意，辅助信息可能会因变化而改变。由于见证态不依赖于该修改，我们实际上可以将见证排除在考虑范围之外。

令 $\mathcal{D}_1$ 表示是情况的分布， $\mathcal{D}_0$ 表示否情况的分布。应用保持见证的放大后，令 V' 为 QMA($c'Tn$)/S 协议；对于足够大的常数 c'，该协议以至少 $1 - 1/N^2$ 的概率解决该问题。于是，我们可以~构造一个 QMA($c'TnN$)/S验证者 V来解决 N个问题：证明者在一条消息中发送见证态 $\rho := \bigotimes_{x\in\{0,1\}^n} \rho_x$，验证者对每个 $x \in \{0,1\}^n$ 运行 V'，并使用 ρ_x 和给定的辅助信息 w_F，即 $\tilde{V}^F(w_F, \rho) := \bigotimes_{x\in\{0,1\}^n}(V')^F(w_F, x, \rho_x)$。根据并集界， V以至少 $1 - 1/N$的概率输出正确的 N位字符串，即

$$\Pr_{b\sim\mathcal{U}_N, F\sim\mathcal{D}_b}\left[\tilde{V}^F(w_F, \rho) = b\right] \geq 1 - 1/N, \tag{143}$$

其中， $\mathcal{U}_N$ 表示在 N 位字符串上的均匀分布， $\mathcal{D}_b$ 表示分布 $\bigtimes_{x\in\{0,1\}^n} \mathcal{D}_{b_x}$。

现在我们将辅助信息 w_F 替换为一个随机字符串（独立于 F），根据 (143)，可得

$$\Pr_{b\sim\mathcal{U}_n, F\sim\mathcal{D}_b, r\sim\mathcal{U}_S}\left[\tilde{V}^F(r, \rho) = b\right] \geq \frac{1 - 1/N}{2^S} \geq \frac{1}{2^{S+1}}. \tag{144}$$

这实际上给出了一个 $c'TnN$-查询算法，以至少 2^{-S-1} 的概率解决 N 问题。对于每个问题，令 p 表示将与函数逼近到误差 $1/3$ 的实多项式。因此，我们的约束为：(i) $p(0) \geq 2/3$；(ii) 对每个 $1 \geq \varepsilon \geq \eta$ 且 εN 为整数，都有 $p(\varepsilon) \leq 1/3$。根据引理 3.7，$\deg(p) \geq \Omega(\sqrt{1/\eta})$。现在根据定理 3.8，对于充分小的常数 c 和 $S = cN$，以概率 2^{-S-1} 解决 N 个独立问题需要 $2cN\sqrt{1/\eta}$ 次查询。因此，必有 $c'TnN \geq 2cN\sqrt{1/\eta}$ 次查询，且 $T = \Omega(\sqrt{1/\eta}/n)$。 □

LLQSV $\notin$QMA/poly。LLQSV $\notin$ QMA/poly 的证明基本遵循 coNP $\not\subset$QMA/poly 的思路，但有以下修改。首先，分布 $\mathcal{D}_1$ 并不描述一个固定函数；相反，我们用 BFBD 中的“是情况”（定义 5.13）替代它。为此，我们基本上应用平均论证。其次，根据引理 5.15，BFBD 的“否情况”是通过在一个大小为 $O(\sqrt{n/N})$ 的随机子集上修改“是情况”得到的，其概率至少为 $1 - 1/N$。QMA/poly 验证者不再需要对每个 $\varepsilon \geq \eta$ 都解决该问题，而这对于使用多项式方法得到下界至关重要。我们证明，通过归约，可以获得足够多的约束，从而得到紧的下界。

这里我们描述相对于以下预言机的 LLQSV 问题：该预言机 F 包含N 个区段，每个区段由一个 n 位字符串 x 索引。每个区段 F_x 均匀采样自 n 位布尔函数，而样本 s_x 要么采样自 $\lceil F_x|^2$，要么是一个均匀分布的 n 位字符串（独立于 F_x）。在输入 x 上，协议需要判断：在是情况下，s_x 采样自 $\lceil F_x|^2$；在否情况下，则采样自均匀分布。

定理 5.20。 存在一个常数 $c > 0$，使得相对于随机预言机，LLQSV $\notin$ QMA$(c(N/n)^{1/4}/n)/(cN)$。

证明。 证明的基本思路与 定理 5.19 的证明相同。首先，根据 引理 5.14，令 $\mathcal{D}_1$ 和 $\mathcal{D}_0$分别表示 BFBD (定义 5.13) 中是情况和否情况对应的分布。在这个构造中，预言机的每个区段都从 $\mathcal{D}_1$ 或 $\mathcal{D}_0$中采样。令 $\mathcal{D}$ 表示 $\mathcal{D}_1$ 与 $\mathcal{D}_0$的等权混合。

思路是证明：对于 $T = o((N/n)^{1/4}/n)$，任意一组见证态 $\{\rho_{F,x} : F \in \{0,1\}^{N\times N}, x \in \{0,1\}^n\}$，若其能以概率 $2/3$ 说服任意 QMA$(T)/S$验证者 V，其中 $F_x \sim \mathcal{D}_1$，则对于某个 $x \in \{0,1\}^n$，它们也能以大于1/3的概率说服验证者 $F_x \sim \mathcal{D}_0$。反设对于每个 x，当 $F_x \sim \mathcal{D}_0$ 时，V 接受的概率至多为 $1/3$。令该修改表示将任意满足 $M_x(F_x)$ 的 F_x 更改为按 $\mathcal{D}_0$ 分布，而其他区段保持不变的操作。根据平均论证，对于每个 $x \in \{0,1\}^n$，都存在一个函数 F_x 和一个大小为 $r_x = O(\sqrt{nN})$ 的随机修改，使验证者以至少 $2/3 - o(1)$ 的概率检测出是否进行了修改。于是，根据随机自归约性，存在一个验证者，对于所有大小为 r_x 的修改，也能以至少 $2/3 - o(1)$ 的概率输出正确答案。

通过保持见证的放大，存在一个 QMA$(O(Tn))/S$ 验证器，它能以至少 $1 - 1/N^2$ 的概率检测每个 x 上是否存在大小为 r_x 的随机修改。假设 ~ ~意味着存在一个 QMA$(O(TNn))/S$验证器 V，它以至少 $1 - O(1/N)$ 的概率解决 N 问题（即，对于每个 $x \in \{0,1\}^n$，V判断是否存在大小为 r_x 的修改），且其见证态 $\rho_F := \bigotimes_{x\in\{0,1\}^n} \rho_F$ 与这些修改$_x$ 独立。现在，我们用一个随机字符串替换辅助字符串，从而得到一个 $O(TNn)$-查询 QMA 验证器，该验证器接收见证态 ρ_F，并以至少 2^{-S-1} 的概率在见证 ρ_F 上解决 N 问题。然后应用定理 3.8 可得，对于任意实多项式 p，只要它对 $S = cN$ 上待计算的函数的近似误差不超过 $1/5$（其中 c 是充分小的常数），就有 $\deg(p) = O(Tn)$。

还需证明：在大小为 $r \leq O(\sqrt{nN})$ 的随机子集R上检测修改的每个 T'-查询算法，都意味着存在一个 T'-查询算法，它能在 $|R'| \in \{1,2,\ldots,|Q'|\}$ 上检测随机修改 $R' \subseteq Q'$，且 $|Q'| = \Omega(q/r)$。因此，我们可以使用多项式方法得出结论：每个解决该问题的 T'-查询算法都必须满足 $2T' = \deg(p)$；对于任何满足以下约束的多项式 p：(i) $p(0) \geq 2/3$，以及 (ii)$p(i) \leq 1/3$，其中 $i \in \{1,2,\ldots,|Q'|\}$。根据引理 3.7，$\deg(p) = \Omega(\sqrt{|Q'|}) = \Omega((N/n)^{1/4})$，因此 $T = \Omega(T'/n) = \Omega((N/n)^{1/4}/n)$。

不失一般性，令 $Q = [q]$ 和 R 为大小为 r的随机子集。对于每个函数$f_0 : [q] \to \{0,1\}$，我们将问题 $\mathcal{P}_{q,r}$ 定义如下：在是情况下，算法可以访问 $f = f_0$；在否情况下，算法可以访问 $f(x) := f_0(x) \oplus \mathbb{I}[x \in R]$，其中 R 是一个大小为 r的随机子集。因此，根据上一段，我们的目标是证明，若有算法能够解决 $\mathcal{P}_{q,r}$，则可以据此得到一个算法，使用相同数量的查询来解决 $\mathcal{P}_{\eta,\ell}$，适用于 $\eta = \lfloor q/r \rfloor$ 和每个 $\ell \in \{1,2,\ldots,\eta\}$。首先，我们可以将参数 η,ℓ 扩展 $\alpha \geq 1$ 倍，从而得到 $\mathcal{P}_{\alpha\eta,\alpha\ell}$中的一个实例 g：定义 $\tilde{g}$：$[\alpha\eta] \to \{0,1\}$, $\tilde{g}(x) := f(((x-1) \bmod \eta) + 1)$，并令函数 $g(x) := \tilde{g} \circ \pi(x)$，其中 π 是在 $[\alpha\eta]$上的一个随机置换。其次，我们可以用β个元素对函数进行填充，从而得到从 $\mathcal{P}_{\eta,\ell}$到 $\mathcal{P}_{\eta+\beta,\ell}$的归约：令 $\tilde{g}$：$[\eta+\beta] \to \{0,1\}$, $\tilde{g}(x) = f(x)$，其中 $x \in [q]$，且 $\tilde{g}(x) = 0$，其中 $x > \eta$；函数 $g := \tilde{g} \circ \pi$，其中 π 是在 $[\eta+\beta]$上的一个随机置换。对于问题 $\mathcal{P}_{\eta,\ell}$，我们先进行扩展，得到 $\mathcal{P}_{\eta r/\ell,r}$，再用 $q - \eta r/\ell$ 个元素进行填充，得到 $\mathcal{P}_{q,r}$。 □

将强大的量子复杂性类与量子辅助信息结合时，需要格外谨慎。例如，Raz [53] 证明了 QIP/qpoly = ALL（ALL 是所有语言组成的复杂性类），Aaronson [2] 也同样证明了 PDQP/qpoly =ALL；其中，PDQP 是 BQP 的推广，允许进行多次非扰动测量 [6]。基于强直接积定理的证明还可以进一步加强我们的结果，得到 LLQSV $\notin$ QMA/qpoly，从而为相对于随机预言机的 QMA/qpoly $\neq$ ALL 提供一种新的证明。此前，Aaronson 证明了 QMA/qpoly $\subseteq$PSPACE/poly [1]。

需要指出的是，该证明技巧无法让我们证明这个问题不属于 QIP[2]/qpoly =ALL，因为目前没有通用的回绕过程可以恢复量子辅助信息以供再次使用。

无论如何，上述内容足以证明以下结论。

定理 5.21。 相对于随机预言机，LLQSV $\notin$ QCAM(c^n)/q(c^n)，对于某个常数 $1 < c < 2$。

6 执行理想测量的设备

在本区段中，我们考虑如下设备：在接收到 Haar 随机电路之前，该设备可以与 Eve 共享任意纠缠 ψ_{DE}。接收到 $C \sim$ Haar(N) 后，该设备 $\mathcal{A}$执行理想测量，即在 ρ_{DE}的系统 D 上运行电路 C，并进行标准基测量以输出字符串。另一方面，窃听者 Eve 可以对第二系统 E施加任意量子操作，从而获取有关该设备输出的信息，但无法直接访问 $\mathcal{A}$的系统及输出。在接下来的讨论中，我们也将这类设备称为 $\mathcal{A}$ 半诚实设备。

6.1 单轮分析

一般而言，第一系统是一个希尔伯特空间 $D \cong \mathbb{C}^{2^d}$，对应于 $d \geq n$。不失一般性，我们只需考虑 $D \cong \mathbb{C}^N$，即 $d = n$的情况。原因在于，对于 $d \geq n$，我们可以将 $D = D' \otimes D''$ 分解，使得 $\mathcal{H}_{D'} \cong \mathbb{C}^N$ 是电路 C 作用的系统，并令 $E' = D'' \otimes E$。在这种情况下，只需找到 $H(D'|E')_\rho$ 的下界，因为 $H(D|E)_\rho \geq H(D'|E')_\rho$ 且$H_{\min}(D|E)_\rho \geq H_{\min}(D'|E')_\rho$；其中，$\rho = \mathcal{A}_D^C \otimes \mathbb{I}_E(\psi)$ 是验证者选取 C 时执行理想测量后得到的经典-量子态。因此，在接下来的分析中，我们假设 $D \cong \mathbb{C}^N$，且 $\mathcal{A}^C$ 是 C 在 D上的酉信道。

6.1.1 Holevo信息

根据量子操作的线性性，不失一般性，我们可以考虑一种特殊情形：设备与窃听者共享一个纯态，该态可写成施密特分解

$$|\psi\rangle = \sum_{i \in \{0,1\}^n} \sqrt{\lambda_i} |\phi_i\rangle_D |\psi_i\rangle_E, \tag{145}$$

其中，对于每个 i， $\lambda_i \geq 0$ 均为实数，并且 $\{|\phi_i\rangle\}$ 和 $\{|\psi_i\rangle\}$ 是两组正交归一向量。我们还记 $\psi := |\psi\rangle\langle\psi|$。

引理6.1。对于任意算法 $\mathcal{A}$，令 $\sigma = \mathcal{A}^C(\psi)$ 为在第一系统 D 上根据 C 执行投影测量后得到的经典-量子态。那么， σ 的 *Holevo*信息记为 $\chi(D:E)_\sigma = H(\lambda)$，其中 $H(\lambda)$ 是分布λ的香农熵。

证明。我们考虑酉算子 $U := \sum_i |\phi_i\rangle\langle i|$，并令 $U_{ij} = \langle i|U|j\rangle$ 为矩阵 U 的一个元素。再令 $U = \sum_{ji} U_{ji} |\psi_i\rangle\langle\psi_j|$， $\rho = \sum_i \lambda |i\rangle\langle i|$ 和 $\bar{\rho} = \sum_i \lambda_i |\psi_i\rangle\langle\psi_i|$。由于 $\{|\psi_i\rangle\}$ 是一组正交归一向量，U 也是一个作用于空间 span$\{|\psi_i\rangle\}$ 上的酉算子。纠缠 $|\psi\rangle$ 可以用标准基表示为:

$$\begin{aligned}
|\psi\rangle &= \sum_i \sqrt{\lambda_i} U |i\rangle |\psi_i\rangle \\
&= \sum_{ij} \sqrt{\lambda_i} U_{ji} |j\rangle |\psi_i\rangle \\
&= \sum_{ij} \sqrt{\lambda_i} |j\rangle |\psi_i\rangle\langle\psi_i| \bar{U} |\psi_j\rangle \\
&= \sum_j |j\rangle_D \bar{\rho}^{1/2} \bar{U} |\psi_j\rangle_E.
\end{aligned} \tag{146}$$

我们定义次归一化纯态

$$\sigma_i := \bar{\rho}^{1/2} \bar{U} |\psi_i\rangle\langle\psi_i| \bar{U}^\dagger \bar{\rho}^{1/2}, \tag{147}$$

并计算 Holevo信息:

$$\begin{aligned}
\chi(D:E)_{\mathcal{A}^C(\psi)} &= H(E)_{\sum_i \sigma_i} - \sum_i \alpha_i H(E)_{\sigma_i/\alpha_i} \\
&= H(\lambda).
\end{aligned} \tag{148}$$

其中 $H(\lambda)$ 是 λ 的香农熵，且 $\alpha_i := \mathrm{tr}(\sigma_i)$。式 (148) 中的第二个等号成立，因为

$$\sum_i \sigma_i = \bar{\rho}, \tag{149}$$

以及 $H(E)_{\bar{\rho}} = H(\lambda)$此外，由于$\frac{1}{\alpha_i}\sigma_i$ 是归一化纯态，因此 $H(E)_{\sigma_i/\alpha_i} = 0$。请注意，$\sum_i \sigma_i$ 独立于 U，因此即使对第一系统 D执行不同的测量，Holevo信息也不会改变。因此，对于每个 C，Holevo信息为 $H(\lambda)$。 □

接下来，我们证明，如果该设备能够解决$\frac{(2-\varepsilon}{N+1}N)$-XHOG，那么 Holevo 信息至多为$\varepsilon n + 1$。这一观察可用于建立条件冯·诺依曼熵的下界。

6.1.2 高 XHOG 得分意味着 Holevo 信息较小

此前，我们已经证明，已知施密特分解时，可以明确计算 Holevo 信息。本区段中，我们将建立 Holevo 信息与任意半诚实设备的得分之间的联系。

首先，我们引入一个有用的技术引理。

引理6.2。 设 p 是 p 上的一个分布，其中 p 是含有 N 个元素的有限集合，并且存在 $x \in \mathcal{X}$、$p(x) \geq 1 - \varepsilon$。那么，香农熵 $H(p) \leq \varepsilon n + 1$。

证明。 令 $p(x) = 1 - \gamma$（对 $\gamma \leq \varepsilon$ 成立），并令 q 为在事件 $y \neq x$ 发生条件下的条件分布，即$q(y) = p(x)/\gamma$（对 $y \neq x$成立）。根据定义，

$$\begin{aligned} H(p) &= -p(x)\log p(x) - \sum_{y\neq x} p(y)\log p(y) \\ &= -(1-\gamma)\log(1-\gamma) - \gamma\sum_{y\neq x} q(y)(\log q(y) + \log\gamma) \\ &= -(1-\gamma)\log(1-\gamma) - \gamma\log\gamma - \gamma\sum_{y\neq x} q(y)\log q(y) \\ &= h(\gamma) + \gamma H(q), \end{aligned} \tag{150}$$

其中，h 是二元熵函数，满足 $h(\gamma) \leq 1$（对 $\gamma \in [0,1]$成立）。由于 q 是定义在 $N-1$ 个元素上的分布，其香农熵的上界为 $\log(N-1) \leq n$。 □

根据 引理6.2，要证明 Holevo信息很小，只需说明当XHOG得分较高时，分布 λ 必须集中在单个点上。

引理 6.3。 由任意半诚实设备获得的、求解$\frac{(2-\varepsilon}{N+1}N)$-XHOG 的经典-量子态的*Holevo*信息至多为 $\varepsilon n + 1$。

证明。 我们分析设备在输入标准基向量 $|i\rangle$ 时的 XHOG得分：

$$S_i := \mathop{\mathbb{E}}_{C\sim\mathrm{Haar}(N)}\left[\sum_z q_{C,i}(z)p_C(z)\right]. \tag{151}$$

其中 $q_{C,\ i}(z)\ = |\langle z|C|i\rangle|^2$。对于 $i = 0$, $q_{C,\ 0} = p_C$ 得分为 $\frac{2}{N+1}$。对于 $i \neq 0$, $p_C(z)$ 和 $q_{C,\ i}(z)$ 的分布可视为 $P \sim$狄利克雷分布 $\mathbf{Dir}(1^N)$ 中的两个不同元素。这些事实意味着

$$\begin{aligned} S_i &= N \cdot \mathop{\mathbb{E}}_{P\sim \mathrm{Dir}(1^N)}[P_0 P_i] \\ &= \frac{1+\delta_{i0}}{N+1}. \end{aligned} \tag{152}$$

根据定义，使用 $|\psi\rangle$ 时的XHOG得分为

$$\begin{aligned} S &= \mathop{\mathbb{E}}_{C}\left[\sum_z p_C(z)\langle\psi|(C^\dagger|z\rangle\langle z|C)\otimes {}_{\mathbb{I}}|\psi\rangle\right] \\ &= \sum_i S_i \cdot \langle\psi_i|\bar{U}^\dagger\bar{\rho}\bar{U}|\psi_i\rangle. \end{aligned} \tag{153}$$

令 $\bar{\tau}$:= $\bar{U}^\dagger\bar{\rho}\bar{U}$和 $\bar{\tau}'$为在基底 $\{|\psi_i\rangle\}$下测量 $\bar{\tau}$后得到的量子态。若 $S \geq {}^{2}$ $\frac{-\varepsilon}{N+1}$,

$$\begin{aligned} \frac{2-\varepsilon}{N+1} &\leq \sum_i S_i \bar{\tau}'_{ii} \\ &= \frac{1+\bar{\tau}'_{00}}{N+1}. \end{aligned} \tag{154}$$

这意味着 t 帽 $\bar{\tau}'_{00} \geq 1-\varepsilon$。根据 引理6.1，Holevo信息可以被上界为 d:

$$\chi(D:E)_{\mathcal{A}^C(\rho)} = H(E)_{\bar{\tau}} \leq H(E)_{\bar{\tau}'} \leq \varepsilon n + 1. \tag{155}$$

由于 $\bar{\tau}'$是通过对 τ进行投影测量 $\{|\psi_i\rangle\}$得到的，根据引理3.11， $H(E)_{\bar{\tau}} \leq H(E)_{\bar{\tau}'}$。第二个不等式由引理6.2得出。此外，当 U是单位矩阵时，不等式取等号，即 $\{|\psi_i\rangle\}$ 是标准基。

□

我们注意到，引理 6.3 中的界几乎是最优的：考虑设备与 Eve 共享的纠缠是如下量子态的情形

$$|\psi\rangle_{DE} = (1-\varepsilon)^{1/2}|0,0\rangle + \left(\frac{\varepsilon}{N-1}\right)^{1/2}\sum_{x\neq 0}|x,x\rangle. \tag{156}$$

由引理6.1 得到的 Holevo 信息为 $\varepsilon\log(N-1)\ + h(\varepsilon)$。

6.1.3 单轮分析

现在我们证明，较小的 Holevo 信息意味着较大的条件冯·诺依曼熵。我们采用 [11] 和 [10]中的思路。令 D 和 E 分别表示设备的输出随机变量和 Eve 的量子寄存器。根据定义，Holevo 信息

$$\chi(D:E)_{\mathcal{A}^C(\rho)} = H(E)_{\mathcal{A}^C(\rho)} - H(E|D)_{\mathcal{A}^C(\rho)}, \tag{157}$$

其中 H 表示冯·诺依曼熵。下述定理给出了设备解决 b-XHOG（针对 $b \approx (2-\varepsilon)$）时冯·诺依曼熵的线性下界。

定理 6.4。 对于任意设备 $\mathcal{A}^C$，若其能够访问 C，并对任意二分量子态 ρ_{DE} 的第一系统 D 执行理想测量，且针对 $b \geq (2-\varepsilon\ N)$ 解决 *b-XHOG*，

$$\Pr_{C\sim\mathrm{Haar}(N)}\Big[H(D|E)_{\mathcal{A}^C(\rho)} \geq (0.99-\varepsilon)n\Big] \geq 1 - O\left(\frac{1}{N^{0.02}}\right). \tag{158}$$

证明。 设 $\mathcal{A}^C$ 是执行理想测量以得到 $\psi^C_{DE} := \mathcal{A}^C(\rho)$ 并输出随机变量 D的任意设备。我们注意到

$$\begin{aligned} H(D|E)_{\psi^C} &= H(DE)_{\psi^C} - H(E)_{\psi^C} \\ &= H(D)_{\psi^C} + H(E|D)_{\psi^C} - H(E)_{\psi^C} \\ &= H(D)_{\psi^C} - \chi(D:E)_{\psi^C}. \end{aligned} \tag{159}$$

第三行中的第一项 (159)，即 $H(D)^{\psi^C}$，表示 Eve 的系统 E 为空时设备输出的冯·诺依曼熵。为了给 (159)中的第一项求下界，回顾$q_{C,\ i}(z) = |\langle z|C|i\rangle|^2 = p_{CX^i}(z)$。由 (44) 以及 Haar 测度的右平移不变性，对每个 i,

$$\begin{aligned} \Pr_{C\sim\mathrm{Haar}(N)}[H(p_{CX^i}) \geq 0.99n+1] &\geq \Pr_C\big[S_C \leq N^{-0.99}/2\big] \\ &\geq 1 - O\left(\frac{1}{N^{1.02}}\right). \end{aligned} \tag{160}$$

由并集界,

$$\Pr_{C\sim\mathrm{Haar}(N)}\left[\min_{i\in\{0,1\}^n} H(p_{CX^i}) \geq 0.99n+1\right] \geq 1 - O\left(\frac{1}{N^{0.02}}\right). \tag{161}$$

现在根据 香农熵的凸性以及定义 $q_C(z) = \mathbb{E}_{i\sim\bar{\tau}'}[q_{C,i}(z)$],

$$\begin{aligned} \Pr_{C\sim\mathrm{Haar}(N)}[H(q_C) \geq 0.99n+1] &\geq \Pr_{C\sim\mathrm{Haar}(N)}\left[\mathop{\mathbb{E}}_{i\sim\bar{\tau}'}[H(p_{CX^i})] \geq 0.99n+1\right] \\ &\geq \Pr_{C\sim\mathrm{Haar}(N)}\left[\min_i H(p_{CX^i}) \geq 0.99n+1\right] \\ &\geq 1 - O\left(\frac{1}{N^{0.02}}\right). \end{aligned} \tag{162}$$

因此，由于 $H(D)_{\psi^C} = H(q_C)$,

$$\Pr_{C\sim\mathrm{Haar}(N)}\big[H(D)_{\psi^C} \geq 0.99n+1\big] \geq 1 - O\left(\frac{1}{N^{0.02}}\right). \tag{163}$$

在引理 6.3中，我们证明了对于每个 C，$\chi(D:\ E)_{\psi^C} \leq \varepsilon n + 1$。于是由(163)，

$$\Pr_{C\sim\mathrm{Haar}(N)}\big[H(D|E)_{\psi^C} \geq (0.99-\varepsilon)n\big] \geq 1 - O\left(\frac{1}{N^{0.02}}\right). \tag{164}$$

□

输入：安全参数 n、轮数 m、得分参数 $\delta \in [0,1]$ 和测试轮次比例 γ。

该协议：

1. 验证者从 $C \sim \text{Haar}(N)$中采样。对于 $i = 1, \ldots, m$，执行以下步骤：

   (a) 验证者向设备发送 C。（此步骤可以省略。）(b) 设备返回一个样本 z_i。

2. 设 $t = |\{i : T_i = 1\}|$ 为测试轮次的数量。验证者计算 s

$$s = \frac{1}{t} \sum_{i:T_i=1} p_C(z_i). \tag{166}$$

   如果 $s \geq (1+\delta)/N$，则验证者接受，并将$(z_1, \ldots, z_m)$输出至抗量子随机性提取器。

图2：执行理想测量的设备所用的熵累积协议。

We denote the output state $\psi = \mathbb{E}_{C\sim\text{Haar}(N)}\big[|C\rangle\langle C| \otimes \psi^C\big]$, and

$$H(D|CE)_\psi := \mathop{\mathbb{E}}_{C\sim\text{Haar}(N)}\big[H(D|E)_{\psi^C}\big]. \tag{165}$$

下面的推论总结了我们对这一理想情形的单轮分析 .

推论 6.5。 设 $\mathcal{A}$ 是执行理想测量、能够解决$(1+\delta)$-XHOG 的任意设备，ψ 是其输出。那么 $H(D|CE)_\psi \geq (\delta - 0.01)n - o(1)$。

证明。 根据定义及 定理 6.4， $H(D|CE)_\psi \geq (\delta - 0.01)n - O(N^{-0.02})$。 □

6.2 熵累积

我们提出一种熵累积协议，适用于任何在图2中执行理想测量的设备。请注意，由于冯·诺依曼熵下界几乎对所有 C都成立，验证者可以在每一轮重复使用该电路。

定理6.6。 设 $\mathcal{A}_1, \ldots, \mathcal{A}_m$ 是可访问双部态 ρ_{DE} 的第一系统、并输出 $z_1,\ldots,z_m$ 的 $n^{O(1)}$-查询序贯过程，它们以概率 p解决$\text{LXEB}_{1+\delta,m}$。那么，对 C的取值，以概率 $1 - 2^{-\Omega(n)}$，

$$H^\varepsilon_{\min}(Z^m|E)_{\mathcal{A}_m\circ\ldots\mathcal{A}_1(\rho)|\Omega} \geq n\big((\delta - 0.01)m - c\sqrt{m} - o(1)\big) \tag{167}$$

其中，Ω 表示输出 $z_1,\ldots,z_m$ 解决 $\text{LXEB}_{1+\delta,\ m}$，即：

$$\Omega := \left\{(z_1, \ldots, z_m) : \frac{1}{m}\sum_{i=1}^m P(z) \geq \frac{1+\delta}{N}\right\}. \tag{168}$$

参数 $c :\ = 4.01\ (1 + \log(\frac{1}{p\varepsilon}))^{1/2}$。

证明。我们应用第4节中给出的熵累积定理。特别地，我们选择 $G := N\sum_z |z\rangle\langle z| P(z)$。根据推论 6.5，我们选择 $f(\delta) = (\delta - 0.01)n - o(1)$。由此得到 $\|\nabla f\|_\infty = n$。接着有 $V = 2(\log(2d_Z + 1) + \|\nabla f\|_\infty) = 2(\log(2N + 1) + n) = 4n + O(1/N) \leq 4.01n$。现在我们有

$$H_{\min}^{\varepsilon}(Z^m|E)_{\mathcal{A}_m\circ\ldots\circ\mathcal{A}_1(\rho)|\Omega} \geq n\left((\delta - 0.01)m - o(1/n) - 4.01\sqrt{m}\sqrt{\log\frac{2}{\Pr_\sigma[\Omega]^2\varepsilon^2}}\right). \tag{169}$$

□

附带说明，同样的分析第6.1节和第6.2节也适用于傅里叶采样电路，即 C 描述了（126）中在随机 n位布尔函数f下的酉变换。在这种情况下，理想设备可以解决 b-XHOG 问题（当 $b \approx 3$ [39] 时），而任何能够解决（$1 + 2\delta$）-XHOG的设备，其条件冯·诺依曼熵都有下界$\Omega(\delta n)$。应用熵累积定理，一个 m轮协议还会累积$\Omega(\delta mn)$ 条件最小熵。

第第6节中的分析旨在说明，在简化设置下为何可以使用 LXEB 来生成随机性。具体而言，对于熵累积，信道 $\mathcal{A}_1$、……、 $\mathcal{A}_m$是 C的理想酉信道，因此这一设置距离完全设备无关性还很远。在下一节中，我们将分析完全通用的设备，此时信道 $\mathcal{A}_1$、……、 $\mathcal{A}_m$ 不一定是理想的。

7 一个完全一般的设备

在本区段中，我们对一般设备进行分析。在证明主要结果之前，我们先提供一些直观说明。设 ρ_{DE} 是设备与 Eve 共享的纠缠态，$\mathcal{A}^C(\rho_{DE})$ 是设备在能够访问第一个子系统 D 和电路 C 的情况下执行的量子算法。不失一般性， $\mathcal{A}^C(\rho_{DE})$ 的输出为形式为 $\sum_z p(z)|z\rangle\langle z|_{D'} \otimes \xi_E(z)$ 的经典-量子态（这也意味着 $\mathcal{A}^C$ 是一个类型为 $D \to D'$、作用于希尔伯特空间 D 和 D' 的量子信道），其中对应的是归一化量子态 $\xi_E(z)$。经典部分，即随机变量 z，会发送给验证者；量子信息 $\xi_E(z)$ 则可用作下一轮交互的输入。在一个 m 轮协议中，设备与验证者重复进行 m 次消息交换，而验证者会输出一个判定位，指示接受或中止。如果验证者接受，设备的输出便会输入抗量子随机性提取器。

我们考虑任意一个获得 C 预言机访问的设备，并证明：如果该设备通过 LXEB$_{b,\ k}$，则其输出必然具有最小熵下界。首先，利用 Haar 随机酉矩阵的旋转不变性，我们形式化定义一种输入模型，其中设备获得以下访问权限：验证者对电路 $C \sim$Haar(N) 和两个酉算子 V、W 进行采样。第一个酉算子 V 是形如 $\sum_z e^{i\theta_z}|z\rangle\langle z|$ 的随机相位酉，其中每个 θ_z 都独立地从 $[0, 2\pi$ 上的均匀分布中采样。第二个酉算子 W 是子空间$\{|x\rangle$ 上的 Haar 随机酉矩阵： $x \in \{0,1\}^n \backslash \{0^n\}\}$。随后，设备获得对 $C' = VCW$ 的预言机访问；根据定义，显然有 $p_C = p_{C'}$，其中 $p_C(z) := |\langle z|C|0\rangle|^2$ 是 p_C 的密度。此外， C 和 C' 具有相同的分布（依据 Haar 测度）。如果一个高效设备能够在其系统 D 的任意大小相同的子集上应用 C'，我们就称该设备获得了对 C 的预言机访问。

对称化使我们能够分析冯·诺依曼熵下界。具体而言，我们证明，在此查询模型中，关于 C 的条件冯·诺依曼熵等于关于 p_C 的冯·诺依曼熵。由于 C 分布在一个无限集合上，我们定义冯·诺依曼熵$H(Z|CE)_\psi := \mathbb{E}_C\left[H(Z|E)_{\psi^C}\right]$，其中 ψ^C 是设备 $\mathcal{A}$ 在 $\mathcal{A}$ 获得对 C 的访问权限时输出的经典-量子态。在下文中，我们使用大写的 P_C 来强调

该分布是概率单纯形上的复值随机变量向量。具体而言，对于 $C \sim \mathrm{Haar}(N)$， P_C按照狄利克雷分布 $\mathrm{Dir}(1^N)$ 进行分布（详见区段 3.4 ）。

定理 7.1。 对于 *Haar* 随机的 C，以及任意设备 $\mathcal{A}$：该设备以双部态 ρ_{DE} 的第一系统为输入，并在获得对 C 的预言机访问后输出经典-量子态 ψ 。于是 $H(Z|CE)_\psi = H(Z|P_C E)_\psi$，其中 $P_C(z)$: $= |\langle z|C|0^n\rangle|^2$服从狄利克雷分布 狄利克雷分布$(1^N)$.

证明。 对于任意分布 P，我们令 S_P 表示满足 $P_C = P$ 的酉算子集合。对于每个 P，令 C_P 表示集合 S_P 中的一个代表元。于是，对于 $C \in S_P$，存在一个对角酉算子V'和一个作用于子空间 $\mathrm{span}\{|x\rangle : x \neq 0^n\}$ 上的酉算子 W'，使得 $C = V' C_P W'$。这意味着可以用一次对 C_P 的查询来模拟一次对 $C \in S_P$ 的查询。更具体地，对于 $C \in S_P$，我们记 $\sigma^P = \psi^C = \psi^{C_P}$。这意味着 $H(Z|E)_{\psi^C} = H(Z|E)_{\sigma^P}$。根据条件冯·诺依曼熵的定义，以及 p_C 服从分布 $\mathrm{Dir}(1^N)$ 这一事实， $H(Z|CE)_\psi = \mathbb{E}_{P\sim \text{狄利克雷分布}(1^N)}[H(Z|E)_{\sigma^P}] = H(Z|PE)_\psi$。 □

我们的分析分为以下几个步骤。首先，我们证明，对于每个 T-查询 $\mathcal{A}$ 和 ρ_{DE}，都存在另一个量子算法 $\mathcal{B}$，它在输入 ρ_{DE} 的第一系统 D 以及根据 P_C 为 Haar 随机 C 独立同分布抽取的随机变量 k 、 z_1、 ...、 z_k时，满足

$$\left\| \mathop{\mathbb{E}}_{C} \mathcal{A}^C(\rho_{DE}) - \mathop{\mathbb{E}}_{C, z_1, \ldots, z_k \sim P_C} \mathcal{B}(\rho_{DE}, z_1, \ldots, z_k) \right\|_{\mathrm{tr}} \leq 2^{-\Omega(n)}, \tag{170}$$

对于 $k = T^2 \cdot 2^{-\Omega(n)}$。因此，不失一般性，我们可以考虑 $\mathcal{B}$ 的行为 .

接下来，我们证明，利用输出 $z \in \{z_1, \ldots, z_k\}$ 的概率，可以轻松计算 $\mathcal{B}$ 的得分。更具体地说，我们证明， $\mathcal{B}$ 的得分与 $\frac{1}{N+k} \cdot (1 + \Pr[z \in \{z_1, \ldots, z_k\}])$ 相差可忽略不计。因此，当 $\mathcal{B}$ 的得分为 $\frac{1+\delta}{N+k}$ 时，设备和窃听者可能会协调配合，使得使用 ρ_{DE} 时的条件冯·诺依曼熵以与 δ 相差可忽略不计的概率达到某个值；否则，由于窃听者不了解 z_1、.....、 z_k 的信息，且每个 z_i 都是从 P_C 中抽取的，条件冯 · 诺依曼熵可以由 P_C 的最小熵界定。接着，由于以压倒性概率，对 C， P_C 的最小熵为 $n - \log\ n - O(1)$，因此，当 $\mathcal{A}$ 在“典型”的 C 上赢得该协议时，其输出必定具有较高的条件冯·诺依曼熵。

7.1 通过样本访问模拟 Haar 随机酉矩阵

在本区段中，我们证明，对于 T 次查询的 $T = 2^{O(n)}$ 算法，若其解决了 $\delta n - o(n)$-XHOG 问题，则它输出的经典-量子态的条件冯·诺依曼熵为 $\delta n - o(n)$。我们证明，可以使用样本访问算法来模拟预言机访问算法。为此，我们借鉴了 Ambainis、Rosmanis 和 Unruh [9] 以及 Kretschmer [39]的思想。

7.1.1 从电路预言机到态制备预言机

对于量子态 $|\psi\rangle$，令 C^ψ 为一个随机酉算子，使得 $C^\psi|0\rangle = |\psi\rangle$ ，且其在与 $|0\rangle$正交的子空间上是 Haar 随机的；令 $\mathcal{O}^\psi$ 为关于 $|\psi_\perp\rangle = \frac{|\psi\rangle - |\perp\rangle}{\sqrt{2}}$的反射，也就是说，它将 $|\psi\rangle \mapsto |\perp\rangle$变为 $|\perp\rangle \mapsto |\psi\rangle$ ，并且对与 $\mathrm{span}\{|\psi\rangle, |\perp\rangle\}$中的量子态正交的量子态作用平凡。

第一步是证明，对于每个 $|\psi\rangle$，给定对 C^ψ的访问权限时，可以使用给定对 $\mathcal{O}^\psi$ 访问权限的 $O(T)$ 次查询算法来近似任意 T 次查询算法。我们证明以下定理，并改进了 [39, 定理 19]中的常数因子。

定理 7.2 (参见 [39, 定理 19])。对于每个量子态 $|\psi\rangle$，每个 T 次查询算法 $\mathcal{A}^{C^\psi}$都可以由一个 ($2T$) 次查询量子算法 $\mathcal{B}^{\mathcal{O}^\psi}$ 近似，使得

$$\left\| \mathcal{B}^{\mathcal{O}^\psi} - \mathop{\mathbb{E}}_{C^\psi} [\mathcal{A}^{C^\psi}] \right\|_\diamond \leq \frac{4T}{2^{n/2}}. \tag{171}$$

证明。只需给出一种使用对 $\mathcal{O}^\psi$ 的预言机访问来模拟 C^ψ 的方法。Kretschmer [39] 的关键想法是：如果我们能够访问 $\mathcal{O}^{\psi^\perp}$，其中 $|\psi^\perp\rangle$ 是任意一个与 $|\psi\rangle$ 正交的量子态，并且能够使用任意酉算子 $V^{\psi^\perp}|0\rangle = |\psi^\perp\rangle$ 制备 $|\psi^\perp\rangle$，那么

$$|0^n\rangle \xmapsto{V^{\psi^\perp}} |\psi^\perp\rangle \xmapsto{\mathcal{O}^\psi} |\psi^\perp\rangle \xmapsto{\mathcal{O}^{\psi^\perp}} |\perp\rangle \xmapsto{\mathcal{O}^\psi} |\psi\rangle. \tag{172}$$

接下来，我们考虑另一个酉算子 $W = |0\rangle\langle 0| \oplus C'$，其中 C' 是希尔伯特空间 $\mathrm{span}\{|x\rangle$ 上的 Haar 随机酉矩阵：$x \neq 0\}$。酉算子的序列

$$|0^n\rangle \xmapsto{W} |0\rangle \xmapsto{V^{\psi^\perp}} |\psi^\perp\rangle \xmapsto{\mathcal{O}^\psi} |\psi^\perp\rangle \xmapsto{\mathcal{O}^{\psi^\perp}} |\perp\rangle \xmapsto{\mathcal{O}^\psi} |\psi\rangle, \tag{173}$$

$$|x\rangle \xmapsto{\mathcal{O}^\psi \mathcal{O}^{\psi^\perp} \mathcal{O}^\psi V^{\psi^\perp} W} |\psi_x\rangle, \qquad x \neq 0, \tag{174}$$

满足 $|\psi_x\rangle$ 的条件，即它是在由与 $|\psi\rangle$ 正交的量子态（当然也包括 $|\perp\rangle$）张成的空间上取 Haar 随机酉矩阵。令 $C^\psi := \mathcal{O}^\psi \mathcal{O}^{\psi^\perp} \mathcal{O}^\psi V^{\psi^\perp} W$，即可满足所有要求。

然而，由于我们不知道 $|\psi\rangle$，因此无法访问 $|\psi^\perp\rangle$、$V^{\psi^\perp}$ 和 $\mathcal{O}^{\psi^\perp}$，所以上述映射可能无法实现（除非对 $\mathcal{O}^\psi$ 进行大量查询）。相反，若我们采样一个 Haar 随机态 $|\varphi\rangle$，则 $\Pr_{|\varphi\rangle}[|\langle\varphi|\psi\rangle| \geq \gamma] \leq e^{-n\gamma^2}$；因此，它们以高概率近乎正交。根据这一观察，我们可以采样一个 Haar 随机态 $|\varphi\rangle$，并在模拟 C^ψ 时用 $|\varphi\rangle$ 代替 $|\psi^\perp\rangle$。由于量子态 $|\varphi\rangle$ 是均匀采样得到的，而非固定的量子态，因此我们必须考虑量子信道

$$\Phi^\psi(\rho) := \mathop{\mathbb{E}}_{|\varphi\rangle} \left[\mathcal{O}^\psi \mathcal{O}^\varphi \mathcal{O}^\psi V^\varphi \rho (\mathcal{O}^\psi \mathcal{O}^\varphi \mathcal{O}^\psi V^\varphi)^\dagger \right]. \tag{175}$$

并证明 Φ^ψ 接近于 $\mathcal{C}^\psi(\rho) := C^\psi \rho (C^\psi)^\dagger$（按菱形范数计）。

Let $\mathcal{V}^\varphi$ 是 V^φ的酉信道。根据三角不等式，为证明二者接近，

$$\|\Phi^\psi - \mathcal{C}^\psi\|_\diamond \leq \left\| \mathop{\mathbb{E}}_{|\varphi\rangle} \mathcal{V}^\varphi - \mathcal{V}^{\psi^\perp} \right\|_\diamond + \left\| \mathop{\mathbb{E}}_{|\varphi\rangle} \mathcal{O}^\varphi - \mathcal{O}^{\psi^\perp} \right\|_\diamond. \tag{176}$$

由于所有量子态 $|\psi^\perp\rangle$在模拟方面的表现都同样出色（也就是说，每个 $|\psi^\perp\rangle$与$|\psi\rangle$ 正交的量子态都可以用来精确模拟 C^ψ），在(176) 中，我们选择的 $|\psi^\perp\rangle$ 实际上可以依赖于 $|\varphi\rangle$。更明确地说，我们将 $|\psi^\perp\rangle \in \mathrm{span}\{|\psi\rangle, |\varphi\rangle\}$ 定义为与 $|\psi\rangle$ 正交的唯一量子态（相位除外）。在这种情况下，菱形范数 $\|\mathcal{V}^\varphi - \mathcal{V}^{\psi^\perp}\|_\diamond \leq 2|\langle\psi|\varphi\rangle|$。由于 $\mathcal{O}^\varphi \mathcal{O}^{\psi^\perp}$ 是角度为 2α 的旋转，其中 $\alpha = \arccos(\cos^2(\theta/2))$，特征值为 $e^{i2\alpha}$，$e^{-i2\alpha}$，1，并且

$$\begin{aligned} \|\mathcal{O}^\varphi - \mathcal{O}^{\psi^\perp}\|_\diamond &\leq 2\sin\alpha \\ &= 2\sqrt{1 - \cos^4(\theta/2)} \\ &= 2\sqrt{1 - \left(\frac{1 + \sqrt{1 - |\varepsilon|^2}}{2}\right)^2} \\ &\leq 2|\varepsilon|, \end{aligned} \tag{177}$$

其中 $\varepsilon = \langle\varphi|\psi\rangle$。式(177) 中的最后一个等号成立，因为 $\sqrt{1-x^2} \le 1$ 对于 $x \in [0,1]$成立。根据(176) 以及混合论证，

$$\begin{aligned}\|\Phi^{\psi} - \mathcal{C}^{\psi}\|_{\diamond} &\le 4 \mathop{\mathbb{E}}_{|\varphi\rangle}[|\langle\psi|\varphi\rangle|] \\ &\le 4 \mathop{\mathbb{E}}_{|\varphi\rangle}[|\langle\varphi|\psi\rangle|^2]^{1/2} \\ &= \frac{4}{2^{n/2}}. \end{aligned} \tag{178}$$

现在令 $\mathcal{A}^{C^{\psi}}$ 为一个可访问 C^{ψ} 和 $\mathcal{B}^{\mathcal{O}^{\psi}} = \mathcal{A}^{\Phi^{\psi}}$的量子算法。根据三角不等式和 (178)，$\|\mathcal{A}^{C^{\psi}} - \mathcal{B}^{\mathcal{O}^{\psi}}\|_{\diamond} \le \frac{4T}{2^{n/2}}$。此外，由 (175)可知，$\mathcal{B}^{\mathcal{O}^{\psi}}$进行了 $2T$次对 $\mathcal{O}^{\psi}$的查询。 □

在上述分析中，注意到 $|\perp\rangle$ 的定义并不唯一：任何与 $\mathrm{span}\{|z\rangle : z \in \{0,1\}^n\}$ 正交的量子态 $|\perp\rangle$都可以使用。特别地，我们可以将 $|\perp\rangle$ 替换为 $e^{i\theta}|\perp\rangle$，分析仍然成立。令 $\mathcal{O}_{\theta}^{\psi}$ 为一个映射 $e^{i\theta}|\perp\rangle \mapsto |\psi\rangle$，$|\psi\rangle \mapsto e^{i\theta}|\perp\rangle$，并且对与 $|\psi\rangle$ 和 $|\perp\rangle$正交的量子态起恒等作用。这一观察得出以下推论。

推论 7.3。令 $|\perp\rangle$ 为一个与 张成空间$\{|z\rangle : z \in \{0,1\}^n\}$正交的固定量子态。对于 $\theta \in [0, 2\pi)$，每个量子态 $|\psi\rangle$ 以及每个 T-查询算法 $\mathcal{A}^{C^{\psi}}$，都存在一个 $(2T)$-查询算法 $\mathcal{B}$，使得

$$\left\| \mathcal{B}^{\mathcal{O}_{\theta}^{\psi}} - \mathop{\mathbb{E}}_{C^{\psi}}[\mathcal{A}^{C^{\psi}}] \right\|_{\diamond} \le \frac{4T}{2^{n/2}}. \tag{179}$$

7.1.2 从规范态制备预言机到资源态

在本节中，我们运用 Ambainis、Rosmanis 和 Unruh 的思路[9] 来证明：给定依赖于 Haar 随机态的资源态，就可以近似任何能够访问规范态制备预言机的算法。

定理 7.4 ([9,定理 3], 的改述)。**令 为一个量子态，为关于 ($|\psi\rangle - |\perp\rangle$) 的反射。**令 $\mathcal{O}$ 为一个预言机，ρ 为一个量子态。令 $|R^{\psi}\rangle = |\psi^{\ell}\rangle \otimes |\alpha_1^{\psi}\rangle \otimes \ldots \otimes |\alpha_m^{\psi}\rangle$，其中 $|\alpha_i^{\psi}\rangle = \cos(\frac{i\pi}{2k})|\psi\rangle + \sin(\frac{i\pi}{2m})|\perp\rangle$。对于任意量子态 ρ和算法 $\mathcal{B}$，若其输入为 ρ且对 $\mathcal{O}^{\psi}$进行 T 次查询，则存在一个算法 $\mathcal{G}$，其输入为 ρ，$|R\rangle$，并且对 $\mathcal{O}$ 进行的查询次数与 $\mathcal{B}$ 相同，使得

$$\|\mathcal{B}^{\mathcal{O}^{\psi},\mathcal{O}}(\rho) - \mathcal{G}^{\mathcal{O}}(\rho, |R^{\psi}\rangle)\|_{\mathrm{tr}} \le O\left(T\left(\frac{1}{\sqrt{m}} + \frac{1}{\sqrt{\ell}}\right)\right). \tag{180}$$

此外，*(180)* 当 $|\psi\rangle$、$\mathcal{O}$ 和 ρ不相互独立时也成立。

详细证明请参见[9]。这里我们提供一些直观解释。令 S 为左循环移位算子，且 $|\tilde{R}^{\psi}\rangle = |\alpha_1^{\psi}\rangle \otimes \ldots \otimes |\alpha_m^{\psi}\rangle$ S $|\perp\rangle|\tilde{R}^{\psi}\rangle$ $S|\perp\rangle|\tilde{R}^{\psi}\rangle =$。对其应用一次会得到，因为保真度 $|\tilde{R}^{\psi}\rangle|\perp\rangle \approx |\psi\rangle|\tilde{R}^{\psi}\rangle$

$$|\langle\psi, \tilde{R}^{\psi}|S|\perp, \tilde{R}^{\psi}\rangle|^2 = \cos\left(\frac{\pi}{2k}\right)^k \ge \left(1 - \frac{\pi^2}{4k^2}\right)^k \ge 1 - \frac{\pi^2}{4k} \tag{181}$$

这意味着迹距离为 $O(k^{-1/2})$。此外，利用满足 $k \to \infty$ 的理想资源态，可以借助控制-S产生关于 $\frac{1}{\sqrt{2}}(|\psi\rangle - |\perp\rangle)$ 的反射，前提是关于 $|\psi\rangle$ 的反射 R

可以实现。由于 $|\psi\rangle$ 未知，因此不知道如何精确实现 R。然而，利用 $|\psi\rangle$ 的 ℓ 份副本，我们可以将 R 近似到菱形距离 $O(\ell^{-1/2})$：令 V 为在置换下不变的 $(\ell+1)$-体量子态空间，令 M 为投影到 V 上的投影。对于满足 $|T\rangle = |\psi\rangle^{\otimes \ell}$ 的 $|\Phi\rangle = |\phi\rangle|T\rangle$，若 $|\phi\rangle = |\psi\rangle$，则 $\langle\Phi|M|\Phi\rangle = 1$；对于与 $|\psi\rangle$正交的 $|\phi\rangle$，则有 $\langle\Phi|M|\Phi\rangle \leq O(1/\ell)$。因此，反射 $\mathbb{I} - 2M$ 将 R 近似到菱形距离 $O(1/\sqrt{\ell})$，而测量后，量子态会受到扰动，其迹距离为 $O(\ell^{-1/2})$。最后，由于共有 T 次查询，根据混合论证，总体菱形距离为 $O(T(m^{-1/2} + \ell^{-1/2}))$。

对于每个量子态 $|\psi\rangle$，令量子态 $|R_\theta^\psi\rangle$ 与 $|R^\psi\rangle$ 相同，只是将 $|\perp\rangle$ 替换为$e^{i\theta}|\perp\rangle$，即

$$|R_\theta^\psi\rangle := |\psi^\ell\rangle \otimes \bigotimes_{i=1}^{k} \left(\cos\left(\frac{i\pi}{2m}\right)|\psi\rangle + \sin\left(\frac{i\pi}{2m}\right)e^{i\theta}|\perp\rangle\right) \tag{182}$$

由于定理 7.4 在将每个 $|\perp\rangle$ 替换为 $e^{i\theta}|\perp\rangle$后仍成立，因此有以下推论：

推论 7.5。设 $|\psi\rangle$ 是一个量子态，$\mathcal{O}_\theta^\psi$ 是关于 $\frac{1}{\sqrt{2}}(|\psi\rangle - e^{i\theta}|\perp\rangle)$ 的反射。设 $\mathcal{O}$ 是一个预言机，ρ 是一个量子态。设 $|R_\theta^\psi\rangle$ 如 (182) 中所定义。对于 $\theta \in [0, 2\pi)$、量子态 ρ 以及任何在输入 ρ 时对 $\mathcal{O}_\theta^\psi$ 进行 T 次查询的算法 $\mathcal{B}$，存在一个算法$\mathcal{G}$，它在输入 ρ 时，$|R_\theta^\psi\rangle$ 对 $\mathcal{O}$ 进行与 $\mathcal{B}$ 相同次数的查询，使得

$$\|\mathcal{B}^{\mathcal{O}_\theta^\psi,\mathcal{O}}(\rho) - \mathcal{G}^{\mathcal{O}}(\rho, |R_\theta^\psi\rangle)\|_{\mathrm{tr}} \leq O\left(T\left(\frac{1}{\sqrt{m}} + \frac{1}{\sqrt{\ell}}\right)\right). \tag{183}$$

此外，(183) 当 $|\psi\rangle$、$\mathcal{O}$ 和 ρ不独立时仍成立。

结合推论 7.3 和推论 7.5，可得以下推论。

推论 7.6。对于量子态 $|\psi\rangle$ 以及每个对 C^ψ进行 T 次查询的量子算法 $\mathcal{A}$，存在一个量子算法 $\mathcal{G}$，它可以访问 $|R_\theta^\psi\rangle$，并且对于均匀分布的 $\theta \in [0, 2\pi)$ 满足

$$\left\| \mathop{\mathbb{E}}_{C^\psi}\left[\mathcal{A}^{C^\psi}\right] - \mathcal{G}\left(\mathop{\mathbb{E}}_{\theta}[|R_\theta^\psi\rangle\langle R_\theta^\psi|]\right)\right\|_\diamond \leq O(Tk^{-1/2}) + \frac{4T}{N^{1/2}}. \tag{184}$$

证明。根据 推论 7.3，对于每个 $\theta \in [0, 2\pi)$ 和 T 次查询算法 $\mathcal{A}^{C^\psi}$，都存在 $\mathcal{B}^{\mathcal{O}_\theta^\psi}$，使得它们的菱形距离至多为 $4TN^{-1/2}$。根据 推论 7.5，对于每个 $\theta \in [0, 2\pi)$ 和 T 次查询算法 $\mathcal{B}^{\mathcal{O}_\theta^\psi}$，都存在 $\mathcal{G}(|R_\theta^\psi\rangle)$，使得它们的菱形距离至多为 $O(Tm^{-1/2})$（我们令 $m = \ell = k/2$ 以简化表达式）。

根据三角不等式，

$$\begin{aligned}\left\| \mathop{\mathbb{E}}_{C^\psi}\left[\mathcal{A}^{C^\psi}\right] - \mathop{\mathbb{E}}_{\theta}[\mathcal{G}(|R_\theta^\psi\rangle\langle R_\theta^\psi|)]\right\|_\diamond &\leq \mathop{\mathbb{E}}_{\theta}\left\| \mathop{\mathbb{E}}_{C^\psi}\left[\mathcal{A}^{C^\psi}\right] - \mathcal{B}^{\mathcal{O}_\theta^\psi}\right\|_\diamond + \mathop{\mathbb{E}}_{\theta}\left\|\mathcal{B}^{\mathcal{O}_\theta^\psi} - \mathcal{G}(|R^\theta\rangle\langle R^\theta|)\right\|_\diamond \\ &\leq O(Tk^{-1/2}) + \frac{4T}{N^{1/2}}.\end{aligned} \tag{185}$$

根据量子操作的线性性，$\mathbb{E}_\theta\left[\mathcal{G}\left(|R_\theta^\psi\rangle\langle R_\theta^\psi|\right)\right] = \mathcal{G}\left(\mathbb{E}_\theta\left[|R_\theta^\psi\rangle\langle R_\theta^\psi|\right]\right)$。

□

7.1.3 从资源态到样本

现在我们从资源态转向样本。对于随机的 $|\psi\rangle$，我们将量子态写作

$$|\psi\rangle = (\sqrt{P_0}e^{i\Theta_0}, \ldots, \sqrt{P_{N-1}}e^{i\Theta_{N-1}}), \tag{186}$$

其中，$P = (P_0, \ldots, P_{N-1})$ ～服从狄利克雷分布 $\mathrm{Dir}(1^N)$，且 $\Theta = (\Theta_0, \ldots, \Theta_{N-1})$ 的每个分量 Θ_i 都是相互独立的随机相位；也就是说，每个 Θ_i 都根据 $[0, 2\pi$ 上的均匀分布进行采样。对于每个分布 P，我们记 $|P\rangle := (\sqrt{P_0}, \ldots, \sqrt{P_{N-1}})$，并记 $|\psi^P\rangle = W|P\rangle$ 为随机对角相位矩阵 $W = \mathrm{diag}(W_0, \ldots, W_{N-1}) := e^{i\mathrm{diag}(\Theta)}$。对于每个 $|\psi\rangle$，令 $|R^{P,W}_{\theta}\rangle$ 为相应的资源态。写成矩阵形式，

$$|R^{P,W}_{\theta}\rangle = |\psi^{P,W}\rangle^{\otimes \ell} \otimes \bigotimes_{j=1}^{m} |\alpha^{P,W}_{i,\theta}\rangle, \tag{187}$$

其中 $|\alpha^{P,W}_{i,\theta}\rangle := \cos(\frac{\pi i}{2k})|\psi^{P,W}\rangle + \sin(\frac{\pi i}{2k})e^{i\theta}|\perp\rangle$。

令 $\tilde{W} = W + e^{i\theta}|\perp\rangle\langle\perp|$。量子态 $|R^{P,W}_{\theta}\rangle$ 可以写成

$$|R^{P,\tilde{W}}\rangle := |R^{P,W}_{\theta}\rangle = (\tilde{W}|P\rangle)^{\otimes \ell} \otimes \bigotimes_{j=1}^{k} (\tilde{W}|P_i\rangle) \tag{188}$$

我们将使用以下引理，出自 [39]。

Le引理 7.7 ([39,引理 15], 改述版)。存在一个算法，可以制备 s

$$\sigma^P := \mathop{\mathbb{E}}_{\tilde{W}} \left[|R^{P,W}\rangle\langle R^{P,W}| \right] \tag{189}$$

通过在标准基下测量 $|\psi\rangle$ 的$(k+\ell)$ 个副本。

令 C^P 为如下随机电路：令 $V|0\rangle = (\sqrt{P_0}, \ldots, \sqrt{P_{N-1}})$，$C'$ 为 $\mathrm{span}\{|z\rangle$ 上的 Haar 随机矩阵：$z \in \{1, \ldots, N-1\}\}$，并且对于随机对角相位矩阵 W，有 $C^P = WVC'$。接下来我们证明以下定理。

定理 7.8。对于每个分布 P，令 C^P 为从上述过程采样得到的随机电路。对于每个对 C^P 进行 T 次查询的算法 $\mathcal{A}$，存在一个量子算法 $\mathcal{F}$，它可以访问从 P 中抽取的k 个样本，使得

$$\left\| \bar{\mathcal{A}}^P - \bar{\mathcal{F}}^P \right\|_{\diamond} \leq O(Tk^{-1/2}) + \frac{4T}{N^{1/2}}, \tag{190}$$

其中 $\bar{\mathcal{A}}^P := \mathbb{E}_{C^P}[\mathcal{A}^{C^P}]$ 以及 $\bar{\mathcal{F}}^P := \mathbb{E}_{z_1,\ldots,z_k \sim P} \mathcal{F}(z_1, \ldots, z_k)$。

证明。令 $|\psi^P\rangle = \tilde{W}|P\rangle$ 为作用于 $\mathrm{span}\{|0\rangle, \ldots, |N-1\rangle, |\perp\rangle\}$ 上的随机相位矩阵 $\tilde{W}$。该量子信道

$$\mathop{\mathbb{E}}_{C^P}\left[\mathcal{A}^{C^P}\right] = \mathop{\mathbb{E}}_{\tilde{W}, C^{\psi}}\left[\mathcal{A}^{C^{\psi}}\right]. \tag{191}$$

设引理 7.7 中的量子过程为 Φ，该过程

$$\begin{aligned} \mathop{\mathbb{E}}_{\tilde{W}}\left[\mathcal{G}(|R^{P,\tilde{W}}\rangle\langle R^{P,\tilde{W}}|)\right] &= \mathcal{G}\left(\mathop{\mathbb{E}}_{\tilde{W}} |R^{P,\tilde{W}}\rangle\langle R^{P,\tilde{W}}|\right) \\ &= \mathcal{G}(\sigma^P) = \mathop{\mathbb{E}}_{z_1,\ldots,z_k \sim P} \mathcal{G} \circ \Phi(z_1, \ldots, z_k). \end{aligned} \tag{192}$$

输入：安全参数 n和样本数 k。协议：

1. Eve 和设备 $\mathcal{F}$ 共享一个任意纠缠态 ρ_{DE}。

2. 验证者从分布 $P \sim \mathrm{Dir}(1^N)$（其中 $N = 2^n$）中抽样，并抽取 $z_1, \ldots, z_k \sim P$，然后将其发送给设备 $\mathcal{F}$（但不发送给 Eve）。此外， P 可以透露给 Eve（但不透露给设备）。 3. 设备发送一个字符串 z。 4. 若 $z \in \{z_1, \ldots, z_k\}$，验证者则接受。

图 3：一个简化协议。

现在令 $\mathcal{F} = \mathcal{G} \circ \Phi$。根据三角不等式和 推论 7.6,

$$\begin{aligned}\left\| \mathop{\mathbb{E}}_{C^P}\left[\mathcal{A}^{C^P}\right] - \mathop{\mathbb{E}}_{z_1,\ldots,z_m\sim P} \mathcal{F}(z_1,\ldots,z_k) \right\|_\diamond &\leq \mathop{\mathbb{E}}_{W} \left\| \mathop{\mathbb{E}}_{C^\psi}\left[\mathcal{A}^{C^\psi}\right] - \mathcal{G}\left(\mathop{\mathbb{E}}_{\theta} |R_\theta^\psi\rangle\langle R_\theta^\psi|\right) \right\|_\diamond \\ &\leq O(Tk^{-1/2}) + \frac{4T}{N^{1/2}}. \end{aligned} \tag{193}$$

□

7.2 单轮分析

在本节中，我们证明第 7 节中的主要结果。我们证明，对于 Haar 随机 C，在选择 P_C 时，任意 T- 查询设备的输出相对于 Eve 所拥有信息的条件冯 · 诺依曼熵，以概率 $1 - N^{-\Omega(1)}$ 至少为 $\Omega(\delta n)$，前提是 $T = 2^{O(n)}$ 且该设备针对 b求解 $b \approx 1 + \delta$-XHOG。

首先，我们考虑一个简化设备 $\mathcal{F}$，它只能通过样本访问获得 P_C，并解决b-XHOG。我们证明，这个博弈等价于以下协议：验证者从分布 $P \sim \mathrm{Dir}(1^N)$ $z_1, \ldots, z_k \sim P$中抽样。验证者将 $z_1, \ldots, z_k$ 发送给设备。不失一般性，我们可以假设 P 会透露给 Eve，但不会透露所有样本。设备需要返回一个字符串 z，若 $z \in \{z_1, \ldots, z_k\}$，验证者便接受。回想一下，如果 C 是 Haar 随机的，那么 P_C 服从分布$\mathrm{Dir}(1^N)$。协议的详细说明见图 3。

简化协议等价于以如下意义解决XHOG： 如果设备解决了$(2 - \varepsilon')$-XHOG，那么在图 3 所述协议中，设备至少以 $1 - \varepsilon'$ 的概率 $\varepsilon' = \varepsilon + O(k^3/N)$被接受。接着，我们证明，对于图 3 中的任意设备，若其以概率 $1 - \varepsilon'$赢得协议，则条件冯·诺依曼熵至少为$(1 - \varepsilon')n - o(n)$。这意味着图 3 中的协议也能认证条件冯·诺依曼熵。

根据定理 7.8，任何 T查询算法 $\mathcal{A}$ 都可以由一个算法 $\mathcal{F}$ 很好地近似；该算法仅能通过样本访问来访问 P_C，且菱形距离为 $\delta = O(Tk^{-1/2})$。此外，我们还将证明，如果 $\mathcal{A}$ 解决了$(2 - \varepsilon)$-XHOG，那么 $\mathcal{F}$ 就能以 b'解决-XHOG。这些结果结合起来，便完成了我们的单轮分析。 $b' = 2 - \varepsilon - \delta$

7.2.1 简化装置

在本区段中，我们证明，对于任意一个 $\mathcal{F}$ 获得 k 个从 P抽取的样本的算法， $\mathcal{F}$ 若要取得高得分，唯一的办法就是输出给定样本之一。因此，图 3中的证明系统等价于求解XHOG。

首先，我们证明一个稍后会用到的技术引理。

引理 7.9. 对于 $P \sim$狄利克雷分布(1^N)和 $z_1, \ldots, z_k \sim P$，设 $m = (m_0, \ldots, m_{N-1})$ 为满足 $m_z = |\{i \in [k] : z_i = z\}|$ 的频数向量。那么 m 服从 $\Phi(N, k)$，即在频数向量上取均匀分布，且这些向量的 N 个元素之和为 k。

证明。 回顾一下，狄利克雷分布(1^N) 的概率密度函数（概率密度函数）为 $f(p) = \Gamma(N)$，其中 $p = (p_0, \ldots, p_{N-1})$ 是概率单纯形中的任意元素。给定一个概率分布 p， k 个样本构成频数向量 m 的概率密度为

$$f(m|p) = p_0^{m_0} \ldots p_{N-1}^{m_{N-1}} \frac{\Gamma(k+1)}{\Gamma(m_0+1)\ldots\Gamma(m_{N-1}+1)}. \tag{194}$$

由于后验分布是狄利克雷分布$(1^N + m)$，概率密度

$$f(p|m) = p_0^{m_0} \ldots p_{N-1}^{m_{N-1}} \frac{\Gamma(N+k)}{\Gamma(m_0+1)\ldots\Gamma(m_{N-1}+1)}. \tag{195}$$

因此， m 的概率密度为

$$f(m) = \frac{f(m|p)f(p)}{f(p|m)} = \frac{\Gamma(k+1)\Gamma(N)}{\Gamma(N+k)} = \binom{N+k-1}{k}^{-1}. \tag{196}$$

这意味着， m 服从频数向量上的均匀分布，这些频数向量有 N 个元素，且元素之和为 k。

□

以下定理表明，任何算法 $\mathcal{F}$ 在获得根据 P 抽取的 k 个独立样本后，若能解决$(2-\varepsilon \frac{N}{N+k})$-XHOG，$\mathcal{F}$ 则必须以至少 $1 - \varepsilon - O(k^3/N)$的概率输出一个给定样本。

定理 7。 **10.** 对于每个量子信道 $\mathcal{F}$，令 $\bar{\mathcal{F}}^P(\rho) := \mathbb{E}_{z_1,\ldots,z_k \sim P}[\mathcal{F}(\rho, z_1, \ldots, z_k)]$。$I$ f

$$\mathop{\mathbb{E}}_{P \sim \mathrm{Dir}(1^N)} \mathop{\mathbb{E}}_{z \sim \bar{\mathcal{F}}^P(\rho)} [P_z] \geq \frac{2-\varepsilon}{N+k}, \tag{197}$$

then

$$\Pr_{P \sim \mathrm{Dir}(1^N), z_1, \ldots, z_k \sim P} [\mathcal{F}(\rho, z_1, \ldots, z_k) \in \{z_1, \ldots, z_k\}] \geq 1 - \varepsilon - O\left(\frac{k^3}{N}\right). \tag{198}$$

证明。 对于每个样本元组$(z_1, \ldots, z_k)$，令 $m = (m_0, \ldots, m_{N-1})$为其频数向量。由于共有 k 个样本，$\|m\|_1 = k$。令 $\Phi(N, k)$为所有可能频数向量上的均匀分布。

抽样 $m \sim \Phi(N, k)$ 可以通过以下过程完成：从 $P \sim$狄利克雷分布 (1^N) 中抽取z_1，....., $z_k \sim P$；输出频数向量 m。根据引理 7.9，该频数向量的无穷

范数 1，即 $\max_z m_z = 1$，其概率为

$$\begin{aligned}\Pr_{m\sim\Phi(N,k)}[\|m\|_\infty = 1] &= \frac{\binom{N}{k}}{\binom{N+k-1}{k}} \\ &= \frac{N!(N-1)!}{(N-k)!(N+k-1)!} \\ &= \frac{(N-1)\dots(N-k+1)}{(N+k-1)\dots(N+1)} \\ &\geq \left(1-\frac{k}{N}\right)^{k-1} \\ &= 1-\frac{O(k^2)}{N}. \end{aligned} \tag{199}$$

第一个等式由引理7.9以及范数为1的频数向量的数量为 $\binom{N}{k}$这一事实得出。其余部分可直接计算得到。

对于每个能学习$(z_1,\dots,z_k)$的 $\mathcal{F}$，后验分布为 $P|m \sim$狄利克雷分布(1^N+m)。也就是说，看到这些样本后，从 P 到 $\mathcal{F}$ 的分布服从狄利克雷分布(1^N+m)。因此，期望

$$\begin{aligned}\mathop{\mathbb{E}}_{P\sim\mathrm{Dir}(1^N)}[P_z|m] &= \mathop{\mathbb{E}}_{P\sim\mathrm{Dir}(m+1^N)}[P_z] \\ &= \frac{m_z+1}{N+k}. \end{aligned} \tag{200}$$

不失一般性，任何算法 $\mathcal{F}(z_1,\dots,z_k,\rho)$的输出都可以用一个分布 $Q(m)$来描述，该分布仅取决于频数向量 m。对于每个 m，算法的得分为

$$\mathop{\mathbb{E}}_{z\sim Q(m)}\mathop{\mathbb{E}}_{P\sim\mathrm{Dir}(1^N+m)}[P_z] = \mathop{\mathbb{E}}_{z\sim Q(m)}\left[\frac{m_z+1}{N+k}\right]. \tag{201}$$

对于每个满足 $\|m\|_\infty = 1$的 m ，

$$\mathop{\mathbb{E}}_{z\sim Q(m)}\mathop{\mathbb{E}}_{P\sim\mathrm{Dir}(1^N+m)}[P_z] = \frac{1}{N+k}\left(1+\Pr_{z\sim Q(m)}[m_z>0]\right). \tag{202}$$

令 γ表示 $\|m\|_\infty > 1$ 对于 $m\sim\Phi(N,\ k)$的概率。由(199)，$\gamma = O(k^2/N)$。算法 $\mathcal{F}$ 的得分可用以下期望计算

$$\begin{aligned}&\mathop{\mathbb{E}}_{m\sim\Phi(N,k)}\mathop{\mathbb{E}}_{z\sim Q(m)}\mathop{\mathbb{E}}_{P\sim\mathrm{Dir}(1^N+m)}[P_z] \\ &\quad\leq (1-\gamma)\frac{1}{N+k}\left(1+\Pr_{m\sim\Phi(N,k),z\sim Q(m)}[m_z>0]\right)+\gamma\frac{k+1}{N+k} \\ &\quad\leq \frac{1}{N+k}+\frac{1}{N+k}\Pr_{m\sim\Phi(N,k),z\sim Q(m)}[m_z>0]+\frac{O(k^3)}{N(N+k)}. \end{aligned} \tag{203}$$

因此，如果得分至少为 $\frac{2-\varepsilon}{N+k}$，

$$\Pr_{m\sim\Phi(N,k),z\sim Q(m)}[m_z>0] \geq 1-\varepsilon-\frac{O(k^3)}{N}. \tag{204}$$

□

对于每个 P，如果 $\mathcal{F}$ 在 图 3 中的协议里输出给定样本之一，那么不难看出， $\mathcal{F}$ 的输出在给定 Eve 的侧信息的条件下，其冯·诺依曼熵至少为 $H_{\min}(P)$，仅有 $O(\log\ k)$ 的加性损失。我们证明，熵下界随 $\mathcal{F}$ 输出给定样本之一的概率线性增长。

定理 7.11。 对于分布 $Pover\ \{0,1\}^n$，设 $\mathcal{F}$是任意一个算法，它可以访问 $z_1,\ldots,z_k\sim_P$以及任意双部态 ρ_{DE}的第一个子系统和 $\mathcal{F}(\rho)=\mathbb{E}_{z_1,\ldots,z_k\sim P}[\mathcal{F}(\rho,z_1,\ldots,z_k)]$。如果

$$\Pr_{z_1,\ldots,z_k\sim P}[\mathcal{F}(\rho,z_1,\ldots,z_k)\in\{z_1,\ldots,z_k\}]=1-\delta, \tag{205}$$

then

$$H(Z|E)_{\bar{\mathcal{F}}(\rho)}\geq(1-\delta)(H_{\min}(P)-2\log k)-2. \tag{206}$$

证明。 我们给出随机变量 $Z\in\{Z_1,\ldots,Z_k\}$ 和 $Z_1,\ldots,Z_k\sim P$ 的冯·诺依曼熵 $H(Z|E)_{\bar{\mathcal{F}}^P(\rho)}$ 的一个下界。这里我们用大写字母 $Z_1,\ldots,Z_k$ 表示寄存器，或描述这些样本的随机变量；用小写字母 $z_1,\ldots,z_k$ 表示一个特定事件。我们定义经典-量子态

$$\psi_{Z_1\ldots Z_kZE}=\sum_{z_1,\ldots z_k}P(z_1)\ldots P(z_k)|z_1,\ldots,z_k\rangle\langle z_1,\ldots,z_k|_{Z_1\ldots Z_k}\otimes\mathcal{F}(\rho,z_1,\ldots,z_k)_{ZE}. \tag{207}$$

根据定义， $\bar{\mathcal{F}}^P(\rho)=\mathrm{tr}_{Z_1\ldots Z_k}(\psi)$，因此 $H(Z|E)_{\bar{\mathcal{F}}^P(\rho)}=H(Z|E)_\psi$。

应用引理3.9 于 $A=Z_1\ldots Z_k$， $B=Z$和 $C=E$，

$$H(Z|E)_\psi\geq H(Z_1\ldots Z_k|E)_\psi-H(Z_1\ldots Z_k|Z)_\psi. \tag{208}$$

由于寄存器 Z与 $Z_1\ldots Z_kE$不相交，

$$\mathrm{tr}_Z(\psi)=\sum_{z_1,\ldots,z_k}P(z_1)\ldots P(z_k)|z_1,\ldots,z_k\rangle\langle z_1,\ldots,z_k|_{Z_1\ldots Z_k}\otimes\rho_E, \tag{209}$$

这是一个乘积态。因此我们有 $H(Z_1\ldots Z_k|E)_\psi=H(Z_1\ldots Z_k)_\psi$，于是

$$\begin{aligned}H(Z|E)_\psi&\geq H(Z_1\ldots Z_k)_\psi-H(Z_1\ldots Z_k|Z)_\psi\\&=I(Z:Z_1,\ldots,Z_k)_\psi.\end{aligned} \tag{210}$$

这意味着，只需给 Z与 $Z_1,\ldots,Z_k$之间的互信息一个界。现在我们给出 $H(Z)_\psi$的下界：回忆一下，ψ 是如下形式的一个量子态

$$\psi=\sum_{z_1,\ldots,z_k}P(z_1)\ldots P(z_k)|z_1,\ldots,z_k\rangle\langle z_1,\ldots,z_k|\otimes\sum_zQ(z|z_1,\ldots,z_k)|z\rangle\langle z|, \tag{211}$$

对于某个条件分布 $Q(\cdot|z_1,\ldots,z_k)$，它可能依赖于 P。我们将每个分布分解为

$$Q(z|z_1,\ldots,z_k)=Q_1(z|z_1,\ldots,z_k)+Q_0(z|z_1,\ldots,z_k) \tag{212}$$

分成两个次归一化分布 $Q_1(\cdot|z_1、\ldots\ldots、z_k)$和 $Q_0(|z_1、\ldots\ldots、z_k)$，使得支撑集$\mathrm{supp}(Q_1(\cdot|z_1、\ldots\ldots、z_k)\subseteq\{z_1,\ldots,z_k\}$和 $\mathrm{supp}(Q_0(\cdot|z_1、\ldots\ldots、z_k))\cap\{z_1,\ldots,z_k\}=\emptyset$。令 $\delta_{z_1,\ldots,z_k}=$

$\sum_z Q_0(z|z_1、\ \ldots\ldots、\ z_k)$。根据定义，$\mathbb{E}_{z_1、\ \ldots\ldots、\ z_k\sim P}[\delta_{z_1,\ldots,z_k}] = \delta$。此外，对于 $b \in \{0,1\}$，令归一化分布

$$\bar{Q}_b(z|z_1,\ldots,z_k) = \frac{1}{p_{b,z_1,\ldots,z_k}} Q_b(z|z_1,\ldots,z_k), \tag{213}$$

其中 $p_{1,\ z_1,\ \ldots\ldots,\ z_k} = 1-\delta_{z_1,\ \ldots\ldots,\ z_k}$ 以及 $p_{0,\ z_1,\ \ldots\ldots,\ z_k} = \delta_{z_1,\ \ldots\ldots,\ z_k}$。现在令 $(p_0, p_1) = (\delta, 1-\delta)$。对于 $b \in \{0,1\}$，定义

$$\psi_b := \frac{1}{p_b} \sum_{z_1,\ldots,z_k} p_{b,z_1,\ldots,z_k} P(z_1)\ldots P(z_k)|z_1,\ldots,z_k\rangle\langle z_1,\ldots,z_k| \otimes \sum_z \bar{Q}_b(z|z_1,\ldots,z_k)|z\rangle\langle z|. \tag{214}$$

我们有 $\psi = p_0\ \psi_0 + p_1\psi_1$。根据 引理 3.12 以及量子互信息的非负性 ，

$$\begin{aligned} I(Z:Z_1\ldots Z_k)_\psi &\geq p_0 I(Z:Z_1\ldots Z_k)_{\psi_0} + p_1 I(Z:Z_1\ldots Z_k)_{\psi_1} - h(\delta) \\ &\geq (1-\delta) I(Z:Z_1\ldots Z_k)_{\psi_1} - 1. \end{aligned} \tag{215}$$

只需给出 $I(Z:\ Z_1\ldots Z_k)_{\psi_1}$ 的一个下界。

令 $\sigma_1 := \mathrm{tr}_{Z_1\ldots Z_k}(\psi_1)$。根据定义，

$$\begin{aligned} \sigma_1 &= \frac{1}{1-\delta} \sum_{z_1,\ldots,z_k} (1-\delta_{z_1,\ldots,z_k}) P(z_1)\ldots P(z_k) \sum_z \bar{Q}_1(z|z_1,\ldots,z_k)|z\rangle\langle z| \\ &\leq \frac{1}{1-\delta} \sum_{z_1,\ldots,z_k} (1-\delta_{z_1,\ldots,z_k}) P(z_1)\ldots P(z_k) \sum_z \mathbb{I}[z\in\{z_1,\ldots,z_k\}]|z\rangle\langle z| \\ &\leq \frac{1}{1-\delta} \sum_{z_1,\ldots,z_k} (1-\delta_{z_1,\ldots,z_k}) P(z_1)\ldots P(z_k) \sum_z \sum_{i=1}^k \mathbb{I}[z=z_i]|z\rangle\langle z|. \end{aligned} \tag{216}$$

因此，对于每个 $z \in \{0,1\}^n$，

$$\langle z|\sigma_1|z\rangle \leq \sum_i \frac{1-\delta_z^{(i)}}{1-\delta} P(z), \tag{217}$$

其中 $\delta_z^{(i)} := \mathbb{E}_{z_1,\ldots,z_{i-1},z_{i+1}\ldots,z_k\sim P}[\delta_{z_1,\ldots,z_k}]$。根据定义，$\delta_z^{(i)} \in [0,1]$，因此 $\langle z|\sigma_1|z\rangle \leq \frac{k}{1-\delta} \max_z P(z)$。这意味着

$$H(Z)_{\psi_1} \geq H_{\min}(Z)_{\sigma_1} \geq H_{\min}(P) - \log k + \log(1-\delta). \tag{218}$$

接下来我们考虑量 $H(Z|Z_1\ldots Z_k)_{\psi_1}$：根据定义，

$$H(Z|Z_1\ldots Z_k)_{\psi_1} = \frac{1}{1-\delta} \sum_{z_1,\ldots,z_k} (1-\delta_{1,z_1,\ldots,z_k}) P(z_1)\ldots P(z_k) H(\bar{Q}_1(\cdot|z_1,\ldots,z_k)) \tag{219}$$

由于 $Q_1(\cdot|z_1,\ldots,z_k)$ 的支撑集位于 $\{z_1,\ldots,z_k\}$ 中，对于每个 $z_1,\ldots,z_k$，

$$S(\bar{Q}_1(\cdot|z_1,\ldots,z_k)) \leq \log k. \tag{220}$$

由此可得

$$H(Z|Z_1\ldots Z_k)_{\psi_1} \leq \log k. \tag{221}$$

结合(210)、(215)、(218) 和(221)，

$$\begin{aligned} H(Z|E)_\psi &\geq (1-\delta)I(Z:Z_1\dots Z_k)_{\psi_1} - 1 \\ &\geq (1-\delta)(H_{\min}(P) - 2\log k) + (1-\delta)\log(1-\delta) - 1 \\ &\geq (1-\delta)(H_{\min}(P) - 2\log k) - 2. \end{aligned} \tag{222}$$

最后一个不等式成立，是因为 $-(1-\delta)\log(1-\delta) \leq h(\delta) \leq 1$。 □

定理 7.11 指出，冯·诺依曼熵取决于设备输出 $z \in \{z_1, \dots, z_k\}$ 的概率。对于 $P \sim$ 狄利克雷分布(1^N)，根据 引理 3.14，以压倒性概率，$S_{\min}(P) \geq n - \log n - O(1)$。现在我们采用以下记号

$$H(Z|PE)_\psi := \mathop{\mathbb{E}}_{P\sim \mathrm{Dir}(1^N)} \Big[H(Z|E)_{\bar{\mathcal{F}}^P(\rho)} \Big], \tag{223}$$

其中，ψ 是联合输出的经典-量子态，定义如下

$$\psi = \mathop{\mathbb{E}}_{P\sim \mathrm{Dir}(1^N)} \big[|P\rangle\langle P| \otimes \bar{\mathcal{F}}^P(\rho) \big], \tag{224}$$

even 尽管 P 不是从有限集合中抽取的样本。接下来我们证明以下定理 .

推论7.12。 对于 $P \sim$ 狄利克雷分布(1^N)，设 $\mathcal{F}$是一个算法，它可以访问 z_1、……、$z_k \sim P$以及任意双部态 ρ_{DE}的第一个子系统，并且 $\bar{\mathcal{F}}^P(\rho) = \mathbb{E}_{z_1、\dots\dots、z_k\sim P}[\mathcal{F}(\rho,\ z_1、\dots\dots、\ z_k)]$。如果

$$\Pr_{P\sim \mathrm{Dir}(1^N), z_1,\dots,z_k\sim P} [\mathcal{F}(\rho, z_1, \dots, z_k) \in \{z_1, \dots, z_k\}] \geq 1 - \varepsilon, \tag{225}$$

then

$$H(Z|PE)_\psi \geq (1-\varepsilon)n - \log n - 2\log k - O(1), \tag{226}$$

其中 ψ 是式 *(224)*中定义的量子态。

证明。 该推论可直接由 定理 7.11得出。设 P 的错误概率为ε_P。根据 定理 7.11，

$$\begin{aligned} H(Z|E)_{\bar{\mathcal{F}}^P(\rho)} &\geq (1-\varepsilon_P)H_{\min}(P) - 2\log k \\ &\geq H_{\min}(P) - \varepsilon_P n - 2\log k. \end{aligned} \tag{227}$$

根据引理 3.13，

$$\begin{aligned} H(Z|PE)_\psi &\geq \mathop{\mathbb{E}}_{P\sim \mathrm{Dir}(1^N)} [H_{\min}(P)] - \mathop{\mathbb{E}}_{P}[\varepsilon_P] n - 2\log k \\ &\geq (1-\varepsilon)n - \log n - 2\log k - O(1). \end{aligned} \tag{228}$$

□

结合 定理7.10 和 推论7.12，我们得出任何满足 $\mathcal{F}$ 的 $(1+\delta)$-XHOG 都具有条件冯·诺依曼熵 $n - o(n)$。

推论 7.13。 设 $\mathcal{F}$ 是任意一个设备，可访问来自 $P = P_C$ 的 k 个样本，用于 $C \sim \mathrm{Haar}(N)$。如果 $\mathcal{F}$ 解决了$(1+\delta)$-XHOG，那么

$$H(Z|PE)_\psi \geq \big(\delta - O(k^3/N)\big)n - \log n - 2\log k - O(1). \tag{229}$$

7.2.2 一般设备的分析

根据对图 3 中协议的分析以及一般设备与简化设备的接近程度，我们表明，任何设备若解决 XHOG，就必须满足冯·诺依曼熵下界。

定理 7.14。对于每个能够解决 b-XHOG 的 T-查询设备 $\mathcal{A}$，存在一个可访问 k 个样本的设备 $\mathcal{F}$，使得 $\mathcal{F}$ 能够在 $b' \geq b - O(nTk^{-1/2})$ 条件下解决 b'-*XHOG*。

证明。对于每个 $\mathcal{A}^P$，根据 定理 7.8，存在 $\mathcal{F}^P$ 使得

$$\begin{aligned}\left|\mathop{\mathbb{E}}_{z\sim\bar{\mathcal{A}}^P(\rho)}[P_z] - \mathop{\mathbb{E}}_{z\sim\bar{\mathcal{F}}^P(\rho)}[P_z]\right| &= \left|\sum_z P_z(p_{\mathcal{A}}(z) - p_{\mathcal{F}}(z))\right| \\ &\leq \max_z P_z \sum_z |p_A(z) - p_F(z)| \\ &\leq \max_z P_z \cdot \|\bar{\mathcal{A}}^P(\rho) - \bar{\mathcal{F}}^P(\rho)\|_{\mathrm{tr}} \\ &\leq \max_z P_z \cdot (O(Tk^{-1/2}) + O(TN^{-1/2})). \end{aligned} \tag{230}$$

对 $P\sim$狄利克雷分布(1^N)取期望，上界至多为 $O(nT(k^{-1/2}+N^{-1/2})/N)$，根据引理 3.13。这意味着，如果 $\mathcal{A}$能够解决 b-XHOG，那么 $\mathcal{F}$能够解决 $(b - O(nTk^{-1/2} + nTN^{-1/2}))$- XHOG。□

定理 7.14 表明，如果给予 $\mathcal{F}$ 足够多的样本，任何设备 $\mathcal{A}$及其简化版本 $\mathcal{F}$ 的得分都必须接近。基于这一事实，我们证明下面的定理。

定理 7.15。设 $\mathcal{A}$ 是一个对 *Haar* 随机酉矩阵 C 进行 T 次查询的任意算法。若 $\mathcal{A}$ 能解决$(1+\delta)$-*XHOG*，则存在一个量子态 ψ，它与 $\mathcal{A}$ 的输出经典-量子态$(Tk^{-1/2})$接近，使得

$$H(Z|CE)_\psi \geq \left(\delta - O(k^3/N) - O(nTk^{-1/2} + nTN^{-1/2})\right)n - \log n - 2\log k - O(1). \tag{231}$$

证明。根据 定理 7.8，对于每个 T-查询 $\mathcal{A}$，都存在 $\mathcal{F}$，可访问 k 个样本（根据 $P\sim$狄利克雷分布(1^N) 抽取），使得$\|\bar{\mathcal{A}}^P - \bar{\mathcal{F}}^P\|_\diamond \leq O\left(Tk^{-1/2}\right)$。此外，根据 定理 7.14，$\mathcal{F}$能解决$b$-XHOG，其中 $b = 1 + \delta - O(nTk^{-1/2})$。根据 推论 7.13，

$$H(Z|PE)_\psi \geq \left(\delta - O(k^3/N) - O(nTk^{-1/2} + nTN^{-1/2})\right)n - \log n - 2\log k - O(1), \tag{232}$$

其中 ψ_{ZPE}是 $\mathcal{F}$ 在 (224) 中定义的输出态，并且与 $O(Tk^{-1/2})$ 的输出 $\mathcal{A}$ 接近。最后，根据定理 7.1，证明得证。□

根据定理 7.15，对于常数 δ，每个求解$(1+\delta)$-XHOG 的算法输出条件冯·诺依曼熵为 $o(n)$ 的样本时，必须进行 $N^{\Omega(\delta)}$ 次查询。对于进行poly(n)次查询的设备，定理 7.15 蕴含以下推论。

推论 7.16。对于 $T=\mathrm{poly}(n)$、$\delta=\Omega(1)$，以及 $\eta\in(0,1]$，每个求解 $(1+\delta)$-XHOG 的 T-查询算法都必须输出一个样本 Z，满足

$$H(Z|CE)_\psi \geq (1-\eta)\delta n - O(\log n), \tag{233}$$

其中，ψ 是一个与 $\mathcal{A}$ 的输出态相差 $N^{-\Omega(\delta\eta)}$ 的量子态。

证明。根据 定理 7.15，选择 $k = T^2N^{\delta\eta}$，$Tk^{-1/2} = N^{-\delta\eta/2}$以及 $k^3/N = n^{O(1)}\cdot N^{-1+3\delta\eta}$。这意味着冯·诺依曼熵具有下界 $(1-\eta)\delta n - O(\log n)$。□

输入：安全参数 n、轮数 m、得分参数 $\delta \in [0,1]$、电路更新比例 $\gamma = O((\log\ n)/m)$，以及测试轮次比例 $\eta = O((n^2 \log n)/m)$。

协议：

1. 对于 $i = 1, \ldots, m$，执行以下步骤：

   (a) 验证者采样 $T_i \sim$ 伯努利分布(γ) 和 $F_i \sim$伯努利分布(η)。如果 $T_{i-1} = 1$ 或 $i = 1$，设备选择一个新电路 $C_i \sim \text{Haar}(N)$。否则，如果 $T_{i-1} = 0$ 和 $i > 1$，则设备将 $C_i = C_{i-1}$ 设为上一轮使用的电路。验证者向设备发送 C_i。

   (b) 证明者返回一个样本 z_i。

2. 令时期数（即使用同一电路$C_i = C$ 的一组连续轮次 i ）为 t。对于每个时期 E_j，令 $t_j = |\{i \in E_j :\ F_i = 1\}|$ 表示该时期中的测试轮次数。验证者计算

$$s_j = \frac{1}{t_j} \sum_{i \in E_j : T_i = 1} p_{C_i}(z_i). \tag{234}$$

   如果$\frac{1}{t}\sum_{j=1}^{t} \delta[s_j \geq (1+\delta)/N] \geq 0.99$，则验证者接受，并将 $(z_1, \ldots, z_m)$ 输出给抗量子随机性提取器。

图 4：熵累积协议。

7.3 熵累积

我们在图 4中给出熵累积协议。根据第4节所示的熵累积定理，我们证明条件最小熵的以下下界。

定理 7.17。设 $\mathcal{A}_1, \ldots, \mathcal{A}_m$ 是可访问双部态 ρ_{DE} 的第一系统的 $n^{O(1)}$-查询序贯过程，并输出 $z_1, \ldots, z_m$，以概率 p 求解 $\text{LXEB}_{1+\delta,k}$。则

$$H_{\min}^{\varepsilon+m\varepsilon'}(Z^m|C^m T^m E)_{\mathcal{A}_m \circ \ldots \mathcal{A}_1(\rho)|\Omega} \geq n\big(0.99\delta m - c\sqrt{m} - o(1)\big) \tag{235}$$

其中 $\varepsilon' = 2^{-\Omega(n)}$ 且Ω 表示未中止事件。参数 $c := 3.99(1+\log(\frac{1}{p\varepsilon}))^{1/2}$.

证明。 我们应用第4节中给出的熵累积定理。具体而言，我们选择$G := N\sum_z |z\rangle\langle z| P(z)$。根据推论 7.16，我们选择 $f(\delta) = (1-\eta)\delta n - O(\log n)$，为 $\eta = 0.01$ 起见。由此得到 $\|\nabla f\|_\infty = 0.99n$。于是我们有

$$\begin{aligned} V &= 2(\log(2d_Z + 1) + \|\nabla f\|_\infty) \\ &= 2(\log(2N+1) + 0.99n) \\ &= 3.98n + O(1) \\ &\leq 3.99n. \end{aligned} \tag{236}$$

现在我们有

$$H_{\min}^{\varepsilon+m\varepsilon'}(Z^m|C^mT^mE)_{\mathcal{A}_m\circ\ldots\circ\mathcal{A}_1(\rho)|\Omega} \geq n\left(0.99\delta m - O\left(\frac{\log n}{n}\right) - 3.99\sqrt{m}\sqrt{\log\frac{2}{\Pr_\sigma[\Omega]^2\varepsilon^2}}\right). \quad (237)$$

□

8 伪随机性与统计零知识

为了在随机性方面获得净增益，我们必须对协议中的挑战电路进行去随机化图 1 和 图 4。然而，已知的量子安全伪随机函数并不被认为能保证认证随机性的安全性，因为其安全性仅能抵抗量子多项式时间对手。在 第8.1节中，我们定义了一个足以保证认证随机性的、更强的伪随机函数安全性概念，并展示了一个相对于随机预言机的构造。随后在 第8.3节中，利用该伪随机函数可以实现多项式扩展。

在本节中，我们将展示，针对量子统计零知识协议的伪随机函数足以实现认证随机性。同样的论证也适用于伪随机酉算子。

根据 定理 3.6 并将其扩展到预言机分布，若存在一对算法 $\mathcal{D}_0$，$\mathcal{D}_1$ 使得当 $\mathbb{E}_{F\sim\mathcal{D}_0}\|\mathcal{A}^F-\mathcal{B}^F\|_{\mathrm{tr}}$和 $\mathbb{E}_{F\sim\mathcal{D}_1}\|\mathcal{A}^F-\mathcal{B}^F\|_{\mathrm{tr}}$ 相距甚远时，两个预言机分布 $\mathcal{D}_0$，$\mathcal{D}_1$ 被称为 量子统计零知识-可区分的。

定义8.1 (量子统计零知识-可区分性)。 如果存在一对算法 $\mathcal{A}$，$\mathcal{B}$ 以及一个多项式 p，使得

$$\left|\mathop{\mathbb{E}}_{F\sim\mathcal{D}_0}\|\mathcal{A}^{\mathcal{F}}-\mathcal{B}^F\|_{\mathrm{tr}} - \mathop{\mathbb{E}}_{F\sim\mathcal{D}_0}\|\mathcal{A}^{\mathcal{F}}-\mathcal{B}^F\|_{\mathrm{tr}}\right| > \frac{1}{p(n)}. \quad (238)$$

如果不存在这样的算法，则称这些分布是量子统计零知识-不可区分的。

定义8.1 通过加强 Zhandry 的 BQP 对手定义 [64]: 如果存在算法 $\mathcal{D}_0$，$\mathcal{D}_1$，使得预言机分布 $\mathcal{A}$ 的输出为 1 的概率相差甚远，则称这两个分布可区分，即

$$\left|\Pr_{F\sim\mathcal{D}_0}[\mathcal{A}^F=1] - \Pr_{F\sim\mathcal{D}_1}[\mathcal{A}^F=1]\right| > \frac{1}{\mathrm{poly}(n)}. \quad (239)$$

为清楚起见，本文将称 $\mathcal{D}_0$，$\mathcal{D}_1$ 是标准可区分的，如果存在 $\mathcal{A}$ 使得(239) 成立。为说明 定义8.1 是一个更强的定义，我们证明以下定理。

定理 8.2. 如果两个预言机分布 $\mathcal{D}_0$，$\mathcal{D}_1$ 是标准可区分的，那么它们就是量子统计零知识-可区分的。

证明。 由于 $\mathcal{D}_0$，$\mathcal{D}_1$ 是标准可区分的，存在 $\mathcal{A}$，它输出一个比特，且 (239) 成立。接着考虑一个平凡算法 $\mathcal{B}$，它以 0 的概率 1 输出。这意味着

$$\mathop{\mathbb{E}}_{F\sim\mathcal{D}_b}\|\mathcal{A}^F-\mathcal{B}^F\|_{\mathrm{tr}} = \Pr_{F\sim\mathcal{D}_b}[\mathcal{A}^F=1], \quad (240)$$

并且(238)成立。 □

8.1 伪随机函数

已知存在一种伪随机函数的构造，它与随机函数在标准意义下不可区分。由于我们不知道定理 8.2 的逆命题是否成立，因此提出以下假设。

假设 8.3 (伪随机函数假设)。 设 $\kappa \in \mathbb{N}$ 为安全参数，ℓ，m 为多项式有界函数。存在一个带密钥函数 F：$\{0,1\}^{\ell(\kappa)} \times \{0,1\}^{m(\kappa)} \to \{0,1\}$，使得以下条件成立。

- $F(k,x)$ 对于每个 $k \in \{0,1\}^{\ell(\kappa)}$ 和 $x \in \{0,1\}^{m(\kappa)}$，都可以在多项式时间内计算。
- 对于每一对量子算法 $\mathcal{A}$，$\mathcal{B}$，都有

$$\left| \mathop{\mathbb{E}}_{k \sim \mathcal{K}_{\ell(\kappa)}} \|\mathcal{A}^{F_k} - \mathcal{B}^{F_k}\|_{\mathrm{tr}} - \mathop{\mathbb{E}}_{F \sim \mathcal{F}_{m(\kappa)}} \|\mathcal{A}^{F} - \mathcal{B}^{F}\|_{\mathrm{tr}} \right| \leq \mathrm{negl}(\kappa) \tag{241}$$

对于充分大的 κ，其中 $\mathcal{F}_m$ 是 m位布尔函数上的均匀分布，而$\mathcal{K}_\ell$ 是 $\{0,1\}^\ell$上的均匀分布。

在本节中，我们证明假设 8.3 相对于一个随机预言机成立：对于 $\kappa = n$,$m(n) = n$，令 $\mathcal{O}$：$\{0,1\}^{\ell+n} \to \{0,1\}$ 为一个随机函数，并令 $\mathcal{O}_k(x) := \mathcal{O}(k,x)$，其中 $k \in \{0,1\}^\ell$和 $x \in \{0,1\}^n$。密钥长度 ℓ 将在后文确定。我们证明，对于任意一对 poly(n)-查询算法 $\mathcal{A}$和 $\mathcal{B}$，$\mathcal{O}, \mathcal{O}_k$ 在均匀分布 $k \in \{0,1\}^\ell$ 下与 $\mathcal{O}, H$ 在随机 H 下不可区分：$\{0,1\}^n \to \{0,1\}$。

回顾一下，对于随机函数 H：$\{0,1\}^n \to \{0,1\}$ 和 $x \in \{0,1\}^n$，对每个 $x' \neq x$，$H(x)$ 都是一个公平硬币，且独立于 $H(x')$。我们还称定义在 n 位布尔函数上的分布 $\mathcal{D}$ 为 ε-偏置随机函数，如果对于 $F \sim \mathcal{D}$，$\{F(x)$中的随机变量 $x \in \{0,1\}^n\}$ 相互独立，并且对于每个 $x \in \{0,1\}^n$，F 在 x 上的边缘分布满足 $|\Pr_{F \sim \mathcal{D}}[F(x) = 1] - 1/2| \leq \varepsilon$。首先，我们证明以下引理：对于定义在 $\{0,1\}^\ell$ 上的均匀分布 $\mathcal{U}_\ell$ 以及任意 $x \in \{0,1\}^n$，在均匀分布 k下，$\mathbb{E}_{k \sim \mathcal{U}_\ell} \mathcal{O}_k(x)$ 是弱偏置的。

引理 8.4. 对于整数 m，令 $\mathcal{F}_m$ 为函数 $\{0,1\}^m \to$上的均匀分布。则 $\{0,1\}$.

$$\Pr_{\mathcal{O} \sim \mathcal{F}_{\ell+n}} \left[\forall x \in \{0,1\}^n, \left| \mathop{\mathbb{E}}_{k \sim \mathcal{U}_\ell} \mathcal{O}_k(x) - 1/2 \right| \leq \varepsilon \right] \geq 1 - 2 \cdot 2^N e^{-L\varepsilon^2}. \tag{242}$$

证明。 根据霍夫丁不等式，对于每个 x,

$$\Pr_{\mathcal{O} \sim \mathcal{F}_{\ell+n}} \left[\left| \mathop{\mathbb{E}}_{k \sim \mathcal{U}_\ell} \mathcal{O}_k(x) - 1/2 \right| \leq \varepsilon \right] \geq 1 - 2e^{-L\varepsilon^2}. \tag{243}$$

根据并集界，我们得出证明。 □

固定一个满足该高概率事件的函数 $\mathcal{O}$。由于对于每个 $k \in \{0,1\}^\ell$，$\{\mathcal{O}_k(x) : x \in \{0,1\}^n\}$彼此独立，因此在均匀分布 k 下，$\mathcal{O}_k$ 是一个偏置为 ε 的随机函数。下面的引理表明，任何一对 T-查询算法都无法以超过 $O(T\sqrt{\varepsilon})$ 的优势，区分一个略有偏置的随机函数和一个随机函数，其中偏置差为 ε。

引理 8.5。 设 $\mathcal{A}$ 和 $\mathcal{B}$ 是两个 T-查询算法，可访问一个从$\mathcal{D}_0$或 $\mathcal{D}_1$ 中采样得到的预言机，使得对于每个 $x \in \{0,1\}^\ell$，$|$概率$_{F \sim \mathcal{D}_0}[F(x) = 1] -$概率$_{F \sim \mathcal{D}_1}[F(x) = 1]| \leq \varepsilon$。那么

$$\left| \mathop{\mathbb{E}}_{F \sim \mathcal{D}_0} \|\mathcal{A}^F - B^F\|_{\mathrm{tr}} - \mathop{\mathbb{E}}_{F \sim \mathcal{D}_1} \|\mathcal{A}^F - \mathcal{B}^F\|_{\mathrm{tr}} \right| \leq 16T\sqrt{\varepsilon}. \tag{244}$$

证明。对于 $b \in \{0,1\}$ 和 $x \in \{0,1\}^n$，令 $p_b(x) := \Pr_{F\sim\mathcal{D}_b}[F(x)=1]$。根据定义，$\varepsilon(x) := p_0(x) - p_1(x)$ 满足 $|\varepsilon(x)| \le \varepsilon$。接下来我们考虑如下定义的混合分布 $\mathcal{R}$：对于每个 x，令

$$\Pr_{F\sim\mathcal{R}}[F(x)=1] = \frac{\min\{p_0(x), p_1(x)\}}{1-|\varepsilon(x)|}. \tag{245}$$

对于 $b\in\{0,1\}$，也定义以下差异分布 $\mathcal{T}_b$

$$\Pr_{F\sim\mathcal{T}_b}[F(x)=1] = \begin{cases} 1 & \text{if } p_b(x) > p_{1-b}(x) \\ 0 & \text{if } p_b(x) < p_{1-b}(x) \\ 1/2 & \text{otherwise.} \end{cases} \tag{246}$$

对于每个 $x\in\{0,1\}^n$，

$$\Pr_{F\sim\mathcal{D}_b}[F(x)=1] = (1-|\varepsilon(x)|)\Pr_{F\sim\mathcal{R}}[F(x)=1] + |\varepsilon(x)|\Pr_{F\sim\mathcal{T}_b}[F(x)=1]. \tag{247}$$

也就是说，可以通过以下过程对 $F\sim\mathcal{D}_b$ 进行采样：对于每个 $x\in\{0,1\}^n$，首先根据分布 $\Pr[X=1] = \Pr_{F\sim\mathcal{R}}[F(x)=1]$ 对 $X\in\{0,1\}$ 进行采样。然后，以概率 $1-|\varepsilon(x)|$ 输出 X；以概率 $|\varepsilon(x)|$，以概率 $\Pr_{F\sim\mathcal{T}_b}[F(x)=1]$ 输出 1。因此，$\mathcal{D}_b$ 可以视为分布 $\mathcal{R}$，其中对每个 x 的修改概率至多为 $|\varepsilon(x)|$。

因此，证明的其余部分旨在说明，对于 $b\in\{0,1\}$，

$$\left| \mathop{\mathbb{E}}_{F\sim\mathcal{D}_b} \|\mathcal{A}^F - B^F\|_{\mathrm{tr}} - \mathop{\mathbb{E}}_{F\sim\mathcal{R}} \|\mathcal{A}^F - \mathcal{B}^F\|_{\mathrm{tr}} \right| \le 8T\sqrt{\varepsilon}. \tag{248}$$

对于任意获得由酉算子 $U_0,\dots,U_T$ 描述的 $F\sim\mathcal{D}_b$ 的预言机访问的 T-查询算法 $\mathcal{A}$，我们使用上述采样过程得到 $F = F_0 \oplus \Delta$，其中 $F_0\sim\mathcal{R}$，且 Δ 是一个偏置随机函数；对于每个 $x\in\{0,1\}^n$，$\Delta(x)=1$ 的概率至多为 $|\varepsilon(x)|$。对于 $b\in\{0,1\}$，令 Δ 的分布为 $\mathcal{P}_b$。对于每个 $F_0,\Delta\colon\{0,1\}^n\to\{0,1\}$，考虑以下混合实验：

$$\begin{aligned} |\phi_T^{\Delta}\rangle &= U_T\mathcal{O}(F_0)U_{T-1}\mathcal{O}(F_0)\dots\mathcal{O}(F_0)U_1\mathcal{O}(F_0)U_0|0\rangle, \\ |\phi_{T-1}^{\Delta}\rangle &= U_T\mathcal{O}(F)U_{T-1}\mathcal{O}(F_0)\dots\mathcal{O}(F_0)U_1\mathcal{O}(F_0)U_0|0\rangle, \\ &\vdots \\ |\phi_0^{\Delta}\rangle &= U_T\mathcal{O}(F)U_{T-1}\mathcal{O}(F)\dots\mathcal{O}(F)U_1\mathcal{O}(F_0)U_0|0\rangle, \\ |\phi_0^{\Delta}\rangle &= U_T\mathcal{O}(F)U_{T-1}\mathcal{O}(F)\dots\mathcal{O}(F)U_1\mathcal{O}(F)U_0|0\rangle. \end{aligned} \tag{249}$$

也就是说，通过先对 F_0 进行 t 次查询，再对 F 进行 $T-t$ 次查询，得到量子态 $|\phi_t^x\rangle$。另令 $|\psi_t^0\rangle = U_t\mathcal{O}(F_0)\dots U_1\mathcal{O}(F_0)U_0|0\rangle$，它与 Δ 独立。

对于每个函数 $\Delta\colon\{0,1\}^n\to\{0,1\}$，令 P_Δ 表示投影到子空间 $\{x:\Delta(x)=1\}$ 上的投影算子。根据三角不等式，

$$\begin{aligned} \||\phi_0^{\Delta}\rangle - |\phi_T^{\Delta}\rangle\| &\le \sum_{t=0}^{T-1} \|\mathcal{O}(F)|\psi_t^0\rangle - \mathcal{O}(F_0)|\psi_t^0\rangle\| \\ &= 2\sum_{t=0}^{T-1} \|P_\Delta|\psi_t^0\rangle\|. \end{aligned} \tag{250}$$

由于 $\Delta(x) = 1$ 的概率至多为 ε, $\mathbb{E}_\Delta P_\Delta \le \varepsilon_{\mathbb{I}}$，并且

$$\begin{aligned}\mathop{\mathbb{E}}_{\Delta\sim\mathcal{P}_b,F_0\sim\mathcal{R}}\|\mathcal{A}^{F_0\oplus\Delta}-\mathcal{A}^{F_0}\|_{\mathrm{tr}} &\le 2\mathop{\mathbb{E}}_{\Delta\sim\mathcal{P}_b,F_0\sim\mathcal{R}}\||\phi_0^\Delta\rangle-|\phi_T^\Delta\rangle\| \\ &\le 4T\mathop{\mathbb{E}}_{F_0\sim\mathcal{R}}\|Q\|_{\mathrm{op}}^{1/2} \\ &\le 4T\sqrt{\varepsilon}. \end{aligned} \tag{251}$$

其中 $Q=\mathbb{E}_\Delta P_\Delta$。由于对 $\mathcal{B}$ 也有相同的界，

$$\begin{aligned}&\left|\mathop{\mathbb{E}}_{F\sim\mathcal{D}_b}\|\mathcal{A}^F-\mathcal{B}^F\|_{\mathrm{tr}}-\mathop{\mathbb{E}}_{F\sim\mathcal{R}}\|\mathcal{A}^F-\mathcal{B}^F\|_{\mathrm{tr}}\right| \\ &\quad=\left|\mathop{\mathbb{E}}_{F\sim\mathcal{R}}\left(\mathop{\mathbb{E}}_{\Delta\sim\mathcal{P}_b}\|\mathcal{A}^{F\oplus\Delta}-\mathcal{B}^{F\oplus\Delta}\|_{\mathrm{tr}}-\|\mathcal{A}^F-\mathcal{B}^F\|_{\mathrm{tr}}\right)\right| \\ &\quad\le\mathop{\mathbb{E}}_{F\sim\mathcal{R}}\left(\mathop{\mathbb{E}}_{\Delta\sim\mathcal{P}_b}\|\mathcal{A}^{F\oplus\Delta}-\mathcal{A}^F\|_{\mathrm{tr}}+\mathop{\mathbb{E}}_{\Delta\sim\mathcal{P}_b}\|\mathcal{B}^{F\oplus\Delta}-\mathcal{B}^F\|_{\mathrm{tr}}\right) \\ &\quad\le 8T\sqrt{\varepsilon}. \end{aligned} \tag{252}$$

第一个不等式由三角不等式得出，第二个不等式由(251)得出。 □

结合引理 8.4 和引理 8.5，我们证明以下定理。

定理8.6。对于 $\ell\ge 2n$、$L=2^\ell$，以及任意一对 T-查询算法 $\mathcal{A}$、$\mathcal{B}$，

$$\Pr_{\mathcal{O}\sim\mathcal{F}_{\ell+n}}\left[\left|\mathop{\mathbb{E}}_{k\sim\mathcal{U}_\ell}\|\mathcal{A}^{\mathcal{O},\mathcal{O}_k}-\mathcal{B}^{\mathcal{O},\mathcal{O}_k}\|_{\mathrm{tr}}-\mathop{\mathbb{E}}_{H\sim\mathcal{F}_n}\|\mathcal{A}^{\mathcal{O},H}-\mathcal{B}^{\mathcal{O},H}\|_{\mathrm{tr}}\right|>16TN^{-1/4}\right]\le 2^{-\Omega(N)}, \tag{253}$$

其中 $\mathcal{U}_\ell$ 是 $\{0,1\}^\ell$ 上的均匀分布，$\mathcal{F}_m$ 是 $\{0,1\}^m\to\{0,1\}$ 上的均匀分布。

证明。对于 $\ell\ge 2n$，$L=2^\ell$，以及 $\varepsilon=N^{-1/2}$，$L\ge N^2$和 $2\cdot 2^N e^{-L\varepsilon^2}=2\cdot 2^N e^{-L/N}\le 2^{-\Omega(N)}$。由引理 8.5，

$$\begin{aligned}&\Pr_{\mathcal{O}\sim\mathcal{F}_{\ell+n}}\left[\left|\mathop{\mathbb{E}}_{k\sim\mathcal{U}_\ell}\|\mathcal{A}^{\mathcal{O},\mathcal{O}_k}-\mathcal{B}^{\mathcal{O},\mathcal{O}_k}\|_{\mathrm{tr}}-\mathop{\mathbb{E}}_{H\sim\mathcal{F}_n}\|\mathcal{A}^{\mathcal{O},H}-\mathcal{B}^{\mathcal{O},H}\|_{\mathrm{tr}}\right|\le 16TN^{-1/4}\right] \\ &\quad\ge\Pr_{\mathcal{O}\sim\mathcal{F}_{\ell+n}}\left[\forall x\in\{0,1\}^n,\ \left|\mathop{\mathbb{E}}_k\mathcal{O}_k(x)-1/2\right|\le N^{-1/2}\right] \\ &\quad\ge 1-2\cdot 2^N e^{-L/N} \\ &\quad\ge 1-2^{-\Omega(N)}. \end{aligned} \tag{254}$$

□

根据 Borel-Cantelli引理，每一对 多项式(n)查询算法都会无穷多次违反假设 8.3，且概率为 0。

Coro推论 8.7。 假设 *8.3* 以概率 *1* 相对于随机预言机成立。

8.2 伪随机酉算子

类似地，我们假设存在伪随机酉算子，并给出一个相对于预言机的构造。该构造与 Kretschmer 给出的构造相同 [38], ，并且我们将困难性增强至 量子统计零知识。

假设 8.8 (伪随机酉算子假设)。 设 $\kappa \in \mathbb{N}$ 为安全参数， ℓ， m 为多项式有界函数。存在一族带密钥酉算子 $\{U_k \in \mathbb{U}(2^{m(\kappa)}) : k \in \{0,1\}^{\ell(\kappa)}\}$ ，满足以下条件。

- 存在一个多项式时间量子算法 G ，它在输入 $k \in \{0,1\}^{\ell(\kappa)}$ 时实现 U_k ；也就是说，在输入 k 和量子态 $|\psi\rangle \in \mathbb{S}(2^{m(\kappa)})$ 时， $G(k, |\psi\rangle) = U_k|\psi\rangle$。
- 对于每一对量子算法 $\mathcal{A}$， $\mathcal{B}$ ，若其进行 $\mathrm{poly}(\kappa)$ 次查询，则有

$$\left| \mathop{\mathbb{E}}_{k\sim\mathcal{K}_{\ell(\kappa)}} \|\mathcal{A}^{U_k} - \mathcal{B}^{U_k}\|_{\mathrm{tr}} - \mathop{\mathbb{E}}_{U\sim\mathrm{Haar}(2^{m(\kappa)})} \|\mathcal{A}^{U} - \mathcal{B}^{U}\|_{\mathrm{tr}} \right| \leq \mathrm{negl}(\kappa). \tag{255}$$

我们给出一个相对于以下预言机的构造：设 $\kappa = n$、 $N = 2^n$、 $L = 2^\ell$ 和 $\mathcal{O} = \sum_{k\in\{0,1\}^\ell} |k\rangle\langle k| \otimes \mathcal{O}_k$，其中对每个 $k \in \{0,1\}^\ell$， $\mathcal{O}_k \in \mathbb{U}(N)$ 都是 Haar 随机酉矩阵。此外，令 $\mu = \mathrm{Haar}(N)^L$ 表示 $\mathcal{O}$ 的测度。我们证明，任何一对算法 $\mathcal{A}$、$\mathcal{B}$ 若要区分 $\mathcal{O}$、$\mathcal{O}_k$ 在均匀分布下与 $\mathcal{O}$、U 在 Haar 随机 U 下，则必须进行关于 ℓ 的指数级数量的查询。这意味着当 $\ell = \Omega(n)$ 时，该构造满足假设 8.8 中的条件。

设 $(P_1 = P, P_0 = \mathbb{I} - P)$ 是任意一个二元测量， $f(U) := \mathrm{tr}(\mathcal{A}^U P)$ 表示测量 $\mathcal{A}^U$ 的输出态时得到结果 1 的概率。我们应用 Kretschmer 的以下引理 [38]。

引理 8.9 ([38, 引理 18], 的转述)。 设 $\mathcal{A}^U$ 是任意一个 T-查询算法，且 $f(U) = \mathrm{tr}(\mathcal{A}^U P)$ 对 $0 \leq P \leq \mathbb{I}$ 成立。那么 $f(U)$ 是关于 *Frobenius* 范数的 $2T$-利普希茨函数。

我们略去引理 8.9 的证明，只概述其思路。详细证明见 [38, 引理 18]。对于满足 U, V 的酉算子 $\|U - V\|_F = d$，它们对应的酉信道之间的菱形距离至多为 $2d$。因此，根据三角不等式，$\|\mathcal{A}^U - \mathcal{A}^V\|_\diamond \leq 2Td = 2T\|U - V\|_F$，从而 $f(U)$ 是 $2T$-利普希茨函数。

就我们的目的而言，我们证明：对于任意的 k 和 U 以及成对的 T 查询算法 $\mathcal{A}$ 和 $\mathcal{B}$，函数

$$f(\mathcal{O}, k, U) := \|\mathcal{A}^{\mathcal{O},\mathcal{O}_k} - \mathcal{B}^{\mathcal{O},\mathcal{O}_k}\|_{\mathrm{tr}} - \|\mathcal{A}^{\mathcal{O},U} - \mathcal{B}^{\mathcal{O},U}\|_{\mathrm{tr}} \tag{256}$$

是关于 $\mathcal{O}$ 的 $2T$-利普希茨函数。

引理 8.10。 对于每一对 T-查询算法 $\mathcal{A}$， $\mathcal{B}$， $k \in [L]$ 以及 $U \in \mathbb{U}(N)$， $f(\mathcal{O}, k, U)$ 如 *(256)* 中所定义， $8T$-利普希茨。

证明。 只需证明，对于每个 k， $\|\mathcal{A}^{\mathcal{O},\mathcal{O}_k} - \mathcal{B}^{\mathcal{O},\mathcal{O}_k}\|_{\mathrm{tr}}$ 是关于 $\mathcal{O}$ 的利普希茨函数；对 (256) 中的第二项也可应用类似的论证。为说明这一点，我们注意到

$$\|\mathcal{A}^{\mathcal{O},\mathcal{O}_k} - \mathcal{B}^{\mathcal{O},\mathcal{O}_k}\|_{\mathrm{tr}} = \max_{0\leq P\leq \mathbb{I}} \left(\mathrm{tr}(\mathcal{A}^{\mathcal{O},\mathcal{O}_k} P) - \mathrm{tr}(\mathcal{B}^{\mathcal{O},\mathcal{O}_k} P)\right). \tag{257}$$

根据引理 8.9，对于每个 P，$\mathrm{tr}(\mathcal{A}^{\mathcal{O},\mathcal{O}_k} P) - \mathrm{tr}(\mathcal{B}^{\mathcal{O},\mathcal{O}_k} P)$ 是 $4T$-利普希茨的，因此（257）左侧也是如此。由于对于每个 $k \in \{0,1\}^\ell$ 和 $U \in \mathbb{U}(N)$， $f(\mathcal{O}, k, U)$ 是两个 $4T$-利普希茨函数之和，因此它是 $8T$-利普希茨的。 □

引理 8.10 意味着我们要给出上界的优势，即

$$\begin{aligned}\mathrm{adv}(\mathcal{O}) &:= \mathop{\mathbb{E}}_{k\sim\mathcal{U}_\ell, U\sim\mathrm{Haar}(N)} f(\mathcal{O},k,U) \\ &= \mathop{\mathbb{E}}_{k\sim\mathcal{U}_\ell} \|\mathcal{A}^{\mathcal{O},\mathcal{O}_k} - \mathcal{B}^{\mathcal{O},\mathcal{O}_k}\|_{\mathrm{tr}} - \mathop{\mathbb{E}}_{U\sim\mathrm{Haar}(N)} \|\mathcal{A}^{\mathcal{O},U} - \mathcal{B}^{\mathcal{O},U}\|_{\mathrm{tr}} \end{aligned} \tag{258}$$

是 $8T$-利普希茨的。

接下来，我们证明一个搜索下界，正式表述于 引理8.12中，用于说明平均 $\mathbb{E}_{\mathcal{O}}\mathrm{adv}(\mathcal{O})$ 在对 $\mathcal{O}$ 的选择上以压倒性概率有界。记 F_0为全零 ℓ-比特布尔函数，并将 F_x 记为其唯一的 1-原像为 x 的函数，即$F_x(y) = \mathbb{I}[x=y]$。下面的引理稍后会很有用。

引理 8.11。 设 $\mathcal{A}$是一个 T-查询算法， $\mathcal{D}$是 $\{F_x:\ x\in\{0,1\}^\ell\}$上的均匀分布，且 F_0 是零函数。那么

$$\mathop{\mathbb{E}}_{F\sim\mathcal{D}} \|\mathcal{A}^F - \mathcal{A}^{F_0}\|_{\mathrm{tr}} \le 4TL^{-1/2}. \tag{259}$$

*Pr*证明。 设该查询算法由 $T+1$ 个酉算子 U_T、.....、 U_0描述，即

$$\mathcal{A}^F|0\rangle = U_T\mathcal{O}(F)\dots U_1\mathcal{O}(F)U_0|0\rangle. \tag{260}$$

其中 $\mathcal{O}(F) := \sum_z (-1)^{F(z)}|z\rangle\langle z|$ 是预言机。令 F_x表示唯一的一个原像为 x的函数。

考虑如下状态序列

$$\begin{aligned}|\phi_T^x\rangle &= U_T\mathcal{O}(F_0)U_{T-1}\mathcal{O}(F_0)\dots\mathcal{O}(F_0)U_1\mathcal{O}(F_0)U_0|0\rangle, \\ |\phi_{T-1}^x\rangle &= U_T\mathcal{O}(F_x)U_{T-1}\mathcal{O}(F_0)\dots\mathcal{O}(F_0)U_1\mathcal{O}(F_0)U_0|0\rangle, \\ &\vdots \\ |\phi_0^x\rangle &= U_T\mathcal{O}(F_x)U_{T-1}\mathcal{O}(F_x)\dots\mathcal{O}(F_x)U_1\mathcal{O}(F_0)U_0|0\rangle, \\ |\phi_0^x\rangle &= U_T\mathcal{O}(F_x)U_{T-1}\mathcal{O}(F_x)\dots\mathcal{O}(F_x)U_1\mathcal{O}(F_0)U_0|0\rangle. \end{aligned} \tag{261}$$

也就是说，量子态$|\phi_t^x\rangle$ 是通过先对 F_0 进行 t 次查询，再对 F_x进行 $T-t$ 次查询而得到的。另令 $|\psi_t^0\rangle = U_t\mathcal{O}(F_0)\dots U_1\mathcal{O}(F_0)U_0|0\rangle$，其与 x独立。

令 $P_x = |x\rangle\langle x|$ 表示到 $|x\rangle$上的投影。根据三角不等式，

$$\begin{aligned}\||\phi_T^x\rangle - |\phi_0^x\rangle\| &\le \sum_{t=0}^{T-1} \|\mathcal{O}(F_x)|\psi_t^0\rangle - \mathcal{O}(F_0)|\psi_t^0\rangle\| \\ &\le 2\sum_{t=0}^{T-1} \|P_x|\psi_t^0\rangle\|. \end{aligned} \tag{262}$$

注意，

$$\begin{aligned}\mathop{\mathbb{E}}_{F\sim\mathcal{D}} \|\mathcal{A}^F - \mathcal{A}^{F_0}\|_{\mathrm{tr}} &\le 4\sum_{t=0}^{T-1} \mathop{\mathbb{E}}_{x\sim\mathcal{U}_n} \|P_x|\psi_t^0\rangle\| \\ &\le 4\sum_{t=0}^{T-1} \left(\mathop{\mathbb{E}}_x \langle\psi_t^0|P_x|\psi_t^0\rangle\right)^{1/2} \\ &\le 4T\cdot L^{-1/2}. \end{aligned} \tag{263}$$

第一个不等式成立，是因为 $\||\psi\rangle\langle\psi| - |\phi\rangle\langle\phi|\|_{\mathrm{tr}} \leq 2\||\psi\rangle - |\phi\rangle\|$ 对于两个归一化态 $|\psi\rangle$ 和 $|\phi\rangle$。第二个不等式根据柯西–施瓦茨不等式成立，第三个不等式则因为 $\mathbb{E}_x P_x = \mathbb{I}/L$而成立。 □

接下来，我们利用 引理 8.11 证明以下搜索下界。

引理 8.12. 设 $\mathcal{A}, \mathcal{B}$ 是两个 T-查询算法， $\mathcal{D}$ 是 $\{F_x\colon x \in \{0,1\}^\ell\}$ 上的均匀分布， F_0 是零函数。那么

$$\left| \mathop{\mathbb{E}}_{F\sim\mathcal{D}} \|\mathcal{A}^F - \mathcal{B}^F\|_{\mathrm{tr}} - \|\mathcal{A}^{F_0} - \mathcal{B}^{F_0}\|_{\mathrm{tr}} \right| \leq 8TL^{-1/2}. \tag{264}$$

证明。 根据引理 8.11，

$$\mathop{\mathbb{E}}_{F\sim\mathcal{D}} \|\mathcal{A}^F - \mathcal{A}^{F_0}\|_{\mathrm{tr}} \leq 4TL^{-1/2}, \tag{265}$$

对于 $\mathcal{B}$ 也有类似的结论。因此，对每个 $F = F_x$ ，对于 $x \in \{0,1\}^\ell$，

$$\begin{aligned} \|\mathcal{A}^F - \mathcal{B}^F\|_{\mathrm{tr}} - \|\mathcal{A}^{F_0} - \mathcal{B}^{F_0}\|_{\mathrm{tr}} &\leq \|\mathcal{A}^F - \mathcal{B}^F - \mathcal{A}^{F_0} + \mathcal{B}^{F_0}\|_{\mathrm{tr}} \\ &\leq \|\mathcal{A}^F - \mathcal{A}^{F_0}\|_{\mathrm{tr}} + \|\mathcal{B}^F - \mathcal{B}^{F_0}\|_{\mathrm{tr}}. \end{aligned} \tag{266}$$

由于上述　　不等式在交换 F 和 F_0 时具有对称性，因此我们也有

$$\|\mathcal{A}^{F_0} - \mathcal{B}^{F_0}\|_{\mathrm{tr}} - \|\mathcal{A}^F - \mathcal{B}^F\|_{\mathrm{tr}} \leq \|\mathcal{A}^F - \mathcal{A}^{F_0}\|_{\mathrm{tr}} + \|\mathcal{B}^F - \mathcal{B}^{F_0}\|_{\mathrm{tr}}. \tag{267}$$

因此我们有

$$\mathop{\mathbb{E}}_{F\sim\mathcal{D}} \left[\left| \|\mathcal{A}^F - \mathcal{B}^F\|_{\mathrm{tr}} - \|\mathcal{A}^{F_0} - \mathcal{B}^{F_0}\|_{\mathrm{tr}} \right| \right] \leq 8TL^{-1/2}. \tag{268}$$

证明的其余部分由三角不等式得出。 □

利用引理8.12，我们可以证明$\mathrm{adv}(\mathcal{O})$ 的平均值在ℓ上呈指数级小。接着，我们应用集中不等式来证明 $|\mathrm{adv}(\mathcal{O})|$ 紧密集中于$|\mathbb{E}_{\mathcal{O}\sim\mu} \mathrm{adv}(\mathcal{O})|$附近。

Lem定理 8.13。 对于任意一对 T-查询算法 $\mathcal{A}$， $\mathcal{B}$, $|\mathbb{E}_{\mathcal{O}\sim\mu} \mathrm{adv}(\mathcal{O})| \leq 8TL^{-1/}$ ^{2}.

证明。我们证 明该引理采用逆否命题的方法。假设存在两个算法 $\mathcal{A}, \mathcal{B}$

$$\mathop{\mathbb{E}}_{\mathcal{O}\sim\mu} \mathrm{adv}(\mathcal{O}) = \mathop{\mathbb{E}}_{\mathcal{O}\sim\mu, k\sim\mathcal{U}_\ell} \|\mathcal{A}^{\mathcal{O},\mathcal{O}_k} - \mathcal{B}^{\mathcal{O},\mathcal{O}_k}\|_{\mathrm{tr}} - \mathop{\mathbb{E}}_{\mathcal{O}\sim\mu, U\sim\mathrm{Haar}(N)} \|\mathcal{A}^{\mathcal{O},U} - \mathcal{B}^{\mathcal{O},U}\|_{\mathrm{tr}} > 8TL^{-1/2}. \tag{269}$$

˜ ˜接下来，我们构造另一对算法 $\mathcal{A}, \mathcal{B}$ ，它们打破引理 8.12 中的界。给定对 F 的访问权限，其中它要么是零函数，要么是均匀分布的 F_x，对于均匀分布的 $x \in \{0,1\}^\ell$, $\tilde{\mathcal{A}}$ 样本 $U_0, \ldots, U_L \sim \mathrm{Haar}(N)$，以及集合 $V = U_0$ 和 $\mathcal{O} = \sum_{k\in[L]} |k\rangle\langle k| \otimes V_k$，其中 $V_k = U_k$ 当且仅当 $F(k) = 0$，而 $V_k = U_0$ 当且仅当 $F(k) = 1$。算法 $\tilde{\mathcal{A}}$ 运行 $\mathcal{A}^{\mathcal{O},V}$，且对 $\mathcal{O}$ 的每次查询都需要对 F 进行一次查询。若 $F = 0$，则 $\tilde{\mathcal{A}}^F$ 对独立的 $\mathcal{O}, U$ 输出 $\mathbb{E}_{\mathcal{O}\sim\mu, U\sim\mathrm{Haar}(N)} |\mathcal{O}, U\rangle\langle\mathcal{O}, U| \otimes \mathcal{A}^{\mathcal{O},U}$；若 $F = F_k$，则 $\tilde{\mathcal{A}}^F$ 输出 $\mathbb{E}_{\mathcal{O}\sim\mu, k\sim\mathcal{U}_\ell} |\mathcal{O}, k\rangle\langle\mathcal{O}, k| \otimes \mathcal{A}^{\mathcal{O},\mathcal{O}_k}$。算法 $\tilde{\mathcal{B}}$ 运行完全相同的算法，唯一的区别是将 $\mathcal{A}$ 替换为 $\mathcal{B}$。结合 $\mathcal{A}, \mathcal{B}$，我们得到一个违反引理 8.12 的界。

现在我们已经证明了 $\mathbb{E}_{\mathcal{O}\sim\mu} \mathrm{adv}(\mathcal{O}) \leq 8TL^{-1/2}$。利用相同的论证可以证明 $-\mathbb{E}_{\mathcal{O}\sim\mu} \mathrm{adv}(\mathcal{O}) \leq 8TL^{-1/2}$，因此证明完毕。 □

我们已经证明，adv($\mathcal{O}$) 是一个 $8T$-Lipschitz函数，且平均值$|\mathbb{E}_{\mathcal{O}\sim\mu}\text{adv}(\mathcal{O})|$的绝对值为 $O(TL^{-1/2})$。现在我们应用以下集中不等式来证明：对于 $\mathcal{O}$、 $|\text{adv}(\mathcal{O})| \leq O(TL^{-1/2})$ 的选择，以压倒性概率成立。

定理 *8.14*（[38, 定理 11] 和 [43, 定理 *5*.17]）。对于 N_1、.....、 $N_k \in \mathbb{N}$，设 $X = \mathbb{U}(N_1) \oplus \ldots \oplus \mathbb{U}(N_k)$。令 $\mu = Haar(N_1) \times \ldots Haar(N_k)$ 表示 X 上 *Haar* 测度的乘积。假设 $f:\ X \to \mathbb{R}$ 关于 *Frobenius*范数是 K-利普希茨的。那么对于任意 $t > 0$,

$$\Pr_{\mathcal{O}\sim\mu}\left[f(\mathcal{O}) \geq \mathop{\mathbb{E}}_{\mathcal{P}\sim\mu} f(\mathcal{P}) + t\right] \leq \exp\left(-\frac{(N-2)t^2}{24K^2}\right), \tag{270}$$

其中 $N =$最小值$\{N_1, \ldots, N_k\}$。

由于 $\mathcal{O} = \sum_{k\in\{0,1\}^\ell} |k\rangle\langle k| \otimes \mathcal{O}_k$其中对于每个 $k \in \{0,1\}^\ell$， $\mathcal{O}_k \sim$Haar(N)，adv($\mathcal{O}$) 是 $\{\mathcal{O}_k\}_{k\in\{0,1\}^\ell}$的函数，因此可以应用集中不等式。

定理 8.15。对于 $\ell = \lceil n - \text{对数 } n\rceil$ 以及 $L = 2^\ell$，概率$_{\mathcal{O}\sim\mu}[|\text{adv}(\mathcal{O})| \geq 16TL^{-1/2}] \leq 2^{-\Omega(n)}$。

证明。 根据定理 8.14,

$$\Pr_{\mathcal{O}\sim\mu}[\text{adv}(\mathcal{O}) \geq 16TL^{-1/2}] \leq \exp\left(-\frac{(N-2)}{1536L}\right). \tag{271}$$

对于 $\ell = \lceil n - \log\ n\rceil$，上界为 $2^{-\Omega(n)}$。可以用相同的论证证明，事件–adv($\mathcal{O}$) $\geq 16TL^{-1/2}$ 以概率 $2^{-\Omega(n)}$发生。应用并集界，我们得出证明。

□

应用 Borel-Cantelli引理，对于 $\ell = \lceil n - \log n\rceil$，每一对 poly($n$)- 查询算法违反 假设 8.8 中条件的事件以概率 0 无限多次发生。

推论 8.16。 存在一个预言机，相对于该预言机，假设 *8.8* 以概率 *1* 成立 .

8.3 随机性扩展

在 第8.1节中介绍的假设下，对于任意认证随机性协议，我们可以将输入熵降至设备，同时输出仍然接近均匀分布。为了解释其原因，我们回顾抗量子随机性提取器的定义 [37, 26]。

定义 8.17（抗量子强提取器 [26, 定义3。2]）。 函数 Ext: $\{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ 是一个带有均匀种子的抗量子（k， ε）-强提取器，若对于所有在 X 上经典的量子态 ρ_{XE}，满足 $H_{\min}(X|E)$，$\geq k$，且对于均匀的 Y,

$$\|\rho_{\text{Ext}(X,Y)YE} - \rho_{U_m} \otimes \rho_Y \otimes \rho_E\|_{\text{tr}} \leq \varepsilon, \tag{272}$$

其中，ρ_{U_m} 是 $\{0,1\}^m$ 上的均匀分布。

或者，如果我们只能保证对于足够小但非零的 δ， $H^\delta_{\min}(X|E) \geq k$，根据三角不等式，提取器输出的分布在给定旁信息 E 的条件下，仍然足够接近均匀分布。

引理 8.18 ([26, 引理 3。5])。 如果 Ext: $\{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ 是一个量子安全 $(k,\ \varepsilon)$-强提取器，那么对于任意 ρ_{XE} 以及 $\delta > 0$ 满足 $H_{\min}^{\delta}(X|E)_\rho \geq k$,

$$\|\rho_{\mathrm{Ext}(X,Y)YE} - \rho_{U_m} \otimes \rho_Y \otimes \rho_E\|_{\mathrm{tr}} \leq \varepsilon + 2\delta. \tag{273}$$

若 E 被限制为经典态，那么我们称满足 定义8.17 的为经典安全 $(k,\ \varepsilon)$-强提取器。此外，若 定义 8.17 在 E 为空的特殊情况下成立，则称这样的提取器为 $(k,\ \varepsilon)$- 更强提取器。

在同一篇论文中，De、Portmann、Vidick 和 Renner [26] 证明了 Trevisan 提取器 [59]是一个抗量子强提取器。我们采用 [26]中的相关定义。

定义 8.19 (弱设计 [26, 定义 4。1])。 对于整数 d，集合族 S_1、……、$S_m \subset [d]$是一个弱$(t,\ r)$-设计，当且仅当

1. 对每个 $i \in [m],\ |S_i| = t$。*2.* 对每个 $i \in [m],\ \sum_{j=1}^{i-1} 2^{|S_i \cap S_j|} \leq rm$。

定义 8.20 (Trevisan 提取器 [26, 定义 4.2][59])。 对于单比特提取器 $C\colon \{0,1\}^n \times \{0,1\}^t \to \{0,1\}$，它使用长度为 t 的（不一定均匀分布的）种子；对于弱 (t,r)-设计，$S_1, \ldots, S_m \subset [d]$，定义一个 m 比特提取器 $\mathrm{Ext}_C\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ 如下：

$$\mathrm{Ext}_C(x,y) := C(x, y_{S_1}) \ldots C(x, y_{S_m}). \tag{274}$$

整数 d在 定义 8.19 中表示提取器 Ext_C 的种子长度，且取决于t（即 1 比特提取器种子的大小） C。如果误差 $d = \mathrm{poly}(\log n)$为 ε =poly$(1/n)$ [26]，则种子的大小始终为 同一篇论文还证明，单比特强提取器也是抗量子强提取器。

定理 *8.21* （[26, 定理 *4.7*]） 。设 $C\colon \{0,1\}^n \to \{0,1\}^t \to \{0,1\}$ 是一个（k, ε）-强提取器，使用 s 位种子——也就是说，种子至少需要 s 位最小熵——且 $S_1, \ldots, S_m \subset [d]$ 构成一个弱（t, r）-设计。那么，对于任意最小熵为 $d -$ （$t - s -$ *log* $\frac{1}{3\sqrt{\varepsilon}}$）的种子，定义 *8.20* 中定义的提取器都是一个量子证明（$k + rm +$*log*$(1/\varepsilon)\, 6m\sqrt{\varepsilon}$）-强提取器。

此外，存在一个 （k，ε）-强提取器，由 Raz、Reingold 和 Vadhan 提出 [54], ，且输入种子的长度为 polylog(n)。

定理 8.22 （[26, 命题 5.2]） 。 对于任意 $\varepsilon > 0$ 和 $n \in \mathbb{N}$，都存在一个（k，ε）-强提取器，其均匀种子为 $\mathrm{Ext}_{n,\ \varepsilon}$： $\{0,1\}^n \times \{0,1\}^t \to \{0,1\}$，其中 $t = O$（log(n/ε) 且 k =3 log$(1/\varepsilon)$。

结合存在抗量子强提取器这一事实以及假设 8.3，我们证明以下定理。

定理 8.23。 假设假设 *5.1* 和假设 *8.3* 成立。存在一种随机性扩展协议，适用于能够解决LXEB$_b$的k 设备，对给定电路中的99% 实现多项式扩展，并且对 $b = 1.02$ 和 $k = O$（n^2）实现多项式扩展，其中 n 是每个电路作用的量子比特数。

证明。在我们的 m轮随机性扩展协议中，如图 1所示，我们使用随机电路，并至少更换电路 $\gamma m = O$ $(\log n)$ 次，且每个电路都可以替换为伪随机电路

其输入为 $\ell = \text{poly}(n)$ 比特（用于生成伪随机函数的密钥）。对于求解 $\text{LXEB}_{1+\delta\text{的}k}$ 设备，在常数 δ 和 $k = O(n^2)$ 条件下，该协议使用 $O(\ell\log\ n)$ 个均匀随机比特作为输入，生成与 $\Omega(m)$ 比特均匀分布相差至多 $\varepsilon + 2\varepsilon' + \text{negl}(n)$ 的分布。对于 $c \geq 2$，令 $m = \ell^c$，该协议可累积净熵。 □

采用与定理 8.23的证明中相同的推理，我们得出，假设 8.8蕴含存在一个随机性扩展协议。

定理 8.24。假设假设 *8.8* 成立。对于一个获得伪随机酉算子预言机访问并求解$\text{LXEB}_{b,\ k}$ 的设备，存在一个随机性扩展协议，该协议对于给定电路中的99% 实现 $b = 1.02$ 和 $k = O(n^2)$的多项式扩展，其中 n 是每个电路作用的量子比特数。

致谢

我们感谢 Fernando Brandão、Alex Halderman、William Kretschmer、John Martinis、Carl Miller、RonPeled、René Peralta、Or Sattath、Thomas Vidick 和 David Zuckerman 所进行的富有帮助的讨论。

参考文献

[1] Scott Aaronson. QMA/qpoly $\subseteq$ PSPACE/poly：去 Merlin 化量子协议。载于第 *21* 届 *IEEE* 计算复杂性年会（*CCC'06*），第 13–pp 页。IEEE，2006 年。

[2]Scott Aaronson. 量子霸权认证随机性。在 *Google* 量子研讨会上的演讲，威尼斯海滩，加利福尼亚州，*2018* 年 *5* 月 *16* 日，2018 年。
https://www.scottaaronson.com/talks/certrand-huji.ppt。[3] Scott Aaronson 和 Andris Ambainis。量子加速中对结构的需求。计算理论，10(1):133–166，2014 年。[4] Scott Aaronson 和 Alex Arkhipov。线性光学的计算复杂性。载于第四十三届 *ACM* 计算理论研讨会论文集，第 333–342 页，2011 年。[5] Scott Aaronson 和 Alex Arkhipov。玻色子采样远非均匀分布。《量子信息与计算》，14(15-16):1383–1423，2014 年。[6] Scott Aaronson、Adam Bouland、Joseph Fitzsimons 和 Mitchell Lee。恰好高于 BQP 的空间。载于*2016* 年 *ACM* 理论计算机科学创新会议论文集，第 271–280 页，2016 年。[7] Scott Aaronson 和 Lijie Chen。量子霸权实验的复杂性理论基础。*arXiv* 预印本 *arXiv:1612.05903*，2016 年。[8] Scott Aaronson 和 Andrew Drucker。量子辅助信息的完整刻画。载于第四十二届 *ACM* 计算理论研讨会论文集，第 131–140 页，2010 年。

[9] Andris Ambainis、Ansis Rosmanis 和 Dominique Unruh。《针对经典证明系统的量子攻击：量子回绕的困难性》。载于*2014*年*IEEE*第*55*届计算机科学基础年会，第474–483页。IEEE，2014年。

[10] Rotem Arnon-Friedman。《设备无关量子信息处理中的归约到独立同分布》。博士论文，苏黎世联邦理工学院，2018年。[11] Rotem Arnon-Friedman、Frédéric Dupuis、Omar Fawzi、Renato Renner 和 Thomas Vidick。《通过熵累积实现实用的设备无关量子密码学》。《自然通讯》，9(1):1–11，2018年。[12] Frank Arute、Kunal Arya、Ryan Babbush、Dave Bacon、Joseph C Bardin、Rami Barends、Rupak Biswas、Sergio Boixo、Fernando GSL Brandão、David A Buell 等。《使用可编程超导处理器实现量子霸权》。《自然》，574(7779):505–510，2019年。[13] Boaz Barak、Chi-Ning Chou 和 Xun Gao。《在浅层量子电路中伪造线性交叉熵基准测试》。载于第十二届理论计算机科学创新会议（ITCS 2021）。Schloss Dagstuhl-Leibniz-Zentrum für Informatik，2021年。[14] Roozbeh Bassirian、Adam Bouland、Bill Fefferman、Sam Gunn 和 Avishay Tal。《关于量子优势实验所认证的随机性》。arXiv预印本 arXiv:2111.14846，2021年。[15] Robert Beals、Harry Buhrman、Richard Cleve、Michele Mosca 和 Ronald de Wolf。《基于多项式的量子下界》。《Journal of the ACM》（JACM），48(4):778–797，2001年。[16] Shalev Ben-David 和 Robin Kothari。《量子判别复杂度、零错误算法与统计零知识》。载于第14届量子计算、通信与密码学理论会议，第21卷，第24页，2019年。[17] Charles H Bennett、Ethan Bernstein、Gilles Brassard 和 Umesh Vazirani。《量子计算的优势与弱点》。《SIAM计算杂志》，26(5):1510–1523，1997年。[18] Peter Bierhorst、Emanuel Knill、Scott Glancy、Yanbao Zhang、Alan Mink、Stephen Jordan、Andrea Rommal、Yi-Kai Liu、Bradley Christensen、Sae Woo Nam 等。《由超光速信号不可能性认证的实验生成随机性》。《自然》，556(7700):223–226，2018年。[19]Joseph Bonneau、Jeremy Clark 和 Steven Goldfeder。《论比特币作为公共随机性来源》。密码学电子印本档案，论文 2015/1015，2015年。https://eprint.iacr.org/2015/1015。[20] Zvika Brakerski、Paul Christiano、Urmila Mahadev、Umesh Vazirani 和 Thomas Vidick。《单个量子设备的量子性密码学测试与可认证随机性》。载于2018年IEEE第59届计算机科学基础年会（FOCS），第320–331页。IEEE，2018年。[21]Fernando GSL Brandão、Aram W. Harrow 和 Michał Horodecki。《局部随机量子电路是近似多项式设计》。《数学物理通讯》，346(2):397–434，2016年。[22] Luís TAN Brandão 和 René Peralta。《关于询问随机量子电路的札记》。NIST白皮书，2020年。[23] Michael J Bremner、Richard Jozsa 和 Dan J Shepherd。《对易量子计算的经典模拟意味着多项式层级坍塌》。《英国皇家学会学报A辑：数学、物理与工程科学》，467(2126):459–472，2011年。

[24] Roger Colbeck。《用于安全多方计算的量子与相对论协议》。博士论文，2009年。[25] Matthew Coudron 和 Henry Yuen。《使用恒定数量设备的无限随机性扩展》。载于第四十六届 *ACM* 计算理论研讨会论文集，第 427–436 页，2014 年。[26] Anindya De 、 Christopher Portmann、Thomas Vidick 和 Renato Renner。《存在量子侧信息时的 Trevisan 提取器》。《*SIAM*计算杂志》，41(4):915–940，2012年。[27] Catherine Donati-Martin 和 Alain Rouault。《Haar 分布矩阵的随机截断与桥》。*arXiv* 预印本 *arXiv:1302.6539*，2013年。[28] Frederic Dupuis、Omar Fawzi 和 Renato Renner。《熵累积》。《数学物理通讯》，379(3):867–913，2020年。[29] Edward Farhi、Jeffrey Goldstone 和 Sam Gutmann。《量子近似优化算法》。*arXiv* 预印本 *arXiv:1411.4028*，2014年。[30] Bela A. Frigyik、Amol Kapila 和 Maya R. Gupta。《狄利克雷分布及相关过程导论》。华盛顿大学电气工程系，*UWEETR-2010-0006*，6:1–27，2010年。[31] Oded Goldreich、Amit Sahai 和 Salil Vadhan。《统计零知识能否变为非交互式？或论 SZK 与 NISZK 的关系》。载于年度国际密码学会议，第 467–484 页。施普林格，1999年。[32] Shafi Goldwasser 和 Michael Sipser。《交互式证明系统中的私有随机币与公开随机币》。载于第十八届 *ACM* 计算理论研讨会论文集，第 59–68 页，1986年。[33]Jonas Haferkamp。《随机量子电路在深度$O\left(nt^{5+o(1)}\right)$下是近似酉 t-设计》。*arXiv* 预印本 *arXiv:2203.16571*，2022年。[34]Joonsuk Huh、Gian Giacomo Guerreschi、Borja Peropadre、Jarrod R McClean 和 Alán Aspuru-Guzik。《用于分子振电光谱的玻色子采样》。《自然·光子学》，9(9):615–620，2015年。[35] Gregory D Kahanamoku-Meyer、Soonwon Choi、Umesh V Vazirani 和 Norman Y Yao。《来自计算型贝尔测试的经典可验证量子优势》。《自然·物理》，18(8):918–924，2022年。[36] John Kelsey、Luís TAN Brandão、Rene Peralta 和 Harold Booth。《随机性信标参考：格式与协议第 2 版》。技术报告，美国国家标准与技术研究院，2019年。[37] Robert Konig 和 Renato Renner。《相对于量子知识的最小熵采样》。《*IEEE*信息论汇刊》，57(7):4760–4787，2011年。[38] William Kretschmer。《量子伪随机性与经典复杂性》。载于第 *16* 届量子计算、通信与密码学理论会议（*TQC 2021*）。Schloss Dagstuhl-Leibniz-Zentrum für Informatik，2021年。

[39] William Kretschmer。《量子霸权 Tsirelson 不等式》。*Quantum*，5:560，2021年。[40] Lars S Madsen、Fabian Laudenbach、Mohsen Falamarzi Askarani、Fabien Rortais、Trevor Vincent、Jacob FF Bulmer、Filippo M Miatto、Leonhard Neuhaus、Lukas G Helt、Matthew J Collins 等。《使用可编程光子处理器实现量子计算优势》。《自然》，606(7912):75–81，2022年。[41] Urmila Mahadev、Umesh Vazirani 和 Thomas Vidick。《来自单个量子设备的高效可认证随机性》。*arXiv* 预印本 *arXiv:2204.11353*，2022年。[42] Chris Marriott 和 John Watrous。《量子 Arthur–Merlin 博弈》。载于《第 *19* 届 *IEEE* 计算复杂性年度会议论文集，*2004*年》，第 275–285 页。IEEE，2004年。[43] Elizabeth S Meckes。《经典紧群的随机矩阵理论》，第 218 卷。剑桥大学出版社，2019年。[44] Sanketh Menda 和 John Watrous。《量子统计零知识的预言机分离》。*arXiv* 预印本 *arXiv:1801.08967*，2018年。[45] Tony Metger、Omar Fawzi、David Sutter 和 Renato Renner。《广义熵累积》。*arXiv*，abs/2203.04989，2022年。[46] Carl A Miller 和 Yaoyun Shi。《使用不可信量子设备安全扩展随机性并分发密钥的鲁棒协议》。*Journal of the ACM*（*JACM*），63(4):1–63，2016年。[47] Carl A Miller 和 Yaoyun Shi。《来自点检协议的随机性扩展的通用安全性》。《*SIAM*计算杂志》，46(4):1304–1335，2017年。[48] Michael A Nielsen 和 Isaac Chuang。《量子计算与量子信息》，2002年。[49] Feng Pan、Keyang Chen 和 Pan Zhang。《求解 Sycamore 量子霸权电路的采样问题》。*arXiv* 预印本 *arXiv:2111.03011*，2021年。[50] Stefano Pironio、Antonio Acín、Serge Massar、A Boyer de La Giroday、Dzmitry N Matsukevich、Peter Maunz、Steven Olmschenk、David Hayes、Le Luo、T Andrew Manning 等。《由贝尔定理认证的随机数》。《自然》，464(7291):1021–1024，2010年。[51]John Preskill。《量子计算与纠缠前沿》。*arXiv* 预印本 *arXiv:1203.5813*，2012年。[52] John Preskill。《NISQ 时代及其之后的量子计算》。*Quantum*，2:79，2018年。[53] Ran Raz。《量子信息与 PCP 定理》。*Algorithmica*，55(3):462–489，2009年。[54] Ran Raz、Omer Reingold 和 Salil Vadhan。《提取全部随机性并降低 Trevisan 提取器中的误差》。载于第三十一届 *ACM* 计算理论研讨会论文集，第 149–158 页，1999年。[55] Ran Raz 和 Avishay Tal。《BQP 与多项式层级的预言机分离》。*ACM Journal of the ACM*（*JACM*），69(4):1–21，2022年。[56] Markus Reiher、Nathan Wiebe、Krysta M Svore、Dave Wecker 和 Matthias Troyer。《阐明量子计算机上的反应机制》。美国国家科学院院刊，114(29):7555–7560，2017年。

[57] Maria Schuld、Kamil Brádler、Robert Israel、Daiqin Su 和 Brajesh Gupt。使用高斯玻色子采样器测量图的相似性。*Physical Review A*，101(3):032314，2020年。[58] Alexander A Sherstov。量子通信和查询复杂度的强直接积定理。载于第*43*届 *ACM* 计算理论研讨会论文集，第 41–50 页，2011年。[59] Luca Trevisan。提取器与伪随机生成器。*Journal of the ACM*，48(4):860–879，2001年。[60] Umesh Vazirani 和 Thomas Vidick。可验证量子骰子：或称能够抵御量子对手的真正随机数生成。载于第*44*届 *ACM* 计算理论研讨会论文集，第 61–76 页，2012年。[61] John Watrous。量子统计零知识的能力极限。载于*2002* 年第 *43* 届 *IEEE* 计算机科学基础年会论文集，第 459–468 页。IEEE，2002年。[62] Yulin Wu、Wan-Su Bao、Sirui Cao、Fusheng Chen、Ming-Cheng Chen、Xiawei Chen、Tung-Hsun Chung、Hui Deng、Yajie Du、Daojin Fan 等。使用超导量子处理器实现强量子计算优势。*Physical review letters*，127(18):180501，2021年。[63] Takashi Yamakawa 和 Mark Zhandry。无结构的可验证量子优势。*arXiv* 预印本 *arXiv:2204.02063*，2022年。[64] Mark Zhandry。如何构造量子随机函数。载于*2012 IEEE* 第 *53* 届计算机科学基础年会，第 679–687 页。IEEE，2012年。[65] Han-Sen Zhong、Hui Wang、Yu-Hao Deng、Ming-Cheng Chen、Li-Chao Peng、Yi-Han Luo、Jian Qin、Dian Wu、Xing Ding、Yi Hu 等。利用光子实现量子计算优势。*Science*，370(6523):1460–1463，2020年。