arXiv:2304.03448v2 [quant-ph] 5 Dec 2023

使用现成设备进行量子委托

Anne Broadbent[1,2],Arthur Mehta[1,2],和 Yuming Zhao[3,4]

[1]渥太华大学数学与统计系[2]渥太华大学量子技术中心[3]滑铁卢大学量子计算研究所[4]滑铁卢大学纯数学系

摘要

鉴于可靠的云量子计算机正逐渐成为现实，量子计算的委托及其可验证性已成为备受关注的核心议题。人们提出了许多模型，各有其优势与不足。在此，我们提出一种新模型：客户端只信任自身的经典处理，不作任何计算假设，并在单 轮中与量子服务器交互。此外，在设置阶段，客户端会指定计算规模 n，并接收一台不可信的现成（*OTS*）量子设备，用于报告一次测量的结果。

我们展示了如何在OTS模型中委托多项式时间量子计算。这还为所有 QMA提供了一个交互式证明系统；此外，我们证明该系统可以在统计零知识中实现。这为 QMA 提供了首个相对论式（单轮）、双证明者零知识证明系统。

作为一种证明方法，我们仅使用常数规模的泡利测量，为 n EPR对提供了一种新的自检方法，并展示了它如何为使用可模拟码进行局部哈密顿量验证提供一条新途径。在此过程中，我们还给出了 Gowers和 Hatami提出的一个著名稳定性结果的增强版本，并展示了它如何完成自检中常用的一项论证。

目录

1 引言 **1**
1.1 背景 .3 1.2 技术背景 .4 1.3 贡献 .5 1.4 证明方法与技术贡献 .7 1.5 未解决的问题 .10 1.6 致谢 .11 1.7 章节概要 .11

2 预备知识 **11**
2.1 记号.11 2.2 量子信息 .12 2.3 群与表示 .13 2.4 非局部博弈与刚性 .13 2.5 复杂性类与零知识 .15 2.6 可模拟码与门的编码 .16 2.7 局部哈密顿量 .17

3 低权重 Pauli 编织测试 **17**
3.1 低权重线性测试 .17 3.2 低权重反对易测试 .20 3.3 形式化陈述 .20

4 低权重泡利编织测试的刚性 **21**
4.1 增强版 Gowers-Hatami 定理 .21 4.2 刚性的证明.23 4.3 相关自测试 .28

5 修改后的哈密顿量博弈 **29**

6 零知识证明系统 **32**
6.1 用于历史态模拟 XZ-哈密顿量 .32 6.2 面向QMA 的双证明者零知识证明系统.33

7 现成模型 **35**
7.1 模型的形式化描述.35 7.2 在零知识和委托计算中的应用 .36

1 引言

在交互式证明系统中，计算能力受限的验证者会与强大的证明者交互，以验证双方商定的问题实例是否真实。从QMA开始，随后是QIP 和 QMIP (以及其他系统)，量子交互式证明系统（其中验证者是量子多项式时间的）得以定义和研究 [Wat00、Wat03、KM03]。

然而，这些量子化方案关键依赖于这样一个心照不宣的假设：验证者能够访问可信的量子多项式时间验证。鉴于当前量子计算发展所处的技术水平、刻画量子系统的内在困难，以及无法可靠验证量子计算轨迹这一事实，有充分证据表明这一假设可能值得质疑。事实上，尽管技术取得了令人瞩目的进步，我们最终可能不得不面对这样一种现实：量子计算机永远无法像经典设备那样值得信赖或可靠。这一前景促使人们考虑这样的模型：验证者能够访问非常有限但可信的量子功能 [ABEM17、Bro18、FK17], ；或者验证者完全是经典的，而证明者受到计算能力限制 [Mah18], ；另一类称为MIP* 的模型则描述了一个高效的经典验证者与多个彼此隔离、计算能力无界的量子证明者进行交互 [CHTW04]。每种方法都带来优势，也面临挑战：早期的量子服务器将十分昂贵，因此在其他条件相同的情况下，要求单个证明者更为可取；另一方面，现有的单证明者协议要么要求可信设备，要么依赖计算假设。多证明者协议利用强大的设备无关性技术，避免了这些假设，但代价高昂：需要多个强大的证明者，并且要求彼此隔离。

当前该领域的时代思潮使我们能够富有想象力地思考如何描述和建模量子世界中的任务。这些方法的共同点在于，我们不再考虑经典协议的直接量子对应物，而是力求进行在量子场景中具有自然动机的思考[1]。在此，我们沿着这一势头继续前进，并介绍一种新颖的证明验证方法，其中设置阶段本身只能在量子场景中获得动机。为此，我们考虑以下问题：

问题 1. 具有单个量子证明者和能够访问**现成的非可信量子设备**的经典验证者的**相对论性**交互式证明系统，其类别的表达能力如何?

现成设备。我们将上述模型称为现成（*OTS*）模型，因为它描述了这样一个事实：验证者除了与标准证明者交互之外，还可以访问一个设备，该设备具有以下特性：(1) 通用（它不依赖于待解决问题的实例，只依赖于实例规模），(2)高效（对于完备性，多项式资源即可满足要求），(3)完全不受信任（对于可靠性，不对其计算能力或内部工作原理作任何假设）。重要的是，相对论指的是一个 1 轮协议；由于相对容易实施隔离，这一点很理想[2]。

从操作层面来看，我们将OTS 模型设想为：证明者在证明验证之前向验证者提供这样一个通用的现成设备。特别是，就其功能而言，此类设备的准备与特定问题实例无关，尽管我们允许其依赖于设备的规模。一旦拥有该设备，验证者便可以查询证明者，同时使用该现成设备进行一次测量，从而使验证者接受 或拒绝。交互式证明系统的性能指标是通常的完备性和可靠性。

[1]例如，可参见近期关于制备量子态和酉算子复杂度的研究 [RY22]。[2]在多证明者场景中，相对论协议非常理想，因为可以利用相对位置和响应时间来实施隔离 [CL17，Gri19]。

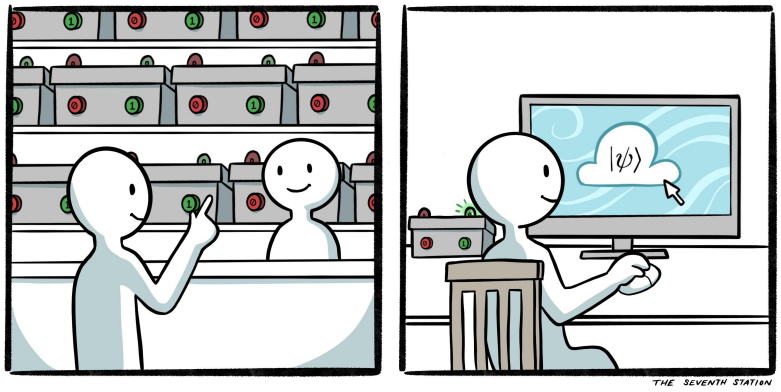

图1：在设置阶段，验证者根据问题实例所需的规模选择一台现成设备。之后，验证者可以自由选择任意语言和实例，并在单轮中同时与证明者和现成设备进行交互，从而得到验证者的接受/拒绝 输出。

由于 OTS 场景刻画了使用不可信量子设备进行近期证明验证的某些方面，因此我们自然希望了解它与交互式证明系统中一些最相关且最受研究的性质之间的关系：

问题 2。OTS模型能否为**零知识证明系统**以及**委托量子计算**提供新方法?

零知识证明系统。零知识（*ZK*）证明系统体现了这一反直觉的概念：交互式证明可以同时具有说服力，又完全隐藏证明者的内部运作机制；这类证明系统在复杂性理论和密码学的许多领域，以及网络安全领域中都发挥着重要作用，因为它们能够防止逆向工程。我们在此关注统计零知识，即隐藏属性对于无界验证者仍然成立。鉴于我们新的 OTS 模型，我们首先要提出的问题之一是：OTS 模型中的证明系统是否可以实现零知识。

委托量子计算。在委托量子计算中，计算能力较弱的客户端将量子计算外包给能力更强（但计算能力有界）的设备，并确保结果可验证。从 OTS 模型出发，我们可以将其缩减规模（使证明者不再是无界的，而仅为量子多项式时间；验证者和现成设备保持不变）。于是问题变为：通过相对论性交互，经典多项式时间客户端能否与一台 OTS 设备协作，在确保可验证的前提下，将自己选择的量子计算外包给一台隔离的量子多项式时间设备，前提是该量子计算的规模与 OTS 设备的参数相匹配?

结果总结。在这项工作中，我们朝着回答上述问题迈出了重要步伐：

- 我们证明，在 OTS 模型中，QMA 中的任何语言都有一个统计零知识证明系统。
- 我们展示上述 OTS 证明系统可以适用于 BQP中的任意问题的委托量子计算，同时保持零知识性并处于 OTS 模型中。

1.1 背景

现在，我们将概述背景材料，并总结量子场景下当前最先进的交互式证明系统和委托计算方法，重点关注与我们主要问题相关的要素，并指出现有方法在适用于我们的场景时存在的不足。

1.1.1 经典与量子交互式证明系统

在交互式证明系统（IP）模型中，高效的经典验证者与一个能力无限但不可信的证明者进行交互，以验证某个命题的正确性 [GMR89]。我们注意到，类NP 对应于单条消息的交互（其MA 为概率版本），而交互式证明系统包含一轮交互（即，两条消息）。

在多证明者交互式证明系统（MIP）中，验证者与多个彼此隔离的证明者进行交互 [BGKW88]。上述每种模型都已被量子化，即扩展到部分或所有参与方均为量子的情形。例如，QMA（MA 的量子版本）、QIP（IP 的量子版本）和 MIP* （多证明者交互式证明系统（MIP）的一种版本，其中多个无界证明者共享纠缠）等复杂性类就体现了这一点。一些重要成果刻画了其中若干量子复杂性类，例如 QIP = PSPACE [JJUW11]和 MIP* =RE [JNV+20]。

1.1.2 零知识

研究交互式证明系统的一个强烈动机，是它与零知识证明系统这一反直觉概念之间的联系 [GMW91，BOGG+88]。非正式地说，当验证者无法获知除已约定的实例为真这一事实之外的任何信息时，证明系统就是零知识的。更形式化地说，这是通过确立一个模拟器的存在来处理的，该模拟器能够重现交互记录。

Watrous [Wat09], 首次将零知识证明系统扩展到了量子场景，他考虑的是验证者能够访问可信的多项式时间量子设备的情形。随后，研究表明，在某些密码学假设下，QMA 中的所有问题都存在零知识证明系统 [BJSW16, BJSW20, BG22] （同样假设验证者拥有可信的多项式时间量子计算能力）。针对完全经典的验证者，人们提出了几种方案。Vidick 和 Zhang 证明，可以使论证协议满足零知识性质 [VZ20]。Cr´epeau 和 Stuart [CS23] 最近的工作为 NP 提供了一个双证明者、单轮零知识证明系统。Chiesa、Forbes、Gur 和 Spooner 的工作为 NEXP 提供了一个双证明者零知识证明系统 [CFGS18], ，不过，他们的工作需要多项式数量的交互轮次。Grilo、Yuen 和 Slofstra [GSY19] 的工作表明，任何适用于 MIP* 的证明系统都可以通过增加四名额外证明者而实现零知识。尽管这些工作为研究 OTS 模型中的零知识证明系统提供了启发，但据我们所知，它们并未直接解决我们关于零知识的核心问题。事实上，根据当前最先进的研究成果，一个尚未解决的开放问题 [Gri19] 是：“是否存在一个具有两名证明者和一名经典验证者的相对论零知识证明系统来处理 QMA？”我们强调，我们的 OTS 模型将这个问题进一步推进，要求其中一名证明者以通用方式运行，且独立于问题实例。

1.1.3 量子计算的委托

委托量子计算使计算能力较弱的经典客户端能够将计算任务委托给不可信的多项式时间量子服务器。在某些条件下，交互式证明系统可以直接导出一种委托量子计算协议。通常，若交互式证明系统刻画了例如，有界错误量子多项式时间，并且证明者在给定见证后能够高效计算；此外，有界错误量子多项式时间 见证的使用方式也很重要：我们需要能够缩小证明系统的规模，从而实现针对有界错误量子多项式时间 （例如， [Gri19]）[3]的委托协议。上述概要同样适用于多服务器场景。需要注意的是，由于交互式证明系统与委托量子计算的模型颇为相似，我们有时会将二者混为一谈——使用复杂性类的缩写来指代证明者与验证者之间的交互模式——但我们强调，在委托量子计算协议中，服务器始终受到计算能力限制（而交互式证明系统中的证明者则不受此限）。

遵循 Reichardt、Unger 和Vazirani [RUV13], 展示了在MIP*设置下的委托量子计- 算，取得了很大进展，旨在改进参数和技术；尽管做出了这些努力，据我们所知，现有工作中没有一项适用于我们的模型。这里值得注意的是 [CGJV19] 的工作，它使用准线性 资源服务于两台 服务器，并且至多实现了常数轮复杂度，以及 [Gri19] 的工作，它是首个用于委托量子计算的双服务器、单轮（相对论）协议，但使用了两台服务器的全部多项式级资源。

我们注意到，在 [RUV13], 的协议以及大多数相关工作中，我们都有这样的性质：委托量子计算的协议可以扩展 为针对 QMA 的交互式证明系统，具体如下。我们让无界证明者推导出一个 QMA 见证，然后对 QMA 验证者的电路应用委托协议，其中 另一个 证明者对见证执行计算，该见证由初始证明者通过量子隐形传态发送（并且量子隐形传态测量的结果会报告给验证者）。通过这种方式，我们可以将针对QMA 的交互式证明系统与用于委托量子计算的双证明者协议密切联系起来。

1.2 技术背景

我们现在介绍量子多证明者交互式证明系统、委托量子计算和零知识证明系统领域中两种近期取得巨大成功的技术：自检 和量子可模拟码。这些技术对我们的工作至关重要。

1.2.1 自检

自测试（也称为设备无关性）是研究MIP* 以及相关委托协议时一种无处不在且功能强大的技术。Mayers 和Yao [MY04]首次提出了这一概念。非正式地说，当某一状态/测量（或其等价版本）是获得最大接受概率所必需的时，某个协议就对该特定状态或测量进行自测试。最广为人知的例子是被称为 CHSH博弈和魔方游戏 [CHSH69, Mer90, Per90,Tsi93]的非局部博弈。随后，大量工作加深了我们对自测试及其在委托量子计算中的应用的理解，例如 [MYS12, McK17,Col17, CRSV18, CGJV19, NV17, NV18]。

上述许多研究成果的出现，某种程度上早于互补的数学形式化以及对自检基本性质的仔细考察。目前，将其形式化的方法

[3]有界错误量子多项式时间在补运算下封闭，因此这对于委托而言已足够

自检使用群的近似表示理论以及 C^*-代数 [Slo19，Slo16， MPS21], 以及关于自检的各种非常基础的问题直到最近才被提出并得到研究 [CMMN20， MNP21， MS23]。这些形式化方法，尤其是其中具有实际操作价值的近似 版本利用了Gowers和Hatami提出的一个关键稳定性结果，该结果使我们能够将近似表示与精确表示联系起来 [GH17]。

1.2.2 可模拟码

Grilo、Yuen 和 Slofstra 的近期工作 [GSY19], 以及 Broadbent 和 Grilo [BG22]提出了可模拟码这一概念，将其作为在量子场景中建立零知识证明系统和协议的工具。其思想是利用量子纠错码中的技术，创建一个用于验证过程的“可模拟”见证或证明。这里的见证之所以是可模拟的，是因为存在一种高效的经典算法，能够在任何足够小的子空间上重现该见证的局部密度矩阵描述。这是建立零知识的关键工具，而该技术的应用包括开发一种验证协议（或者在 [BG22] 的情况下称为验证电路），用于验证此类可模拟见证；随后可以将其应用于将例如，一个用于 QMA 的见证编码 [BG22]。

我们注意到，将可模拟码视为用于编码量子态的工具时，才能最好地体会其全部威力：得益于此类编码，我们得以实现这样一种情形：局部描述易于计算，而全局关联却可能难以计算——这种情形在经典世界中没有对应，因为一系列局部描述可以轻而易举地定义一个全局描述。

1.3 贡献

现在，我们将从概念层面进一步详细介绍我们的模型及其动机，并概述我们的主要贡献。

1.3.1 模型

如前文所述，我们关注于对近期证明验证以及量子计算委托进行建模。为此，我们提出了一种特别适用于量子场景的新范式：验证者能够访问 OTS设备。为阐明这一模型，考虑复杂性类 QMA对以下情形进行建模：验证者能够访问完全可信的多项式时间量子计算。虽然这样的验证者对证明者持怀疑态度（因此需要独立验证所声称的证明），但在量子情形下，还可能存在更高层次的怀疑，即验证者的量子处理过程是不可信的。在这种情况下，一种常见的解决方案是假定存在两个 （或更多）不可信且全能的设备，并配备一个经典验证者；这就是 MIP* 所研究的领域。在本文中，我们提出了一种以非对称方式对待证明者的新范式。我们从一个传统的双证明者交互式证明系统出发，要求只有一个证明者承担繁重的工作（利用其无界的计算能力），而第二个证明者则变得高效且完全通用（为保证完备性，这个证明者甚至不需要获得有关手头任务的描述；然而，对于两个 无界证明者，可靠性仍得到了证明）。

我们将 OTS 表示为以下模型中所有语言 L 的集合：这些语言可以在常数完备性-可靠性差距下被判定。在选择实例 $x \in L$ 之前，经典验证者会获得一个不可信的现成设备，该设备仅取决于参数 n，参数表示问题实例的大小（不失一般性，我们可以假设证明者提供这样的 OTS 设备）。为保证完备性，这样的设备会与量子证明者共享一个纠缠态 $|\psi\rangle_n$，并声称能够从预先确定的列表中执行高效测量

可用选项中的。验证者可以选择任意选项 $x \in L$ 前提是 $|x| \leq n$ 并且同时向证明者和设备各使用一个问题；随后，验证者根据回答决定是否接受。我们强调，一次性设备证明系统同时能够抵御无界证明者和无界 OTS。

我们注意到 OTS 是 MIP* 的一种细化，因此包含于其中。反过来，OTS 模型是 交互式证明系统的一种推广，其中原本的经典验证者额外拥有对一个小型现成量子设备的 1 轮查询访问权限。总之，我们有以下直接的包含关系（另见图 2）

$$\mathsf{AM} \subseteq \mathsf{OTS} \subseteq \mathsf{MIP}^* \tag{1}$$

在经典证明系统中，一个OTS 可以被理解为与实例无关的硬件令牌。该设备可用于为NP [GMW91]的零知识证明系统提供承诺；此外，OTS 的一次性属性可以被用作不经意传输设备，进而为NP [Kil88]提供非交互式零知识证明系统。我们注意到，在量子情形下，我们的模型要求验证者是完全经典的，因此QMA [BJSW16、BG22] 在 OTS 模型中的情形要复杂得多，并且上述NP 证明系统的经典验证者类比并不直接适用。其他基于将 OTS 用作一次性存储器的方法 [BGS13] 也因我们要求验证者是完全经典的这一事实而陷入困境。

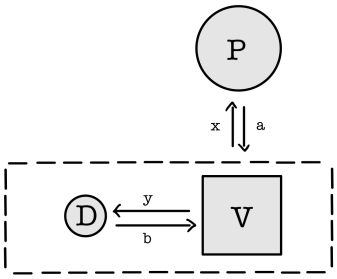

图2：现成（OTS）证明系统。 P 是量子证明者， V 是经典验证者， D 是一个简陋的现成设备；每条箭头表示一条经典消息。我们可以将该模型等价地理解为对 AM 中验证者的强化（V 可访问一个额外的 OTS 设备 D），或对 MIP* 的弱化（其中一名证明者 D受到严格限制）。

1.3.2 面向 QMA 的 OTS 证明系统

我们的第一个结果是，QMA 中的任何语言也属于 OTS。对此结果的一种理解是：从一个针对 QMA 的传统证明系统出发，我们可以将验证者在量子验证过程中始终不变的信任，转换为一个具备两个新特征的经典验证者：（1）验证者可以访问一个不受信任且与实例无关的现成量子设备；（2）验证者与证明者（以及设备）进行单轮同时交互。总而言之，我们得到：

定理1.1。 （作为定理 *7.2*） $\mathsf{QMA} \subseteq \mathsf{OTS}$。

1.3.3 用于 QMA 的零知识 OTS 证明系统

此外，我们还证明了 QMA 的 OTS 证明系统也是统计零知识的，这意味着我们可以在经典多项式时间内模拟验证者的交互记录（在交互过程中）

与处于肯定实例中的证明者一起。

定理 1.2。 （重述于定理 7.2）对于每个属于 L 的 QMA语言 L，都存在一个针对 L的统计零知识 *OTS* 证明系统。

1.3.4 OTS 模型中的委托量子计算

作为最后一项概念性贡献，我们展示如何将针对QMA （定理 1.1）的 OTS 证明系统改造为适用于委托量子计算的场景（见第 1.1.3 节）；请注意，上文所述的零知识性质也适用于委托量子计算范式。

定理 1.3。 （重述于定理 7.3）有界错误量子多项式时间 在 *OTS* 模型中具有一个满足统计零知识性质的相对论式委托量子计算协议。

我们认为，这一结果影响尤为深远，因为它提出了一种新的委托量子计算模型，相较于现有的委托协议具有明显的概念优势：

1. 将我们的委托量子计算协议与单服务器协议进行比较时，可以看到我们额外假设存在一台现成且隔离的设备。不过，其优势在于：

   (a) 我们针对计算能力不受限的服务器实现了可靠性；现有的单服务器、经典客户端委托协议需要计算假设 [Mah18]。（b）客户端完全不信任任何 量子设备；现有的用于委托量子计算的单服务器统计安全协议需要信任一个小型量子制备设备 [Bro18，FK17]。

2. 将我们的委托量子计算协议与现有的多服务器（MIP*）协议进行比较，我们注意到：

   (a) 我们的方法只需要一台负责处理大部分计算的高性能量子服务器，以及一台高效且通用的辅助设备；后者甚至不需要获知问题实例的描述。这具有实际优势，尤其是考虑到该现成设备可以在验证阶段之前购得（图1）。(b) 我们的方法只需单轮通信，这意味着可以采用相对论手段来强制实现隔离。唯一已知的其他相对论协议要求两台服务器都具备完整的量子计算能力，并且不是零知识 [Gri19]。

1.4 证明方法与技术贡献

下面我们概述证明主要结果的方法，包括对主要技术贡献的非正式陈述。

1.4.1 直接方法面临的障碍

在双服务器或多服务器模型中委托量子计算时，经典验证者能够指挥量子证明者 [RUV13] 使用两个相互交织的测试：(1) 计算测试，其接受概率取决于所要求的量子计算（例如，基于隐形传态的计算 [RUV13] 或对局部哈密顿量进行能量检验 [Ji17， Gri19]）；(2) 刚性测试，

确保证明者的操作处于已知范围内（例如，通过 CHSH 博弈或泡利编织测试进行自检）。为确立零知识性质，我们必须证明，证明者的回答可以由经典概率多项式时间（PPT）设备模拟。通常，用于刚性测试的方法可以直接模拟，因此在这种设置下，实现零知识的难点在于模拟能量测试。此外，即使这两种测试单独来看都可模拟，也不能保证零知识性质，因为恶意验证者可能在单轮中提出分别来自不同测试的问题对。

Grilo [Gri19] 提出了一个由"XZ型"$\mathcal{G}(H)$ 哈密顿量[4] 所确定的博弈 H。该博弈的诚实证明者共享足够多的 EPR 对，其中一名证明者私下持有 H的基态。博弈 $\mathcal{G}(H)$ 将能量测试与泡利编织测试 [NV17、Vid18]相结合。在能量测试中，一名证明者报告随机选取项的测量结果 H_i ，该测量在其一侧的 EPR 对上进行；另一名证明者则提供在另一批 EPR 对和基态上进行贝尔基测量所得的隐形传态密钥。将能量测试与泡利编织测试结合起来，可以使验证者确保证明者共享 n EPR 对，并且在测量局部项时执行所需的泡利 X/泡利 Z 测量 H_i。

获得双证明者零知识证明系统的一种直接方法，是结合关于可模拟码的最新结果，使 Grilo 能量测试中的测量结果可模拟。更具体地说，可以利用 [BG22]中给出的可模拟验证电路族，应用众所周知的电路到哈密顿量构造。对于这样的电路 V，已有研究证明，对应哈密顿量 H_V基态上的局部测量是可模拟的，因此这种方法可以使能量测试的结果可模拟。不幸的是，这种方法因两个技术原因而行不通。

编码的选择。首先，不能采用先前已知的自检技术来证明参与者会在给定于 [BG22]中的可模拟基态上执行所需的测量。一方面，先前研究的单轮自测试技术只能用于证明参与者执行泡利X和泡利 Z 测量。另一方面，Broadbent 和 Grilo 在编码逻辑门时所使用的物理门的选择，可能导致得到的局部哈密顿量并非 XZ型，因此局部项 H_i 可能需要使用尚无已知自检方法的测量。

测量的规模。 第二个障碍源于这样一个事实：在这种设置下，现有的刚性测试要求两位参与者都对其共享态进行大规模测量。这些大规模测量可能为恶意验证者提供攻击途径，从而危及零知识性质。具体而言，由于泡利编织测试允许请求对所有量子比特进行测量，恶意验证者可以告知一位参与者当前进行的是能量测试，同时请求对大量量子比特执行泡利-X 和泡利-Z 测量。这样的测量结果无法使用可模拟码进行模拟，因为可模拟码只能防护常数规模测量，因此这会危及零知识性质。

1.4.2 证明与技术结果概述

为了修正编码的恰当选项，我们证明可以使用 [GSY19] 提出的可模拟码方法，重新构建 Broadbent 和 Grilo 给出的验证电路。这一改变使我们能够使用另一组物理门来编码 Broadbent 和 Grilo 给出的验证电路中的逻辑门，因此我们证明

[4] 这些是哈密顿量，其中每个局部项 H_i 是泡利-X和泡利-Z 算子的张量积的实线性组合。

局部哈密顿量 nian corresponding to the 电路 is of XZ-type, while preserving simulatabilit y.

定理 1.4 （定理 6.1的非正式版本）。对于 QMA 中的任意语言 $L = (L_{yes}, L_{no})$，存在一族验证电路 V_x，满足：（*1*）对 V_x 应用电路到哈密顿量构造，会得到一个 XZ 型的哈密顿量 H_x；（*2*）如果 $x \in L_{yes}$ 存在一个多项式时间算法，能够近似通过对 H_x 的基态进行偏迹、舍弃除 *6* 个量子比特以外的所有量子比特而得到的约化密度矩阵。

为克服大规模测量问题[5], 我们引入一种新的自检，称为低权重*Pauli*编织测试（LWPBT），它可以对低权重泡利测量的张量积和 n EPR 对进行自检，但只要求参与者在恒定数量的量子比特上进行测量。

定理 1.5 （推论的非正式版本4.10）。低权重 *Pauli* 编织测试可以对 n *EPR* 对和 6 量子比特泡利测量进行自检。此自检具有鲁棒性，即任何ε-完美策略都必须与规范策略相差不超过 $poly(n)\sqrt{\varepsilon}$。

我们采用群论方法来证明 LWPBT 的刚性。这里简要介绍实现这一结果所面临的挑战。我们的证明涉及群的近似表示和近似同态。非正式地说，给定群的一个表示$\langle S : R\rangle$，对于群 G，若映射 $f : S \to \mathscr{U}$ 从生成集 S 映射到酉算子集合 $\mathscr{U}$，并且以误差 ε满足中的关系， R则称其为一个 ε-表示。更一般的 ε-同态是指映射 $f : G \to \mathscr{U}$ 在误差 ε范围内保持群中元素的乘法。当 $\varepsilon = 0$ 时，这两个概念一致。著名的 Gowers-Hatami 定理 [GH17]指出，有限群的每个近似同态都必定接近某个精确同态。

在 [Vid18] 关于 n-量子比特泡利编织测试的刚性证明中，隐含地采用了一个 n-量子比特 Weyl-Heisenberg 群的表示，该群有 $exp(n)$ 个生成元，并受 $exp(n)$ 个关系约束。随后证明，任意 ε-完美策略都会形成一个 $O(\sqrt{\varepsilon})$-近似表示；鉴于该表示的规模很大，可以直接证明这个近似表示确实是一个 $O(\sqrt{\varepsilon})$-近似同态。

LWPBT 的分析需要为 n量子比特 Weyl-Heisenberg 群提供一种表示，其中仅有 $poly(n)$ 个生成元和 $poly(n)$ 个关系。生成元和关系较少，使得刚性分析更加复杂。具体而言，为了证明近乎完美策略所给出的近似表示确实是近似同态，我们需要针对这一“精简”表示指定 Weyl-Heisenberg 群的标准形式，并找到一种重写过程，将群中的任意词转化为其标准形式。这样便能跟踪所得到的近似同态的精确误差界，并得出结论：任何 ε-完美策略都会构成一个 $poly(n)\sqrt{\varepsilon}$-近似同态。

为了最终将近似同态修正为精确同态，我们进一步推进了对有限群稳定性的前沿理解。具体而言，在定理 4.1 中，我们陈述并证明了 Gowers-Hatami 定理的一个增强版本，可用于 Weyl-Heisenberg 群的稳定性分析。除了适用于我们的场景之外，这个新版本还可以简化以往的自检方法。简而言之，在由近似同态构造精确同态时，我们的增强版本允许忽略无关的子表示，而无需截断 Gowers-Hatami 定理给出的等距映射。这一改进有助于澄清一些微妙问题，因为一般来说，截断等距映射可能会使其不再是等距映射。

[5] In 第 4.3 节讨论应对大型测量问题的其他潜在方法 .

定理 *1.6*（定理*4.1* 的非正式表述）。若 f 是有限群 G 在某个希尔伯特空间 H 上的近似同态，则存在希尔伯特空间 K、等距映射 $V: H \to K$，以及 G 在 K 上的一个精确同态 ϕ，使得 $V^*\phi V$ 与 f 接近。此外，若 f 在给定子群 S *of* G 上限制为一个表示，且不可约表示 ξ 在 $f|_S$ 中的傅里叶系数为零，则 ξ 在 ϕ中的支撑为零。

我们使用上述技术结果，推导出一个改进版本的 [Grilo19] ，其通过交错执行以下测试构成：(1) 一个计算测试，由一次能量测试组成，其中可模拟的见证使用低权重 Pauli-X 和 Pauli-Z 测量；(2) 一个刚性测试，由 LWPBT 构成。这个改进版 Grilo 协议的结果是一个具有逆多项式完备性-可靠性间隙的零知识 OTS 协议。最后，我们将阈值并行重复定理应用于上述协议，将完备性-可靠性间隙放大到常数，从而证明定理 1.1 和定理 1.2。随后，我们证明该证明系统具有一种形式，可以缩减规模以得到一个委托协议，从而证明定理 1.3。

1.5 未解决的问题

在这项工作中，我们展示了 OTS 模型具有许多有趣的性质，这些性质与交互式证明的单证明者模型和多证明者模型都相关。我们相信，对该模型进行进一步研究具有巨大的空间，而且我们的新颖技术也将在其他领域找到应用。下面列出一些尚未解决的问题。

要恢复 MIP*，两个证明者都必须拥有全知全能的能力吗？ 我们的结果表明，QMA $\subset$OTS。至于更大的复杂性类（如 QIP）是否也能如此，仍是一个悬而未决的问题。进一步而言，或许可以刻画不可信的设置阶段设备需要具备多强的能力，才能恢复所有 MIP*。更具体地说，如果允许不可信设备进行任意测量，但仍要求其独立于输入，我们能否恢复 MIP*？与这个问题有些对偶的是，能否为我们的新模型证明一个自然的上界。一个看似合理的候选是 QIP，但即便如此，也并非显而易见，原因之一是现成设备可能与证明者共享任意数量的纠缠。

量子知识证明的应用。作为零知识（ZK）概念的扩展，在知识证明（*PoK*）中，验证者还会确信证明者“知道”一个可接受的见证。形式上，这通过证明存在一个高效的知识提取器来实现：该提取器可通过预言机访问证明者并输出一个见证；这一概念近期已扩展到量子场景 [BG22], [CVZ19]。我们猜想，自测试所提供的保证为使验证者确信证明者确实持有量子见证提供了另一种途径；通过针对更完整的博弈给出结果，或许可以进一步完善我们的自检方法。具体而言，我们将寻找一种双证明者、单轮协议，使其能够对局部哈密顿量的基态进行自测试，并确定这如何为量子知识证明（PoK）提供一种新方法，作为一个悬而未决的问题。

用于委托量子计算的OTS设备。 我们已经证明，OTS 模型足以支持有界错误量子多项式时间中的委托量子计算；尽管看起来我们不太可能完全摆脱 OTS 设备 [ACGK19], 一个开放问题是确定该设备所需的最小 能力（假设有界错误量子多项式时间 $\neq$ BPP）。

LWPBT的进一步用途和改进。我们认为，新的 LWPBT 可能具有更广泛的适用性，因为它或许可以进一步推广，从而在针对 EPR对和泡利测量的自检中，为问题/答案大小与鲁棒性之间提供一种直接的权衡。例如，可以分析与我们主要结果中相同的博弈，但允许测量大小为 $\log(n)$ ，而不是常数。我们将这一模型及其影响留待未来研究。

进一步应用。除了我们所研究的内容之外，交互式证明系统在量子场景中还有各种有趣的应用和需要考虑的问题。近期的研究引入了态/酉复杂性类的概念 [RY22]。非正式地说，这种方法旨在研究高效量子验证者在获得不受信任的量子证明者访问权限的情况下，输出目标量子态的能力。在我们的OTS 模型中也可以作出类似考虑：经典验证者可能希望证明不受信任的设置阶段设备的寄存器上存在目标量子态。

1.6 致谢

我们感谢 Seyed Sajjad Nezhadi、Gregory Rosenthal、William Slofstra、Jalex Stark 和 Henry Yuen 就该模型展开讨论。我们感谢 Alex Grilo 就部分证明技术展开讨论。我们还感谢 Thomas Vidick 就定理 4.1 的表述和证明进行了详细讨论。我们感谢匿名审稿人建议将 OTS 用于经典证明系统。

本工作得到 Mitacs Accelerate计划 IT24833 的支持，该项目与产业合作伙伴 Agnostiq 合作，在线地址为 agnostiq.ai。A.B. 获得空军科学研究办公室项目编号 FA9550-20-1-0375、NSERC 以及渥太华大学研究讲席计划的支持。

1.7 概要

本文的其余部分安排如下。我们在第 2 节介绍所需的预备知识。在第 3 节中，我们介绍低权重 Pauli 编织测试，并在第 4 节证明该测试的刚性性质。第 4 节还陈述并证明 Gowers-Hatami稳定性结果的增强版本。在第 5 节中，我们给出 Grilo [Gri19] 首先提出的哈密顿量博弈的一个修改版本，并证明该博弈的完备性和可靠性。在第 6 节中，我们介绍可模拟码的相关背景，并将其应用于第 5 节概述的博弈，以确定适用于QMA的 OTS 证明系统。在第 7 节中，我们介绍并形式化定义 OTS 模型，并展示前述各节的技术贡献如何汇聚起来，从而证明全部三个概念性结果。

2 预备知识

我们介绍本文所用的记号，并对群的表示论、非局域博弈和零知识 MIP* 协议等主题进行背景讨论。我们还定义若干相关的复杂性类。

2.1 记号

我们用 $[n]$ 表示集合 $\{1,\dots n\}$。给定两个实值函数 $f,g\colon \mathbb{R}\to\mathbb{R}$，若存在一个正实数 M 和一个 $x_0\in\mathbb{R}$，使得对所有 $x\geq x_0$都有$|f(x)|\leq Mg(x)$（分别为 $|f(x)|\geq Mg(x)$），则记作$f=O(g)$（分别记作 $f=\Omega(g)$）。我们称函数 f为可忽略函数，并记作$f=\mathrm{negl}(n)$；若对所有常数 $c>0$，均有 $f=O(n^{-c})$。对于有限集合 X 上的两个分布 P和 Q， P与 Q之间的统计差异定义为 $\sum_{x\in X}|P(x)-Q(x)|$。

在本文中，所有希尔伯特空间都是有限维的。给定一个希尔伯特空间$\mathcal{H}$，我们用 $\mathscr{B}(\mathcal{H})$表示作用于$\mathcal{H}$上的有界线性算子集合，用 $\mathscr{U}(\mathcal{H})$ 表示$\mathcal{H}$上的酉算子群，并用$\mathbb{1}_{\mathcal{H}}$ 表示$\mathcal{H}$上的单位算子。给定一个算子 $A\in\mathscr{B}(\mathcal{H})$

我们用 A^* 表示伴随算子（等价地，共轭转置），并定义迹范数 $\|A\|_{tr}$ ： $=\mathrm{Tr}\sqrt{A^*A}$。

2.2 量子信息

H 上的量子态 ρ 是 $\mathscr{B}(\mathrm{H})$ 中满足 $\mathrm{Tr}(\rho) = 1$ 的正算子。它在 $\mathscr{B}(\mathrm{H})$ 上诱导一个半范数$\|A\|_\rho$ ： $= \sqrt{\|A^*A\rho\|}$ ，我们称之为 ρ-范数。该范数是左酉不变的，这意味着对于所有 $U \in \mathscr{U}(\mathrm{H})$ 和 $A \in \mathscr{B}(\mathrm{H})$， $\|UA\|_\rho = \|A\|_\rho$。给定两个量子态 ρ 和 σ，我们定义它们的迹距离 $D(\rho,\sigma)$ $= \frac{1}{2}\|\rho-\sigma\|_{tr} = \max_P \mathrm{Tr}(P(\rho-\sigma))$，其中最大值取遍所有投影算子 $P \in \mathscr{B}(\mathrm{H})$。

我们使用 $|\Phi_{\mathrm{EPR}}\rangle$ 表示 $\mathbb{C}^2 \otimes \mathbb{C}^2$ 中的 EPR 对，并使用$|\Phi^{\otimes n}{}_{\mathrm{EPR}}\rangle$ 表示 n-量子比特 EPR对。我们还用 σ_I、 σ_X 和 σ_Z表示以下泡利算子:

$$\sigma_I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \sigma_X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \text{ and } \sigma_Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{2}$$

对于每个 $a \in \{0,1\}^n$ 以及 $W \in \{I、 X、 Z\}^n$，我们用 $\sigma_W(a)$ 表示作用于 $\otimes_{i\in[n]}\sigma_{W_i}^{a_i}$ 上的算子($\mathbb{C}^2)^{\otimes n}$ ，其中 $\sigma_I^0 = \sigma_X^0 = \sigma_Z^0 = \sigma_I$。量子计算中这些门以及其他基本概念的定义可见 [NC00]。

量子电路族一个酉量子电路 就是一个可以写成某个通用门集$\mathcal{U}$中的门之乘积的酉算子。除非另有说明，我们将假设通用门集是以下通用门集$\{H, \Lambda(X), \Lambda^2(X)\}$，其中， H 是哈达玛门， $\Lambda(X)$ 是受控 σ_X 门，而 $\Lambda^2(X)$ 是托福利门。一个一般量子电路 或简称量子电路是一个酉量子电路，它还可以应用非酉门，这些门可引入初始化为0状态的量子比特、对量子比特进行迹运算，或在标准基下测量量子比特。

定义 2.1(多项式时间一致电路族)。 我们称量子电路族$\{Q_n\}_{n\in\mathbb{N}}$ 是多项式规模量子电路族，如果存在多项式 r 使得 Q_n的规模至多为 $r(n)$。量子电路族 $\{Q_n\}$称为多项式时间一致族，如果存在一个多项式时间图灵机，在输入 1^n 时输出 Q_n的描述。在这种情况下，该族也将是多项式规模量子电路族。

给定一个量子电路 Q，我们用 $|Q|$表示其规模（门数和线路数）。委托计算 Q 的任务可由以下承诺问题描述:

定义 2.2 (Q-CIRCUIT)。输入是一个量子电路 Q 在 n 量子比特上。问题是要在以下两种情况之间作出判断:

- ***Yes.*** $\|((|1\rangle\langle 1| \otimes I_{n-1})Q|0^n\rangle\|^2 \geq 1-\gamma$
- ***No.*** $\|((|1\rangle\langle 1| \otimes I_{n-1})Q|0^n\rangle\|^2 \leq \gamma$

当我们被告知这两种情况之一成立时。

定义中的问题2.2 已知对于 $1-2\gamma >$ [1] 多项式(n)是有界错误量子多项式时间完全的。

2.3 群与表示

在本文中，我们研究群及其（近似）表示。我们用 1 表示群中的单位元，并用 $[g,h] := ghg^{-1}h^{-1}$ 表示群交换子。若一个群包含有限个元素，则称其为有限群。群 G 在希尔伯特空间 H 上的（酉算子）表示 $\phi: G \to \mathscr{U}(\mathrm{H})$，是从 G 到 $\mathscr{U}(\mathrm{H})$ 的群同态。若子空间 $\mathrm{K} \subset \mathrm{H}$ 满足 $\phi(G)\mathrm{K} := \{\phi(g)|k\rangle : g \in G, |k\rangle \in \mathrm{K}\} = \mathrm{K}$，则称其为 ϕ 的不变子空间。如果一个表示没有非零真不变子空间，则称其为不可约。设 $\phi_1 : G \to \mathscr{U}(\mathrm{H}_1)$ 和 $\phi_2 : G \to \mathscr{U}(\mathrm{H}_2)$ 是群 G的两个表示。若存在酉算子 $U: \mathrm{H}_1 \to \mathrm{H}_2$，使得对所有 $g \in G$，$U\phi_1(g)U^* = \phi_2(g)$，则称 ϕ_1 和 ϕ_2 酉等价。ϕ_1和 ϕ_2的直和记为 $\phi_1 \oplus \phi_2$，它是群 G在 $H_1 \oplus H_2$上的一个表示，将 $g \mapsto \phi_1(g) \oplus \phi_2(g)$。马施克定理指出，有限群 G 的每个表示 ϕ 都酉等价于 G的一组不可约表示 $\{\phi_i : 1 \le i \le k\}$ 的直和。在这种情况下，我们称 $\bigoplus_{i=1}^{k} \phi_i$ 是 ϕ的不可约分解，而每个 ϕ_i 都是 ϕ的不可约分量。

对于有限群 G，我们用 $\mathrm{Irr}(G)$ 表示完备的不等价不可约表示集（其中的元素在酉等价意义下唯一）。不失一般性，我们假设每个 $\varphi \in \mathrm{Irr}(G)$ 都是作用于 $\mathbb{C}^{d_\varphi}$ 上、以标准基$\{|i\rangle$ 为基的表示: $i \in [d_\varphi]\}$。众所周知，

$$\sum_{\varphi \in \mathrm{Irr}(G)} d_\varphi \mathrm{Tr}\Big(\varphi(g)\Big) = \begin{cases} |G| & \text{if } g = 1, \\ 0 & \text{otherwise.} \end{cases}$$

给定有限群 G、函数 $f: G \to \mathscr{U}$（$\mathcal{H}$）以及不可约表示 $\phi: G \to \mathscr{U}$（$\mathbb{C}^d$），f 的傅里叶变换在 ϕ 处是一个算子

$$\widehat{f}(\phi) := \frac{1}{|G|} \sum_{g \in G} f(g) \otimes \overline{\phi(g)} \tag{3}$$

作用于 $\mathcal{H} \otimes \mathbb{C}^d$，其中 $\overline{\phi(g)}$是矩阵 $\phi(g) \in M_d(\mathbb{C})$ 在标准基下的共轭矩阵。

令 $f: G \to \mathscr{U}(\mathrm{H})$ 为有限群 G的一个函数。给定 H上的量子态 ρ 和一个正实数 ε，如果对于所有 $g \in G$，$f(g^{-1}) = f(g)^*$ 且$\frac{1}{|G|}\sum_{h \in G} \| f(g)f(h) - f(gh)\|_\rho^2 \le \varepsilon$，我们称 f 是一个 (ε, ρ)-同态。在这种情况下，根据著名的Gowers-Hatami 定理 [GH17，Vid18], 存在一个希尔伯特空间K、一个等距映射 V: $\mathrm{H} \to \mathrm{K}$，以及一个表示$\phi: G \to \mathscr{U}(\mathrm{K})$，使得对于所有 $g \in G$，$\| f(g) - V^*\phi(g)V \|_\rho \le \varepsilon$。在第4.1 节中，我们介绍了该定理的一个增强版本，该版本允许我们忽略 Weyl-Heisenberg 群的所有一维不可约表示。早期的工作通过调用Gowers-Hatami 定理给出的等距映射的截断来处理这些一维表示。遗憾的是，一般而言，对等距映射进行截断可能会导致其不再是等距映射。

我们还研究群表示。给定集合 S，我们用 $\mathrm{F}(S)$ 表示由 S生成的自由群，并用$S : R$表示将 $\mathrm{F}(S)$ 对由 R 生成的正规子群取商所得的商群。我们称 $S : R$ 由 S 生成，并满足关系 R。当 S 和 R 都是有限集时，我们称群 $S : R$ 是有限表示的。给定群 $G = S : R$，关于 S 的 G 的正规形式是从 G 到 $S \cup S^{-1}$ 上的词的一个单射函数 N，使得对于所有 $g \in G$，$\mathrm{N}(g) = g$ 于 G 中。

2.4 非局域博弈与刚性

一个双玩家[6] 单轮非局域博弈$\mathcal{G}$是一个元组 $\Big(\lambda, \mu, \mathcal{I}_A, \mathcal{I}_B, \mathcal{O}_A, \mathcal{O}_B\Big)$，其中 $\mathcal{I}_A$、$\mathcal{I}_B$是有限输入集，$\mathcal{O}_A$、$\mathcal{O}_B$是有限输出集，μ是在 $\mathcal{I}_A \times \mathcal{I}_B$上的概率分布，且

[6]这两位玩家通常被称为 Alice 和 Bob。

$\lambda : \mathrm{O}_A \times \mathrm{O}_B \times \mathrm{I}_A \times \mathrm{I}_B \to \{0, 1\}$决定胜负条件。博弈G的量子策略 S由有限维希尔伯特空间 H_A 和 H_B、单位向量 $|\psi\rangle \in \mathrm{H}_A \otimes \mathrm{H}_B$、$\mathrm{H}_A$上的 Alice 的POVM$\{E_a^x : a \in \mathrm{O}_A\}$、$x \in \mathrm{I}_A$，以及 H_B上的 Bob 的POVM$\{F_b^y : b \in \mathrm{O}_B\}$、$y \in \mathrm{I}_B$给出。S 在博弈 G 中的获胜概率为

$$\omega(\mathcal{G}, \mathcal{S}) := \sum_{a,b,x,y} \mu(x, y)\lambda(a, b|x, y)\langle\psi|E_a^x \otimes F_b^y|\psi\rangle.$$

若非局域博弈$\mathcal{G}$ 的量子策略$\mathcal{S}$ 满足 $\omega(\mathcal{G},\mathcal{S}) = 1$，则称其为完美的。若上下文中的博弈明确，我们就简写为 $\omega(\mathcal{S})$ 来表示获胜概率。非局域博弈$\mathcal{G}$ 的量子值定义为

$$\omega^*(\mathcal{G}) := \sup\{\omega(\mathcal{S}) : \mathcal{S} \text{ a quantum strategy for } G\}.$$

本文假设量子策略中使用的所有测量都是投影值测度（PVM）。一个m结果的投影值测度$\{P_1, \cdots, P_m\}$ 对应一个可观测量 $\sum_{j\in[m]} \exp(\frac{2\pi i}{m} j)P_j$，因此，博弈 $\mathcal{G} = \left(\lambda, \mu, \mathcal{I}_A, \mathcal{I}_B, \mathcal{O}_A, \mathcal{O}_B\right)$ 的量子策略也可以由三元组表示

$$\mathcal{S} = (\tau^A, \tau^B, |\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B)$$

其中 $\tau^A(x)$、$x \in \mathcal{I}_A$是作用于$\mathcal{H}_A$上的$\mathcal{O}_A$结果可观测量，而 $\tau^B(y)$、$y \in \mathcal{I}_B$是作用于$\mathcal{H}_B$上的$\mathcal{O}_B$结果可观测量。

这里我们介绍著名的梅明-佩雷斯魔方游戏。在该游戏中，Alice 和 Bob 试图说服验证者相信，他们找到了一个方程组的解，该方程组定义在 $\mathbb{Z}_2$上。共有 9 个变量 v_1、…、v_9，排列在一个 3×3 阵列中，其行标记为 r_1、r_2、r_3，列标记为c_1、c_2、c_3。

	c_1	c_2	c_3
r_1	v_1	v_2	v_3
r_2	v_4	v_5	v_6
r_3	v_7	v_8	v_9

表 1：魔方游戏

每一行或每一列对应一个方程：$\{r_1, r_2, r_3, c_1, c_2\}$中的行变量或列变量之和为 0；$c_3$ 列中的变量之和为 1。每一轮中，Bob 会收到 6 个可能方程中的一个，他必须针对收到的方程给出一个满足赋值。随后，Alice 会被要求为 Bob 收到的方程中包含的某个变量提供一致的赋值。下表描述了这一方程组的一个算子解：

$$\begin{array}{lll} A_1 = \sigma_I \otimes \sigma_Z & A_2 = \sigma_Z \otimes \sigma_I & A_3 = \sigma_Z \otimes \sigma_Z \\ A_4 = \sigma_X \otimes \sigma_I & A_5 = \sigma_I \otimes \sigma_X & A_6 = \sigma_X \otimes \sigma_X \\ A_7 = \sigma_X \otimes \sigma_Z & A_8 = \sigma_Z \otimes \sigma_X & A_9 = \sigma_X\sigma_Z \otimes \sigma_Z\sigma_X \end{array}$$

表 2：魔方游戏的算子解

该博弈的典范完美量子策略是一种这样的策略，其中

- 参与者共享两个 EPR 对，

- 给定变量 v_i，Alice 在她的量子寄存器上执行 A_i，并且
- 给定一行或一列，其中包含三个变量 v_j、v_l 和 v_ℓ，Bob 对他的量子寄存器执行 $A_j A_k A_\ell$。

定义2.3.设$S = (\tau^A, \tau^B, |\psi\rangle \in H_A \otimes H_B)$ 和 $\tilde{S} = (\{\tilde{\tau}^A\}, \{\tilde{\tau}^B\}, |\tilde{\psi}\rangle \in \tilde{H}_A \otimes \tilde{H}_B)$ 是博弈 $G = \left(\lambda, \mu, I_A, I_B, O_A, O_B\right)$的两个量子策略。我们称 S与 $\tilde{S}$ 是 δ-接近的，记作 $\tilde{S} \succeq_\delta S$，如果存在希尔伯特空间 H_A^{aux}和H_B^{aux}、等距映射 $V_A : H_A \to H_A \otimes H_A^{aux}$和 $V_B : \tilde{H}_B \to H_B \otimes H_B^{aux}$，以及一个单位向量 $|aux\rangle \in H_A^{aux} \otimes H_B^{aux}$，使得

$$\|(V_A \otimes V_B)(\tau^A(x) \otimes \tau^B(y)|\psi\rangle) - (\tilde{\tau}^A(x) \otimes \tilde{\tau}^B(y)|\tilde{\psi}\rangle) \otimes |aux\rangle\|^2 \leq \delta \tag{4}$$

对于所有$(x,\ y) \in I_A \times I_B$。

魔方游戏的刚性已得到充分研究 [WBMS16]:

引理 2.4。如果 S 是魔方游戏的一个策略，且获胜概率为 $1-\varepsilon$，那么 S 与典范完美策略是 $O(\sqrt{\varepsilon})$ 接近的。

2.5 复杂性类与零知识

定义 2.5 (QMA)。承诺问题 $L = (L_{yes},\ L_{no})$ 属于QMA，如果存在多项式p 和 q，以及一个多项式时间一致的量子电路族$\{Q_n\}$，其中 Q_n 以字符串 $x \in \Sigma^*$（满足 $|x| = n$）、一个 $p(n)$量子比特的量子态 $|\psi\rangle$，以及处于状态$|0\rangle^{\otimes q(n)}$的 $q(n)$ 个辅助量子比特作为输入，使得：

- （完备性）如果 $x \in L_{yes}$，那么存在某个 $|\psi\rangle$，使得 Q_n 以至少 $1 - \mathrm{negl}(n)$ 的概率接受 $(x,\ |\psi\rangle)$，并且
- （可靠性）如果 $x \in L_{no}$，那么对于任意状态 $|\psi\rangle$，Q_n 接受 $(x, |\psi\rangle)$ 的概率至多为$\mathrm{negl}(n)$。

我们有时将电路族$\{Q_n\}$ 在定义 2.5 简称为一族验证电路。

非正式地说，如果一个语言可以由与多个 彼此隔离、全能且纠缠的证明者交互的多项式时间经典验证者判定，则该语言属于MIP*。在这项工作中，我们只处理涉及两名证明者和一轮交互的 MIP* 证明系统；其定义如下。

定义 2.6。一个承诺语言 $L = (L_{yes},\ L_{no})$ 属于 $\mathsf{MIP}^*[2,1]_{c,\ s}$ 当且仅当存在一个多项式时间可计算函数，该函数将实例 $x \in L$ 映射为一个满足以下条件的非局域博弈 G_x。

- （完备性）对于每个 $x \in L_{yes}$，我们都有 $\omega^*(G_x) \geq c$。
- （可靠性）对于每个 $x \in L_{no}$，我们有 $\omega^*(G_x) < s$。

我们将映射，$x \mapsto \mathcal{G}_x$，称为$\mathsf{MIP}^*[2,1]_{c,\ s}$证明系统，或在某些地方称为 $\mathsf{MIP}^*[2,1]_{c,\ s}$协议。当上下文中的参数明确时，我们简单地将其称为 MIP* 证明系统。

接下来，我们讨论零知识，它是证明系统的一项附加性质。直观地说，在零知识证明系统中，没有任何验证者（包括恶意验证者）能够获知超出所考虑实例所属语言成员关系以外的任何信息。对于我们的 $\mathsf{MIP}^*[2,1]$ 场景，只需对每个证明者最多发送一个有效问题的验证者进行量化（否则，我们可以要求证明者中止协议）。因此，恶意验证者只能

通过按照另一种分布采样初始问题，并自适应地采样第二个问题，从而偏离诚实策略。

更正式地，概率多项式时间恶意验证者图灵机，其输入为 x 和随机性 θ，并为 Alice 或 Bob 采样问题 q_1。给定回复 r_1后，恶意验证者以可能依赖于 q_1 和 r_1的方式采样问题 q_2。对于给定的量子策略$\mathcal{S}$和恶意验证者 $\widehat{V}$，我们将 $View(\widehat{V}(x), \mathcal{S})$ 视为对应于问题与答案交互记录 $(x, \theta, q_1, r_1, q_2, r_1)$的随机变量。当对于所有"是"实例，模拟器都能从上述分布中采样时，该协议就是零知识的。

定义 2.7。 如果对于每个 $x \in L_{yes}$，都存在一个满足以下条件的诚实证明者策略 S，则称一个MIP$^*[2,1]_{c,s}$ 证明系统是统计零知识 的：

1. $\omega^*(S) \geq c$。

2. 对任意概率多项式时间恶意验证者 V，都存在一个概率多项式时间模拟器 $Sim_{\widehat{V}}$，其输出分布与 $View(\widehat{V}(x), S)$ 的统计距离至多为 ε，其中 $\varepsilon(|x|)$是某个可忽略函数。

2.6 可模拟码和门的编码

回顾一下，量子纠错码（QECC）$\mathcal{C} = [[n,k]]$ 是一个映射 Enc : $(\mathbb{C}^2)^{\otimes k} \to (\mathbb{C}^2)^{\otimes n}$，它将一个 k 量子比特状态 $|\psi\rangle$ 编码为一个 n 量子比特状态 Enc$(|\psi\rangle)$，其中 $n \geq k$。如果原始状态可以从经过任意量子操作变换后的编码状态中恢复，而该量子操作至多作用于 $(d-1)/2$ 个量子比特，则称该编码的距离为 d。给定一个带有映射 Enc 的$[[m,1]]$ 量子纠错码（QECC），我们滥用记号，对应的 $[[mn,n]]$编码也记作 Enc；该编码通过将 Enc 应用于一个 n量子比特系统中的每个量子比特得到。

在本节中，我们用 A_n^k 表示 1 到 n 之间的 k 个不同数字的集合。于是$A^k := \bigcup_{n \geq k} A_n^k$ 是 k 个不同数字的集合。给定一个 k量子比特逻辑门 U 和一个元素$a = (a_1, \ldots, a_k) \in A^k$，令 $U(a)$ 表示作用于量子比特 $a_1, \cdots a_k$ 上的门 U。

下面我们回顾可模拟码的定义，该定义最初由 Grilo、Slofstra 和 Yuen [GSY19]提出。

定义 2.8。给定一个作用于 k 个量子比特的逻辑门 U 和一个量子纠错码 $C = [[m,1]]$，设 (σ_U, σ'_U) 为一对状态，并设 ℓ 为一个正整数。对于每个 $1 \leq i \leq \ell$，令 O_i 为一个映射，将 $a = (a_1, \cdots, a_k)$ 中的元素映射为酉算子 $O_i(a)$，它们仅作用于

(i) C 中码字对应于逻辑量子比特 $a_1, \cdots, a_k$ 的物理量子比特，以及

(ii) 保存 σ_U 的寄存器。

若元组 $(\sigma_U, \sigma'_U, \ell, O_1, \cdots, O_\ell)$ 满足以下条件，则称其为代码 C 中 U 的一个编码：

$$(\mathcal{O}_\ell(\underline{a}) \ldots \mathcal{O}_1(\underline{a}))(Enc(\rho) \otimes \sigma_U)(\mathcal{O}_\ell(\underline{a}) \ldots \mathcal{O}_1(\underline{a}))^* = Enc\Big(U(\underline{a})\rho U(\underline{a})^*\Big) \otimes \sigma'_U \tag{5}$$

对于所有 $n \geq k$、元素 $a \in A_n^k$ 以及 n 量子比特状态 ρ，均满足该条件。此外，如果对于所有 $A \in A^k$，酉算子 $O_1(a), \cdots, O_\ell(a)$都是某个集合 U 中的门，则称该编码 $(\sigma_U, \sigma'_U, l, O_1, \cdots, O_\ell)$ 使用集合 U 中的物理门。

给定一个逻辑门电路 $V = U_1 \ldots U_k$我们将对 V的编码称为通过对每个门应用编码 U_i而得到的相应物理门电路。

定义 2.9。一个编码 $(\sigma_U,\ \sigma'_U,\ O_1,\ \ldots,\ O_\ell)$ 的 k-量子比特逻辑门 U 在 *QECCC* 中称为 s-可模拟的：如果对于所有 $0 \le t \le \ell$、n-量子比特状态 ρ，以及 S 物理量子比特的子集 $Enc(\rho) \otimes \sigma_U$ 满足 $|S| \le s$，则偏迹

$$\mathrm{Tr}_{\overline{S}}\Big((\mathcal{O}_t(\underline{a})\ldots\mathcal{O}_1(\underline{a}))(Enc(\rho)\otimes\sigma_U)(\mathcal{O}_t(\underline{a})\ldots\mathcal{O}_1(\underline{a}))^*\Big)$$

是一个 $2^{|S|}\times 2^{|S|}$ 矩阵，其元素为有理数，并且可以根据 t、a 和 S 在多项式时间内计算得出。_ 特别是，如果 *C* 能够纠正 *s* 个量子比特上的任意错误，那么该矩阵与 ρ 无关。

定理 2.10 ([GSY19]中的定理 6。设 $U = \{H,\ \Lambda(X),\ \Lambda^2(X)\}$。对于每个 $s \in \mathbb{N}$，都存在一个常数 $n \in \mathbb{N}$ 和一个 $[[n,1]]$ 量子纠错码 *C*，使得 *U* 中的任意逻辑门都能在 *C* 中通过使用 *U* 中的物理门实现 s-可模拟编码。

2.7 局部哈密顿量

我们定义局部哈密顿量问题。

定义 2.11。设 $k \in \mathbb{N}$、$\alpha,\ \beta \in \mathbb{R}$ 满足 $\alpha < \beta$，则参数为 α 和 β 的 k-局部哈密顿量 问题是如下承诺问题。设 n 为量子系统的量子比特数。输入是一组 $m(n)$ 哈密顿量 $H_1,\ \ldots\ldots,\ H_{m(n)}$，其中 m 是关于 n 的多项式，并且

每个 H_i 作用于 k 个量子比特组成的 n 量子比特系统中的量子比特，并具有 $\|H_i\| \le 1$。对于 $H = \sum^{m(n)}_{j=1} H_j$，承诺问题是要在以下情况之间作出判定。

是的。存在一个 n 量子比特态 $|\varphi\rangle$，使得 $\langle\varphi|H|\varphi\rangle \le a\cdot\ m(n).$

否。对于每个 n-量子比特状态 $|\varphi\rangle$，都有 $\langle\varphi|H|\varphi\rangle \ge b\cdot m(n)$。

上述问题在量子证明中起着核心作用，因为已有证明表明，对于参数 $k=5$ QMA完全 $\beta-\alpha = \quad ^1$ 和 $\beta-\alpha = \quad ^1$ 多项式(n) [KSV02]；这一事实的证明使用了著名的电路到哈密顿量构造。

3 低权重泡利编织测试

在本节中，我们介绍一种非局域博弈，该博弈可以对 Alice使用 n量子比特的泡利 σ_X 和 σ_Z 权重至多为 6 的“编织”进行自检，使其对抗 n EPR 对。也就是说，Alice 执行形式为 $\otimes_i\sigma_{W_i}$的测量，其中每个 $W_i \in \{X,\ Z,\ I\}$，并且对于除 6 个指标之外的所有指标，我们都有 $W_i = I$。正如我们在第 1.4 节中所讨论的，我们还希望当 Alice被限制为只能对至多 6个量子比特执行测量时，也能够完美赢得该博弈。因此，我们不能使用典型的泡利编织测试。为此，我们引入泡利编织测试的低权重版本。我们针对权重6引入该博弈，但下一节中的刚性论证同样适用于字符串具有任意常数权重的类似博弈。该博弈由两个子博弈构成，我们称之为低权重线性测试和低权重反对易测试。

3.1 Low-weightlinearity test

对于任意 $a \in \{0,1\}^n$ 和 $W \in \{X,Z\}^n$，我们用 $W(a)$ 表示序列 $W_1^{a_1}W_2^{a_2}\cdots W_n^{a_n}$，其中 $X^0 = Z^0 = I$。令 $\mathrm{I}_A := \{W(a) : W \in \{X,Z\}^n, a \in \{0,1\}^n$ 使得 $|a| \le 6\}$，并令 $\mathrm{I}_B := \{(W(a), W(a')) : W \in \{X,Z\}^n, a,a' \in \{0,1\}^n$ 使得 $|a|,|a'| \le 6\}$ 分别为Alice和 Bob 的问题集合。我们首先在图 3 中描述低权重线性测试。

1. 验证者从 $W \in \{X, Z\}^n$ 和字符串 $a, a' \in \{0, 1\}^n$ 中均匀随机地选择，满足 $|a|, |a'| \leq 6$（即 a, a' 的非零项均不超过 6 个）。 2. 验证者向 Bob 发送 $(W(a), W(a'))$。如果 $a + a'$ 的重量至多为 6，则验证者从 $W' \in \{W(a), W(a'), W(a + a')\}$ 中均匀随机地选择并发送给 Alice。否则，验证者从 $W' \in \{W(a), W(a')\}$ 中均匀随机地选择并发送给 Alice。 3. 验证者从 Bob 收到两个比特 (b_1, b_2)，并从 Alice 收到一个比特 c 。 4. 如果 Alice 收到 $W(a)$，则验证者要求 $b_1 = c$。如果 Alice 收到 $W(a')$，则验证者要求 $b_2 = c$。如果 Alice 收到 $W(a + a')$，则验证者要求 $b_1 + b_2 = c$。

图3：低权重线性测试。

对于这个博弈，我们让 μ 表示可能问题上的隐含概率分布 $\mathcal{I}_A \times \mathcal{I}_B$。我们看到，对于任意 $x \in \mathcal{I}_A$ 和 $y \in \mathcal{I}_B$，要么是 $\pi(x, y) = 0$ ，要么是 $\pi(x, y) = \frac{1}{O(n^6)}$。

假设 $S = (\tau^A, \tau^B, |\psi\rangle \in \mathrm{H}_A \otimes \mathrm{H}_B)$ 是该博弈的量子策略。在每个输入$x \in \mathrm{I}_A$上，Alice执行一个二结果投影值测度 $\{E_0^x, E_1^x\}$，其中 $E_0^x - E_1^x = \tau^A(x)$。类似地，在每个输入 $y = (W(a), W(a'))$ $\in I_B$上，Bob执行一个四结果投影值测度$\{F_0^y, 0, F_1^y, 0, F_0^y, 1, F_1^y, 1\}$，并定义以下可观测量：

$$\begin{aligned}
&\tau_y^B(W(a)) := F_{0,0}^y + F_{0,1}^y - F_{1,0}^y - F_{1,1}^y, \\
&\tau_y^B(W(a')) := F_{0,0}^y + F_{1,0}^y - F_{0,1}^y - F_{1,1}^y, \text{ and} \\
&\tau_y^B(W(a + a')) := F_{0,0}^y + F_{1,1}^y - F_{0,1}^y - F_{1,0}^y.
\end{aligned}$$

我们花一点时间解释上述记号中的一些细微之处。我们不为所有可能的 $W(a)$ 指定单个可观测量 $\tau^B(W(a))$，而是引用每个特定的问题对 $y = (W(a), W(a'))$。这是因为，对于不同的 $W(a')$ 选项，同一个 $W(a)$ 可能被包含在不同的问题对中。特别是，我们不能假设 Bob 针对 $W(a)$ 的测量在这些不同的可能选项下保持不变。对于 Alice，情况则更为直接，我们可以为每个 $W(a)$ 定义唯一的可观测量 $\tau^A(W(a))$。注意，可以很容易验证，对于每个 $y = (W(a), W(a'))$，我们有

$$\tau_y^B(W(a + a')) = \tau_y^B(W(a))\tau_y^B(W(a')) = \tau_y^B(W(a'))\tau_y^B(W(a)). \tag{6}$$

引理 3.1。 设 $S = (\tau^A, \tau^B, |\psi\rangle \in H_A \otimes H_B)$ 是低权重线性测试的一种策略，获胜概率为 $1 - \varepsilon$。设 $\rho_A := \mathrm{Tr}^{\mathcal{H}_B}(|\psi\rangle\langle\psi|)$。则下列界成立。

1. 对于每个 $y = (W(a), W(a')) \in I_B$,

(a) $\langle\psi|\tau^A(W(a)) \otimes \tau_y^B(W(a))|\psi\rangle \geq 1 - O(n^6)\varepsilon$, *(b)* $\langle\psi|\tau^A(W(a')) \otimes \tau_y^B(W(a'))|\psi\rangle \geq 1 - O(n^6)\varepsilon$, 以及 *(c)* 如果此外， $W(a + a') \in I_A$，那么 $\langle\psi|\tau^A(W(a + a')) \otimes \tau_y^B(W(a + a')) \geq 1 - O(n^6)\varepsilon$。

2. 对于每个 $W \in \{X, Z\}^n$ 和 $a, a' \in \{0, 1\}^n$ 与 $|a|, |a'|, |a + a'| \leq 6$,

(a) $\|\tau^A(W(a))\tau^A(W(a')) - \tau^A(W(a + a'))\|_{\rho_A}^2 \leq O(n^6)\varepsilon$,

(b) $\|\tau^A(W(a'))\tau^A(W(a)) - \tau^A(W(a+a'))\|_{\rho_A}^2 \le O(n^6)\varepsilon$, *and*
(c) $\|\tau^A(W(a))\tau^A(W(a')) - \tau^A(W(a'))\tau^A(W(a))\|_{\rho_A}^2 \le O(n^6)\varepsilon$

证明。假设 $S = (\tau^A, \tau^B, |\psi\rangle)$ 以概率 $1-\varepsilon$赢得此博弈。如果我们限定在 Bob 收到问题 $y = (W(a), W(a'))$ 且 Alice收到 $x = W(a)$的一轮，那么他们在这一问题对上输掉的概率至多为 $(1/\pi(x,y))\varepsilon \le O(n^6)\varepsilon$。否则，他们输掉整个博弈的概率将大于 ε。因此，对于任意 $x = W(a) \in \mathrm{I}_A$ and$y = (W(a), W(a')) \in \mathrm{I}_B$，我们有

$$\begin{aligned}
\langle\psi|\tau^A(W(a)) \otimes \tau_y^B(W(a))|\psi\rangle =& \langle\psi|(E_0^x - E_1^x) \otimes (F_{0,0}^y + F_{0,1}^y - F_{1,0}^y - F_{1,1}^y)|\psi\rangle \\
=& \langle\psi|(E_0^x \otimes F_{0,0}^y + E_0^x \otimes F_{0,1}^y + E_1^x \otimes F_{1,0}^y + E_1^x \otimes F_{1,1}^y)|\psi\rangle \\
& - \langle\psi|(E_0^x \otimes F_{1,0}^y + E_0^x \otimes F_{1,1}^y + E_1^x \otimes F_{0,0}^y + E_1^x \otimes F_{0,1}^y)|\psi\rangle \\
=& Pr(\mathrm{win}|x,y) - Pr(\mathrm{lose}|x,y) \\
=& 1 - 2Pr(\mathrm{lose}|x,y) \ge 1 - O(n^6)\varepsilon
\end{aligned}$$

当 Bob 收到问题 $y = (W(a), W(a'))$ 而 Alice 收到问题 $x = W(a')$时，也有类似的分析。特别地，我们得到

$$\langle\psi|\tau^A(W(a')) \otimes \tau_y^B(W(a'))|\psi\rangle \ge 1 - O(n^6)\varepsilon.$$

接下来考虑这样的实例：Bob 收到问题 $y = (W(a), W(a'))$，而 Alice 收到问题 $x = W(a+a')$，其中 $|a+a'| \le 6$。在这种情况下，获胜条件要求 $b_1 + b_2 = c$，因此我们有

$$\begin{aligned}
\langle\psi|\tau^A(W(a+a')) \otimes \tau_y^B(W(a+a')) =& \langle\psi|(E_0^x - E_1^x) \otimes (F_{0,0}^y + F_{1,1}^y - F_{0,1}^y - F_{1,0}^y)|\psi\rangle \\
=& \langle\psi|(E_0^x \otimes F_{0,0}^y + E_0^x \otimes F_{1,1}^y + E_1^x \otimes F_{1,0}^y + E_1^x \otimes F_{0,1}^y)|\psi\rangle \\
& - \langle\psi|(E_0^x \otimes F_{1,0}^y + E_0^x \otimes F_{0,1}^y + E_1^x \otimes F_{0,0}^y + E_1^x \otimes F_{1,1}^y)|\psi\rangle \\
=& Pr(\mathrm{win}|x,y) - Pr(\mathrm{lose}|x,y) \\
=& 1 - 2Pr(\mathrm{lose}|x,y) \ge 1 - O(n^6)\varepsilon.
\end{aligned}$$

为证明第二部分中的不等式对固定的 $W(a)$和 $W(a')$（其中 $|a+a'| \le 6$）成立，我们令 $x = W(a+a')$、$y = (W(a), W(a'))$ 分别作为 Alice 和 Bob 对应的输入。令$\rho := |\psi\rangle\langle\psi|$。根据上述推导，我们有

$\|\tau^A(W(a)) \otimes \mathbb{1} - \mathbb{1} \otimes \tau_y^B(W(a))\|_\rho^2 = 2 - 2\psi|\tau^A(W(a)) \otimes \tau_y^B(W(a))|\psi \le O(n^6)\varepsilon$,$\|\tau^A(W(a'))$
$\otimes \mathbb{1} - \mathbb{1} \otimes \tau_y^B(W(a'))\|_\rho^2 = 2 - 2\psi|\tau^A(W(a')) \otimes \tau_y^B(W(a'))|\psi \le O(n^6)\varepsilon$，以及$\|\tau^A(W(a+a'))$
$\otimes \mathbb{1} - \mathbb{1} \otimes \tau_y^B(W(a+a'))\|_\rho^2 = 2 - 2\psi|\tau^A(W(a+a')) \otimes \tau_y^B(W(a+a'))|\psi \le O(n^6)\varepsilon$。

注意，$\tau_y^B(W(a+a')) = \tau_y^B(W(a'))\tau_y^B(W(a))$以及 $\tau^A(W(a))$和 $\tau_y^B(W(a'))$都是酉算子。我们有

$$\begin{aligned}
\|\tau^A(W(a))\tau^A(W(a')) - \tau^A(W(a+a'))\|_{\rho_A} =& \|\left(\tau^A(W(a))\tau^A(W(a')) - \tau^A(W(a+a'))\right) \otimes \mathbb{1}\|_\rho \\
\le& \|\tau^A(W(a))\tau^A(W(a')) \otimes \mathbb{1} - \tau^A(W(a)) \otimes \tau_y^B(W(a'))\|_\rho \\
+& \|\tau^A(W(a)) \otimes \tau_y^B(W(a')) - \mathbb{1} \otimes \tau_y^B(W(a'))\tau_y^B(W(a))\|_\rho \\
+& \|\mathbb{1} \otimes \tau_y^B(W(a+a')) - \tau^A(W(a+a')) \otimes \mathbb{1}\|_\rho \\
\le& O(n^3)\sqrt{\varepsilon}.
\end{aligned}$$

因此，2 (a) 成立，基于相同的理由，2(b) 也成立，而 2(c) 则由 2(a) 和 2(b) 推出 . □

3.2 低权重反对易测试

接下来，我们介绍一种自然的反对易测试，它基于著名的魔方游戏；我们在第2.4节中介绍过该游戏。为了将这一博弈纳入我们的反对易测试，我们要求玩家在其共享的 n量子比特态中指定的双量子比特寄存器上进行魔方游戏。重要的是，除一个问题外， v_9 Alice 无法分辨自己是在进行低权重线性测试还是反对易测试，因此我们可以结合这两种博弈各自的刚性约束。回想一下，魔方游戏中的方程组有一个算子解$\{A_1$、$\cdots$、 $A_9\}$，其定义见第2.4节。我们在图4中介绍低权重反对易测试。

1. 验证者均匀随机抽取一个字符串 $a \in \{0$、$1\}^n$，其中恰有两个非零项 $i < j$。验证者还随机抽取一行或一列 $q \in \{r_1, r_2, r_3, c_1, c_2, c_3\}$，以及一个 v_k 包含于 q 中的变量，具体如魔方游戏所示。2. Bob 收到问题 (q, a)。3. 如果 $k \neq 9$，那么 Alice 收到 $W(a)$ $= I^{i-1}W_iI^{j-i}W_jI^{n-j} \in \mathcal{I}_A$，其中 $\sigma_{W_i} \otimes \sigma_{W_j} = A_k$。如果$k = 9$，那么 Alice 收到问题 $(v_9$, $a)$。4. 当且仅当 Bob 对 q 给出一个满足赋值，并且 Alice 为变量 v_k 提供一个与 Bob 的赋值一致的赋值时，玩家获胜。

图 4：低权重反对易测试。

在上述博弈中，对于每个字符串 $a \in \{0,1\}^n$ 满足 $|a| = 2$ 我们为 Alice 定义以下可观测量集合 $\{O_1(a)$、.....、 $O_9(a)\}$。如果玩家以概率 $1 - \varepsilon$ 通过反对易测试，那么上述可观测量必然确定一个量子策略的算子，该量子策略在魔方游戏中的获胜概率至少为 $1 - O(n^2)\varepsilon$。应用魔方游戏的刚性（引理 2.4），我们得到以下引理。

引理 3.2。 如果玩家以概率 $1 - \varepsilon$ 通过低权重反对易测试，那么对于任意 $a \in \{0,1\}^n$，满足 $|a| = 2$，我们有

$$\|O_1(a)O_5(a) + O_5(a)O_1(a)\|_\sigma^2 \leq O(n)\sqrt{\varepsilon}, \text{ and}$$
$$\|O_4(a)O_2(a) + O_2(a)O_4(a)\|_\sigma^2 \leq O(n)\sqrt{\varepsilon}.$$

3.3 形式化陈述

结合前几节中的低权重线性测试和低权重反对易测试，我们现在构造低权重 Pauli 编织测试，并陈述其刚性结果。

定义 3.3。 低权重 *Pauli* 编织测试（*LWPBT*）的执行方式是：以$1/2$ 的概率执行低权重反对易测试，或执行低权重线性测试。

如果某个量子策略 $S = (\tau^A, \tau^B, |\psi\rangle)$ 以概率 $1 - \varepsilon$赢得 LWPBT，那么它以至少 $1 - 2\varepsilon$的概率同时通过低权重线性测试和低权重反对易测试。对于每个 $W \in \{X, Z\}$和 $i \in [n]$，我们用 $\tau_W^A($ $e_i)$ 表示 $\tau^A(I^{i-1}WI^{n-i})$。对于任意比特串 $a = 0^{j-2}110^{n-j}$，若 $2 \leq j \leq n$，由于 Alice 无法分辨问题 $I^{j-1}WI^{n-j}$ 属于低权重线性测试还是低权重反对易测试，因此必有 $O_1(a) = \tau_X^A(e_j)$

以及 $O_5(a) = \tau_Z^A(e_j)$。同样，对于任意比特串 $a = 0^{j-1}110^{n-j-1}$，若 $1 \le j \le n-1$，则必有 $O_2(a) = \tau_X^A(e_j)$ 以及 $O_4(a) = \tau_Z^A(e_j)$。由引理3.1 和引理3.2可直接得到以下定理。

定理 3.4. 设 $S = (\tau^A, \tau^B, |\psi\rangle \in H_A \otimes H_B)$ 是 *LWPBT* 的一种策略，获胜概率为 $1-\varepsilon$。令 $\rho_A := \mathrm{Tr}_{\mathcal{H}_B}(|\psi\rangle\langle\psi|)$。

1. 对每个 $y = (W(a), W(a')) \in I_B$，一致性满足以下界。

(a) $\langle\psi|\tau^A(W(a)) \otimes \tau_y^B(W(a))|\psi\rangle \ge 1 - O(n^6)\varepsilon$，*(b)* $\langle\psi|\tau^A(W(a')) \otimes \tau_y^B(W(a'))|\psi\rangle \ge 1 - O(n^6)\varepsilon$，以及 *(c)* 若另外 $|a+a'| \le 6$，则 $\langle\psi|\tau^A(W(a+a')) \otimes \tau_y^B(W(a+a')) \ge 1 - O(n^6)\varepsilon$。

2. 对于每个 $W \in \{X, Z\}^n$ 和 $a, a' \in \{0,1\}^n$，若满足 $|a|, |a'|, |a+a'| \le 6$，则有以下线性界和对易界。

(a) $\|\tau^A(W(a))\tau^A(W(a')) - \tau^A(W(a+a'))\|_{\rho_A}^2 \le O(n^6)\varepsilon,$

(b) $\|\tau^A(W(a'))\tau^A(W(a)) - \tau^A(W(a+a'))\|_{\rho_A}^2 \le O(n^6)\varepsilon,$ *and*

(c) $\|\tau^A(W(a))\tau^A(W(a')) - \tau^A(W(a'))\tau^A(W(a))\|_{\rho_A}^2 \le O(n^6)\varepsilon$

3. 对于任意 $i, j \in [n]$，我们有以下对易／反对易界 .

(a) $\|\tau_X^A(e_i)\tau_Z^A(e_j) - (-1)^{\delta_{ij}}\tau_Z^A(e_j)\tau_X^A(e_i)\|_{\rho_A}^2 \le O(n)\sqrt{\varepsilon}.$

4 低权重 Pauli 交织测试的刚性

本节中，我们采用群论方法分析 LWPBT。我们证明，LWPBT 的每个近最优策略都会构成 Weyl-Heisenberg 群的一个近似同态。为了将近似同态舍入为精确表示，我们提出了一个增强版 Gowers-Hatami 定理。将这一新的稳定性结果应用于 Weyl-Heisenberg 群，我们证明，任何获胜概率为 $1-\varepsilon$ 的 LWPBT 策略都必须与典范完美策略 $poly(n)\sqrt{\varepsilon}$ 接近。 –

4.1 增强的Gowers-Hatami 定理

Gowers-Hatami 定理 [GH17] 及其变体 [Vid18] 在非局域博弈的刚性分析中发挥着重要作用。该定理指出，有限群的每个近似同态都接近一个表示。某些非局域博弈 G 可以用有限群 G 建模，即 G 的最优策略对应于 G 的表示，而 G 的近最优策略对应于 G的近似同态。如果此外，G 还有一个~典范最优策略 S，那么该定理意味着 G 的每个近最优策略 S 都接近~S。然而，正如第 1 节和第 2.3 节所讨论的，早期方法中出现了一些微妙的数学问题。特别是，可能需要舍弃表示中与 S 不对应的一些不可约分量~。在以下增强版 Gowers-Hatami 定理中，我们指出，只要近似同态满足某些额外的对称性，它就必定接近一个不含此类“冗余”不可约分量的表示。

定理4.1。设 G 为一个有限群。设 $f\colon\ G \to \mathscr{U}(H)$ 为一个(ε,ρ)-同态，并设 S 是 G 的一个子群，满足

$$f(sg) = f(s)f(g) \text{ for all } s \in S, g \in G. \tag{7}$$

于是 $f|_S\colon\ \ S \to \mathscr{U}(H)$ 是 S 的一个表示，并且存在一个希尔伯特空间 K、一个等距映射$V\colon H \to K$，以及一个表示 $\phi\colon\ \ G \to \mathscr{U}(K)$，使得

$$\|Vf(g) - \phi(g)V\|_\rho^2 \le \varepsilon \text{ for all } g \in G, \tag{8}$$

并且 ϕ 的每个不可约分量 ξ都满足 $f|_S(\xi|_S) \neq 0$。

证明。 $f|_S$保留了 S 的群结构，因此它是 S 的一个表示。令 $\mathrm{Irr}(G, f|_S) := \{\varphi \in \widehat{\ } \mathrm{Irr}(G)\colon\ f|_S(\varphi|_S) \neq 0\}$。对于任意 $\varphi \in \mathrm{Irr}(G)$和 $s \in S$，我们有

$$\Big(f(s) \otimes \overline{\phi(s)}\Big)\widehat{f}(\varphi) = \frac{1}{|G|}\sum_{g\in G} f(s)f(g) \otimes \overline{\varphi(s)\varphi(g)} = \frac{1}{|G|}\sum_{g\in G} f(sg) \otimes \overline{\varphi(sg)} = \widehat{f}(\varphi).$$

由于 $\widehat{f|_S}(\varphi|_S) = \frac{1}{|S|}\sum_{s\in S}\Big(f(s) \otimes \overline{\phi(s)}\Big)\widehat{f}(\varphi)$，因此可得

$$\widehat{f|_S}(\varphi|_S)\cdot \widehat{f}(\varphi) = \widehat{f}(\varphi). \tag{9}$$

特别地，对于任意 $\xi \in \mathrm{Irr}(G) \setminus \mathrm{Irr}(G, f|_S)$，由于 $f|_S(\xi|_S) = 0$，方程 (9) 推出 $f(\xi) = 0$。令 $\mathrm{K} := \bigoplus \mathbb{C}^{d_\varphi} \otimes \mathrm{H} \otimes \mathbb{C}^{d_\varphi}$，并定义线性映射 $V\colon \mathrm{H} \to \mathrm{K}$，将$\varphi \in \mathrm{Irr}(G, f|_S)$映射至

$$|v\rangle \mapsto \bigoplus_{\varphi\in \mathrm{Irr}(G,f|_S)} \sqrt{d_\varphi}\sum_{i=1}^{d_\varphi} |i\rangle \otimes \Big(\widehat{f}(\varphi)(|v\rangle \otimes |i\rangle)\Big),$$

其中 $\{|i\rangle\}_{i=1}^{d_\varphi}$是 $\mathbb{C}^{d_\varphi}$ 的标准基。由于对所有 $\varphi \in Irr(G) \setminus Irr(G, f|_S)$，均有 $\widehat{f}(\varphi) = 0$，

$$\begin{aligned}
V^*V &= \sum_{\varphi\in \mathrm{Irr}(G,f|_S)} d_\varphi \sum_{i=1}^{d_\varphi} \Big(\mathbb{1}_{\mathcal{H}} \otimes \langle i|\Big)\widehat{f}(\varphi)^*\widehat{f}(\varphi)\Big(\mathbb{1}_{\mathcal{H}} \otimes |i\rangle\Big) \\
&= \sum_{\varphi\in \mathrm{Irr}(G)} d_\varphi \sum_{i=1}^{d_\varphi} \Big(\mathbb{1}_{\mathcal{H}} \otimes \langle i|\Big)\widehat{f}(\varphi)^*\widehat{f}(\varphi)\Big(\mathbb{1}_{\mathcal{H}} \otimes |i\rangle\Big) \\
&= \frac{1}{|G|^2}\sum_{\varphi\in \mathrm{Irr}(G)} d_\varphi \sum_{g,h\in G} f(g)^* f(h) \sum_{i=1}^{d_\varphi} \langle i|\varphi(g)^T\overline{\varphi(h)}|i\rangle \\
&= \frac{1}{|G|^2}\sum_{g,h\in G} f(g)^* f(h) \sum_{\varphi\in \mathrm{Irr}(G)} d_\varphi \mathrm{Tr}\Big(\varphi(g^{-1}h)\Big) \\
&= \frac{1}{|G|}\sum_{g\in G} f(g)^* f(g) = \mathbb{1}_{\mathcal{H}}.
\end{aligned}$$

因此， V是一个等距映射。现在考虑表示 $\phi\colon\ G \to \mathscr{U}(\mathcal{K})$，其定义为发送

$$g \mapsto \bigoplus_{\varphi\in \mathrm{Irr}(G,f|_S)} \varphi(g) \otimes \mathbb{1}_{\mathcal{H}} \otimes \mathbb{1}_{\mathbb{C}^{d_\varphi}}.$$

我们看到， φ是 ϕ的不可约分量，当且仅当 $\varphi \in \mathbf{Irr}(G, f|_S)$。注意，对于任意 $A \in M_d(\mathbb{C})$，对于所有基向量 $|i\rangle$ 和 $|j\rangle$，都有 $\langle i|A|j\rangle = \langle j|A^T|i\rangle$。于是，对于任意 $g \in G$，我们得到

$$\begin{aligned}
V^*\phi(g)V &= \sum_{\varphi\in \mathrm{Irr}(G,f|_S)} d_\varphi \sum_{i,j=1}^{d_\varphi} \langle i|\varphi(g)|j\rangle \Big(\mathbb{1}_{\mathcal{H}} \otimes \langle i|\Big) \widehat{f}(\varphi)^* \widehat{f}(\varphi) \Big(\mathbb{1}_{\mathcal{H}} \otimes |j\rangle\Big) \\
&= \sum_{\varphi\in \mathrm{Irr}(G)} d_\varphi \sum_{i,j=1}^{d_\varphi} \langle i|\varphi(g)|j\rangle \Big(\mathbb{1}_{\mathcal{H}} \otimes \langle i|\Big) \widehat{f}(\varphi)^* \widehat{f}(\varphi) \Big(\mathbb{1}_{\mathcal{H}} \otimes |j\rangle\Big) \\
&= \frac{1}{|G|^2} \sum_{\varphi\in \mathrm{Irr}(G)} d_\varphi \sum_{h,k\in G} f(h)^* f(k) \sum_{i,j=1}^{d_\varphi} \langle i|\varphi(g)|j\rangle \langle i|\varphi(h)^T \overline{\varphi(k)}|j\rangle \\
&= \frac{1}{|G|^2} \sum_{\varphi\in \mathrm{Irr}(G)} d_\varphi \sum_{h,k\in G} f(h)^* f(k) \sum_{i,j=1}^{d_\varphi} \langle i|\varphi(g)|j\rangle \langle j|\varphi(k)^* \varphi(h)|i\rangle \\
&= \frac{1}{|G|^2} \sum_{h,k\in G} f(h)^* f(k) \sum_{\varphi\in \mathrm{Irr}(G)} d_\varphi \mathrm{Tr}\Big(\varphi(k^{-1}hg)\Big) = \frac{1}{|G|} \sum_{h\in G} f(h)^* f(hg).
\end{aligned}$$

于是我们得到

$$\begin{aligned}
\|Vf(g) - \phi(g)V\|_\rho^2 &= 2 - \frac{1}{|G|} \sum_{h\in G} 2\mathfrak{Re}\mathrm{Tr}\Big(f(g)^* f(h)^* f(hg)\rho\Big) \\
&= \frac{1}{|G|} \sum_{h\in G} \Big(2 - 2\mathfrak{Re}\mathrm{Tr}\Big(f(g)^* f(h)^* f(hg)\rho\Big)\Big) \\
&= \frac{1}{|G|} \sum_{h\in G} \|f(h)f(g) - f(hg)\|_\rho^2.
\end{aligned}$$

由于 f 是一个 (ε, ρ) G 的同态，因此对于所有 $g \in$，都有 $\|Vf(g) - \phi(g)V\|_\rho^2 \le \varepsilon$ G. □

4.2 刚性证明

现在我们旨在证明低权重泡利编织测试的刚性。首先，在本节中（推论 $n \in \mathbb{N}$，我们固定一个 $\varepsilon > 0$，以及一个量子策略 $S := (\tau^A, \tau^B, |\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B)$除外），固定一个用于 n量子比特 LWPBT 的获胜概率 $1 - \varepsilon$，其中 4.10）。

令 $H(n)$为由不定元 $\{J, X_i, Z_i, i \in [n]\}$生成的 n 量子比特 Weyl-Heisenberg 群，其满足以下关系

(R0) J is central, and $J^2 = X_i^2 = Z_i^2 = 1$ for all $1 \le i \le n$,

(R1) $[X_i, Z_i] = J$ 对所有或所有 $1 \le i \le n$，且

(R2) $[X_i, X_j] = [Z_i, Z_j] = [X_i, Z_j] = 1$对所有 $i \ne j$。

直观而言，这个群刻画了 n量子比特的泡利测量。它有一个不可约表示σ： $H(n) \to \mathscr{U}((\mathbb{C}^2)^{\otimes n})$发送 $J \mapsto -\mathbb{1}$, $X_i \mapsto \sigma_X(e_i)$，并且对所有 $i \in [n]$, $Z_i \mapsto \sigma_Z(e_i)$。在本节中，符号 σ 将专门用于指代这个不可约表示。以下两个引理是众所周知的。

引理 4.2。 不可约表示集$(H(n)) = \{\sigma\} \cup \{\chi_i : 1 \le i \le 2^{2n}\}$，其中每个 $\chi_i : H(n) \to \mathbb{C}$都是一个将 $J \mapsto 1$ 映射为.....的一维表示。

引理4.3。 $H(n)$具有正规形式$N(w) = J^{\alpha}X_{i_1}\cdots X_{i_k}Z_{j_1}\cdots Z_{j_l}$，其中 $\alpha\in\{0,1\}$，$1\le i_1<\cdots<i_k\le n$，以及 $1\le j_1<\cdots<j_l\le n$。

对于任意的 $W\in\{X,Z\}$ 和 $i\in[n]$，我们分别用 $\tau_W^A(e_i)$ 和 $\tau_W^B(e_i)$ 表示 $\tau^A(I^{i-1}WI^{n-i})$ 和$\tau_y^B($ $I^{i-1}WI^{n-i})$，其中 $y=(I^{i-1}WI^{n-i},I^n)$。定义函数 $f_P\colon H(n)\to\mathscr{U}(\mathrm{H}_P),P\in\{A,B\}$，其定义方式为

$$J^{\alpha}X_{i_1}\cdots X_{i_k}Z_{j_1}\cdots Z_{j_l}\mapsto(-1)^{\alpha}\tau_X^P(e_{i_1})\cdots\tau_X^P(e_{i_k})\tau_Z^P(e_{j_1})\cdots\tau_Z^P(e_{j_l}),$$

~ ~因此，特别地，$f_P(\ 1\ =\mathbb{1}_{\ P}\qquad f_P\ J\ =-\mathbb{1}_{\mathcal{H}_P}\qquad f_A\ f_B\quad H\ n\ \to)$ H 和 ( ) 。我们还通过 $f_A(g):=f_A(g)\otimes\mathbb{1}_{\mathrm{H}_B}$ 以及 $f_B(g):=\mathbb{1}_{\mathrm{H}_A}\otimes f_B(g)$ 定义函数 , : ( ) $\mathscr{U}(\mathrm{H}_A\otimes\mathrm{H}_B)$。本节中，我们用$\rho$、$\rho_A$和 ρ_B分别表示 $|\psi\rangle\langle\psi|$、$\mathrm{Tr}_{\mathcal{H}_B}(\rho)$ 和 $\mathrm{Tr}_{\mathcal{H}_A}(\rho)$。

命题 4.4。 令 $\delta:=O(n^6)\sqrt{\varepsilon}$。每个 $f\in\{\widetilde{f}_A,\ \widetilde{f}_B\}$ 都满足以下条件。

(1) f 遵守 *R0* 中的所有关系。

(2) $\|f(X_i)f(Z_i)+f(Z_i)f(X_i)\|_\rho^2\le\delta$对所有 $1\le i\le n$。

(3) $\|f(X_i)f(X_j)-f(X_j)f(X_i)\|_\rho^2$、$\|f(Z_i)f(Z_j)-f(Z_j)f(Z_i)\|_\rho^2$，以及 $\|f(X_i)f(Z_j)-f(Z_j)f(X_i)\|_\rho^2$在 $i\ne j$ 时均由 δ 界定。

(4) 对于每个 W_i，其中 $W\in\{X,\ Z\}$，$i\in[n]$，都存在一个与所有 $\{f(X_j),\ f(Z_j),\ j\in[n]\}$ 对易的酉算子 W_i，使得 $\|f(W_i)-\widehat{W}_i\|_\rho^2\le\delta$。

(5) 对任意 $s\ge1$ 以及每个[7] $v=v_1\cdots v_s$ 上次数为 s 的单项式，其中 $\{f(X_i),f(Z_i),i\in[n]\}$，存在一个酉算子 $\widehat{v}$，它与所有 $\{f(X_i),f(Z_i),i\in[n]\}$ 对易，使得 $\|v-\widehat{v}\|_\rho\le s\sqrt{\delta}$。

~证明。 我们首先考察 f_A 是否满足 (1)、(2)、(3) 和 (4)。由于对于所有 $W\in\mathcal{B}(\mathcal{H}_A)$，$\|W\otimes\mathbb{1}_{\mathcal{H}_B}\|_\rho=\|W\|_{\rho_A}$ 都有~，根据定理 3.4 可知，f_A 满足 (1)、(2) 和 (3)。为证明~ ~ ~的 (4)，注意到对于所有 $j\in[n]$，每个 $f_B(W_i)$都与 $f_A(X_j)$、$f_A(Z_j)$对易，并且

$$\|\widetilde{f}_A(W_i)-\widetilde{f}_B(W_i)\|_\rho^2=2-2\langle\psi|\tau_W^A(e_i)\otimes\tau_W^B(e_i)|\psi\rangle\le O(n^6)\sqrt{\varepsilon}\tag{10}$$

~根据定理 3.4。因此，取 $W_i=f_B(W_i)$ 即可推出 (4)。

接下来我们将研究这一点 $\widetilde{f}_B$ 满足（1）、（2）、（3）和（4）。第（1）部分显然。由于

$$\begin{aligned}\widetilde{f}_B(X_i)\widetilde{f}_B(Z_i)+\widetilde{f}_B(Z_i)\widetilde{f}_B(X_i)=&\widetilde{f}_B(X_i)\big(\widetilde{f}_B(Z_i)-\widetilde{f}_A(Z_i)\big)+\widetilde{f}_B(Z_i)\big(\widetilde{f}_B(X_i)-\widetilde{f}_A(X_i)\big)\\&+\widetilde{f}_A(Z_i)\big(\widetilde{f}_B(X_i)-\widetilde{f}_A(X_i)\big)+\widetilde{f}_A(X_i)\big(\widetilde{f}_B(Z_i)-f_A(Z_i)\big)\\&+\widetilde{f}_A(Z_i)\widetilde{f}_A(X_i)+\widetilde{f}_A(X_i)\widetilde{f}_A(Z_i),\end{aligned}$$

并且右侧的每一项都具有 ρ-范数 $\le O(n^6)\sqrt{\varepsilon}$根据定理 3.4，可得$\|\widetilde{f}_B(X_i)\widetilde{f}_B(Z_i)+\widetilde{f}_B(Z_i)\widetilde{f}_B(X_i)\|_\rho^2\le O(n^6)\sqrt{\varepsilon}$。因此，对于 $\widetilde{f}_B$，第（2）部分成立。通过类似的~论证，我们得到第（3）部分成立。第（4）部分由方程（10）推出，取 $W_i=\sim f_A(W_i)$即可。

现在我们通过对单项式次数 $s\ge1$ 进行归纳来证明第 (5) 部分。基础情形 $s=1$ 直接由第 (4) 部分得到。假设对于次数为 s 的所有关于 $\{f(X_i),f(Z_i),i\in[n]\}$ 的单项式，第 (5) 部分均成立。对于任意一个次数为 $s+1$ 的关于 $\{f(X_i),f(Z_i),i\in[n]\}$ 的单项式 $v=v_1\cdots v_sv_{s+1}$，令$v':=v_1\cdots v_s$。根据归纳假设，存在与所有对象对易的酉算子 $\widehat{v}'$ 和 $\widehat{v}_{s+1}$，它们与所有

[7]在这里，我们允许单项式的系数为 1 或 -1。

$\{f(X_i), f(Z_i), i \in [n]\}$，使得 $\|v' - \widehat{v}'\|_\rho \le s\sqrt{\delta}$和 $\|v_{s+1} - \widehat{v}_{s+1}\|_\rho \le \sqrt{\delta}$。特别地， $\widehat{v}_{s+1}$与 v'对易，因此 $v = v'(v_{s+1} - \widehat{v}_{s+1}) + \widehat{v}_{s+1}(v' - \widehat{v}') + \widehat{v}_{s+1}\widehat{v}'$。由于 ρ-范数是左酉不变的，且 $\widehat{v}'$、$\widehat{v}_{s+1}$是与所有 $\{f(X_i), f(Z_i), i \in [n]\}$ 对易的酉算子，因此可得 $\widehat{v}_{s+1}\widehat{v}' =: \widehat{v}$是一个与所有 $\{f(X_i), f(Z_i), i \in [n]\}$ 对易的酉算子，并且满足

$$\|v - \widehat{v}\|_\rho \le \|v_{s+1} - \widehat{v}_{s+1}\|_\rho + \|v' - \widehat{v}'\|_\rho \le (s+1)\sqrt{\delta}.$$

我们得出，对于 $\{f(X_i)$、$f(Z_i)$、$i \in [n]\}$ 上的所有单项式，(5) 均成立。 □

命题 4.5。设 $\delta := O(n^6)\sqrt{\varepsilon}$。则每个 $f \in \{\widetilde{f}_A, \widetilde{f}_B\}$ 都是 $\left(O(n^6)\delta, \rho\right)$- $H(n)$ 的同态。

证明。设 $R := \{f(X_i)f(X_j) - f(X_j)f(X_i), f(Z_i)f(Z_j) - f(Z_j)f(Z_i), f(X_i)f(Z_j) - f(Z_j)f(X_i) : i \ne j\} \cup \{f(X_i)f(Z_i) + f(Z_i)f(X_i) : i \in [n]\}$。根据命题 4.4 的第 (2) 和 (3) 部分，$\|r\|_\rho \le \sqrt{\delta}$对所有 $r \in R$ 均成立。由于 $f(X_i)$ 和 $\overline{f}(Z_i)$ 是酉算子，因此可推出，$\|r\|_{op} \le 2$对所有 $r \in R$ 均成立。

根据以及的定义$H(n)$的标准形定理，对于任意 $g, h \in H(n)$，我们看到 $f(g)f(h)$和 $f(gh)$是关于$\{f(X_i), f(Z_i), i \in [n]\}$的次数小于$4n$的单项式，并且 $f(g)f(h) - f(gh) = \sum_{i=1}^k u_i r_i v_i$其中 $k \le 4n^2$，$r_1, \cdots r_k \in R$, $u_1, \cdots u_k, v_1, \cdots, v_k$是关于$\{f(X_i), f(Z_i), i \in [n]\}$的单项式，且每个 v_i的次数都小于 $2n$。最后一个条件意味着，对于每个 $i \in [k]$，存在一个与所有$\{f(X_i), f(Z_i), i \in [n]\}$交换的酉算子 $\widehat{v}_i$，使得$\|v_i - \widehat{v}_i\|_\rho \le 2n\sqrt{\delta}$，根据命题4.4的第(5)部分。于是对于每个 $i \in [k]$，我们有

$$\begin{aligned}\|u_i r_i v_i\|_\rho &= \|r_i(v_i - \widehat{v}_i + \widehat{v}_i)\|_\rho \le \|r_i(v_i - \widehat{v}_i)\|_\rho + \|\widehat{v}_i r_i\|_\rho \\ &\le \|r_i\|_{op} \cdot \|v_i - \widehat{v}_i\|_\rho + \|r_i\|_\rho \le (4n+1)\sqrt{\delta}.\end{aligned}$$

因此 $\|f\ g\ f\ h - f\ gh\|_\rho \le \sum_{i=1}^k \|u_i r_i v_i\|_\rho \le O\ n^3\ \sqrt{\delta}$ $\|f\ g\ f\ h - f\ gh\|_\rho^2 \le ()()()()$。我们得出，对于所有 $O\ n^6\ \delta$ $h \in H\ n$ g, (), ()()()()。 □

由于 $\|f_P(g)f_P(h) - f_P(gh)\|_{\rho_P}^2 = \|\widetilde{f}_P(g)\,\widetilde{f}_P(h) - \widetilde{f}_P(gh)\|_\rho^2$对于每个 $P \in \{A, B\}$ 以及所有 $g, h \in H(n)$，我们有：

推论 4.6。函数 f_A（分别为 f_B）是 $H(n)$ 的$(O(n^{12})\sqrt{\varepsilon}, \overline{\rho}_A)$-同态（分别是$(O(n^{12})\sqrt{\varepsilon}, \rho_B)$-同态）。

现在，我们可以将定理4.1应用于 $f \in \{f_A, f_B\}$。由 J生成的子群 J 仅包含两个元素 1 和 J，并且我们看到，对于所有 $s \in J$ 和 $g \in H(n)$，$f(sg) = f(s)f(g)$。因此，$f|_{\langle J\rangle}$ 是 $H(n)$ 的一个表示。特别地，f 将 $1 \mapsto \mathbb{1}$ 和 $J \mapsto -\mathbb{1}$ 发送到相应位置，因此对于 $H(n)$ 的所有一维不可约表示 χ，$f|_{\langle J\rangle}(\chi|_{\langle J\rangle}) = f(1)\chi(1) + f(J)\chi(J) = \mathbb{1} - \mathbb{1} = 0$。这意味着，$\sigma$ 是 $H(n)$ 中满足 $f|_{\langle J\rangle}(\sigma|_{\langle J\rangle}) \ne 0$ 的唯一不可约表示。因此，我们得到：

定理 4.7。存在一个希尔伯特空间 H_A^{aux}（分别为 H_B^{aux}）以及一个等距映射 $V_A : H_A \to \mathbb{C}^{2^n} \otimes H_A^{aux}$（分别为 $V_B : H_B \to \mathbb{C}^{2^n} \otimes H_B^{aux}$），使得 $\|V_A f_A(g) - \left(\sigma(g) \otimes \mathbb{1}_{K_A}\right) V_A\|_{\rho_A}^2 \le O(n^{12})\sqrt{\varepsilon}$（分别为 $\|V_B f_B(g) - \left(\sigma(g) \otimes \mathbb{1}_{K_B}\right) V_B\|_{\rho_B}^2 \le O(n^{12})\sqrt{\varepsilon}$）对所有 $g \in H(n)$ 均成立。

证明。令 $\delta = O(n^{12})\sqrt{\varepsilon}$。推论 4.6 表明，$f_A$ 是 $H(n)$ 的(δ, ρ_A)-同态。从上述讨论中，我们知道，σ 是满足 $f_A|_{\langle J\rangle}(\sigma|_{\langle J\rangle}) \ne 0$的唯一不可约表示。然后根据定理4.1，存在一个希尔伯特空间K、一个等距映射 $V : \mathrm{H}_A \to \mathrm{K}$，以及一个表示$\phi$：$H(n) \to \mathscr{U}(\mathrm{K})$，使得对于所有 $g \in H(n)$，$\|V f_A(g) - \phi(g) V\|_\rho^2 \le \delta$，并且 ϕ具有唯一

不可约分量 σ。后一条件意味着$\mathcal{K} \cong \mathbb{C}^{2^n} \otimes \mathcal{H}_A^{aux}$，其中$\mathcal{H}_A^{aux}$是某个希尔伯特空间，并且存在酉算子 U: $\mathcal{K} \to \mathbb{C}^{2^n} \otimes \mathcal{H}_A^{aux}$，使得 $U\phi(g)U^* = \sigma(g) \otimes \mathbb{1}_{\mathcal{H}_A^{aux}}$对所有 $g \in H(n)$ 均成立。由于 ρ_A-范数是左酉不变的，因此可知

$$\begin{aligned}\|Vf(g) - \phi(g)V\|_{\rho_A} &= \|U^*UVf(g) - U^*\Big(\sigma(g) \otimes \mathbb{1}_{\mathcal{H}_A^{aux}}\Big)UV\|_{\rho_A} \\ &= \|UVf(g) - \Big(\sigma(g) \otimes \mathbb{1}_{\mathcal{H}_A^{aux}}\Big)UV\|_{\rho_A}\end{aligned}$$

对所有 $g \in H(n)$ V_A，我们得出 $= UV$: $\mathcal{H}_A \to \mathbb{C}^{2^n} \otimes \mathcal{H}_A^{aux}$ 是一个等距映射，使得$\|V_A f_A(g)$ $- \Big(\sigma(g) \otimes Id_{\mathcal{H}_A^{aux}}\Big)V_A\|_{\rho_A}^2 \leq \delta$。关于 f_B 的论证类似。 □

上述定理表明，在 LWPBT 的近完美策略中，参与者必须执行与典范完美策略中的测量接近的测量。下面的引理表明，参与者共享的联合态也必须接近最大纠缠态。

引理 4.8. 如果 $|\psi\rangle \in \mathbb{C}^{2^n} \otimes \mathbb{C}^{2^n}$ 是满足下式的单位向量

$$\frac{1}{4n} \sum_{a,b \in \{0,1\}, i \in [n]} \langle\psi| \Big(\sigma_X(e_i)^a \sigma_Z(e_i)^b \otimes \sigma_X(e_i)^a \sigma_Z(e_i)^b\Big) |\psi\rangle \geq 1 - \delta \tag{11}$$

对于某个 $0 \leq \delta \leq 1/n$，则 $|\langle\psi|\Phi^{\otimes n}{}_{EPR}\rangle|^2 \geq 1 - n\delta$。
证明。令 S: $= \frac{1}{4n} \sum_{a\, b \in 0,1,\{\},i \in [n]} \sigma_X(e_i)^a \sigma_Z(e_i)^b \otimes \sigma_X(e_i)^a \sigma_Z(e_i)^b$，并令 $P_1 := |\Phi_{\text{EPR}}\rangle\langle\Phi_{\text{EPR}}|$和 $P_0 = \mathbb{1}_{\mathbb{C}^4} - P_1$。由于 $\frac{1}{4}(\sigma_I \otimes \sigma_I + \sigma_X \otimes \sigma_X + \sigma_Z \otimes \sigma_Z + \sigma_X\sigma_Z \otimes \sigma_X\sigma_Z) = |\Phi_{\text{EPR}}\rangle\langle\Phi_{\text{EPR}}|$，我们有

$$S = \frac{1}{n} \sum_{i \in [n]} \mathbb{1}_{\mathbb{C}^4}^{\otimes(i-1)} \otimes |\Phi_{\text{EPR}}\rangle\langle\Phi_{\text{EPR}}| \otimes \mathbb{1}_{\mathbb{C}^4}^{\otimes(n-i)} = \frac{1}{n} \sum_{i \in [n]} (P_0 + P_1)^{\otimes(i-1)} \otimes P_1 \otimes (P_0 + P_1)^{\otimes(n-i)}.$$

这意味着 S 是半正定的，且有唯一的特征向量$|\Phi^{\otimes n}$ EPR，其特征值为 $+1$ 。 S 的任何其他特征向量的特征值都小于$\frac{n-1}{n}$ 。换言之， S 有一个谱分解$\sum_{i=1}^{2^{2n}} s_i |\alpha_i\alpha_i|$ ，其中 $s_1 = 1$，对所有 $i \geq 2$ 都有 $s_i \in [0, \frac{n-1}{n}]$， $|\alpha_1 =$ $|\Phi^{\otimes n}$ EPR，且$\{|\alpha_i\}_{i=1}^{2^{2n}}$ 是 $\mathbb{C}^{2^n} \otimes \mathbb{C}^{2^n}$的一组标准正交基。现在假设 $|\psi$ $= \sum_{i=1}^{2^{2n}} \lambda_i |\alpha_i$是 $\mathbb{C}^{2^n} \otimes \mathbb{C}^{2^n}$中的一个单位向量，满足等式（11）。那么

$$\begin{aligned}1 - \delta \leq \langle\psi|S|\psi\rangle &= |\lambda_1|^2 + \sum_{i \geq 2} s_i |\lambda_i|^2 \leq |\lambda_1|^2 + \sum_{i \geq 2} (\frac{n-1}{n}) |\lambda_i|^2 \\ &= |\lambda_1|^2 + (\frac{n-1}{n})(1 - |\lambda_1|^2) = \frac{n-1}{n} + \frac{1}{n}|\lambda_1|^2.\end{aligned}$$

因此 $|\langle\psi|\Phi^{\otimes n}{}_{\text{EPR}}\rangle|^2 = |\lambda_1|^2 \geq 1 - n\delta.$ □

定理 4.9。 存在希尔伯特空间 H_A^{aux}和 H_B^{aux}、等距映射 $V_A : H_A \to \mathbb{C}^{2n} \otimes H_A^{aux}, V_B : H_B \to \mathbb{C}^{2n} \otimes H_B^{aux}$，以及一个单位向量 $|aux\rangle \in H_A^{aux} \otimes H_B^{aux}$，使得

$$\|(V_A \otimes V_B)\Big(f_A(g) \otimes \mathbb{1}_{\mathcal{H}_B}|\psi\rangle\Big) - \Big(\sigma(g) \otimes \mathbb{1}_{\mathbb{C}^{2^n}}|\Phi_{EPR}^{\otimes n}\rangle\Big) \otimes |aux\rangle\|^2 \leq O(n^{12})\sqrt{\varepsilon} \tag{12}$$

对所有 $g \in H(n)$。

证明。 根据定理 3.4，我们看到

$$\begin{aligned}
&\|f_A(X_i)\otimes\mathbb{1}-\mathbb{1}\otimes f_B(X_i)\|_\rho^2 = 2-2\langle\psi|f_A(X_i)\otimes f_B(X_i)|\psi\rangle \le O(n^6)\varepsilon,\\
&\|f_A(Z_i)\otimes\mathbb{1}-\mathbb{1}\otimes f_B(Z_i)\|_\rho^2 = 2-2\langle\psi|f_A(Z_i)\otimes f_B(Z_i)|\psi\rangle \le O(n^6)\varepsilon, \text{ and}\\
&\|\Big(f_A(X_i)f_A(Z_i)-f_A(Z_i)f_A(X_i)\Big)\otimes\mathbb{1}\|_\rho^2 = \|f_A(X_i)f_A(Z_i)-f_A(Z_i)f_A(X_i)\|_{\rho_A}^2 \le O(n)\sqrt{\varepsilon}
\end{aligned}$$

对所有 $i\in[n]$。我们得到

$$\begin{aligned}
&\|f_A(X_i)f_A(Z_i)\otimes\mathbb{1}-\mathbb{1}\otimes f_B(X_i)f_B(Z_i)\|_\rho\\
=&\|\Big(f_A(X_i)f_A(Z_i)-f_A(Z_i)f_A(X_i)\Big)\otimes\mathbb{1}+f_A(Z_i)f_A(X_i)\otimes\mathbb{1}-\mathbb{1}\otimes f_B(X_i)f_B(Z_i)\|_\rho\\
\le&\|f_A(Z_i)f_A(X_i)\otimes\mathbb{1}-\mathbb{1}\otimes f_B(X_i)f_B(Z_i)\|_\rho+O(n)\varepsilon^{1/4}\\
=&\|\Big(f_A(Z_i)\otimes\mathbb{1}\Big)\Big(f_A(X_i)\otimes\mathbb{1}-\mathbb{1}\otimes f_B(X_i)\Big)-\Big(\mathbb{1}\otimes f_B(X_i)\Big)\Big(\mathbb{1}\otimes f_B(Z_i)-f_A(Z_i)\otimes\mathbb{1}\Big)\|_\rho+O(\sqrt{n})\varepsilon^{1/4}\\
\le&\|f_A(X_i)\otimes\mathbb{1}-\mathbb{1}\otimes f_B(X_i)\|_\rho+\|\mathbb{1}\otimes f_B(Z_i)-f_A(Z_i)\otimes\mathbb{1}\|_\rho+O(\sqrt{n})\varepsilon^{1/4}\\
\le&O(n^3)\sqrt{\varepsilon}+O(n^3)\sqrt{\varepsilon}+O(\sqrt{n})\varepsilon^{1/4}\le O(n^3)\varepsilon^{1/4}.
\end{aligned}$$

这意味着 $\langle \psi|f_A\ X_i\ f_A\ Z_i\ \otimes f_B\ X_i\ f_B\ Z_i\ |\psi\ = 1-\frac{1}{2}\|f_A\ X_i\ f_A\ Z_i\ \otimes\mathbb{1}-\mathbb{1}\otimes f_B\ X_i\ f_B\ Z_i\ \|_\rho^2 \ge()()()()\rangle()()()()()\sqrt{\varepsilon}$。
因此我们有 $1-O(n^6)$

$$\langle\psi|F_A\otimes F_B|\psi\rangle \ge 1-O(n^6)\sqrt{\varepsilon} \tag{13}$$

对于所有 $F_A\otimes F_B\in\{f_A(X_i)^a f_B(Z_i)^b\otimes f_A(X_i)^a f_B(Z_i)^b:\ a,b\in\{0,1\},\ i\in[n]\}$。

根据定理 4.7，存在希尔伯特空间 H_A^{aux} 和 H_B^{aux}、等距映射 $V_A:\mathrm{H}_A\to\mathbb{C}^{2^n}\otimes\mathrm{H}_A^{aux}$ 和 $V_B:\mathrm{H}_B\to\mathbb{C}^{2^n}\otimes\mathrm{H}_B^{aux}$，以及表示 $\phi_A(g):=\sigma(g)\otimes\mathbb{1}_{\mathrm{H}_A^{aux}}$ 和 $\phi_B(g):=\sigma(g)\otimes\mathbb{1}_{\mathrm{H}_B^{aux}}$，使得 $\|V_A f_A(g)-\phi_A(g)V_A\|_{\rho_A}^2\le O(n^{12})\sqrt{\varepsilon}$，且 $\|V_B f_B(g)-\phi_B(g)V_B\|_{\rho_B}^2\le O(n^{12})\sqrt{\varepsilon}$。

令 $|\widetilde{\psi}\rangle=V_A\otimes V_B|\psi\rangle\in(\mathbb{C}^{2^n}\otimes\mathrm{H}_A^{aux})\otimes(\mathbb{C}^{2^n}\otimes\mathrm{H}_B^{aux})$。那么对于每个 $(F_A\otimes F_B,\Phi_A\otimes\Phi_B)\in\{\Big(f_A(X_i)^a f_B(Z_i)^b\otimes f_A(X_i)^a f_B(Z_i)^b,\phi_A(X_i)^a\phi_B(Z_i)^b\otimes\phi_A(X_i)^a\phi_B(Z_i)^b\Big):\ a,b\in\{0,1\},\ i\in[n]\}$，我们可得

$$\begin{aligned}
&|\langle\psi|F_A\otimes F_B|\psi\rangle-\langle\widetilde{\psi}|\Phi_A\otimes\Phi_B|\widetilde{\psi}\rangle|\\
=&\frac{1}{2}|\|V_AF_A\otimes V_B-V_A\otimes V_BF_B\|_\rho^2-\|\Phi_AV_A\otimes V_B-V_A\otimes\Phi_BV_B\|_\rho^2|\\
=&\frac{1}{2}\Big(|\|V_AF_A\otimes V_B-V_A\otimes V_BF_B\|_\rho+\|\Phi_AV_A\otimes V_B-V_A\otimes\Phi_BV_B\|_\rho|\Big)|\|V_AF_A\otimes V_B\\
&-V_A\otimes V_BF_B\|_\rho-\|\Phi_AV_A\otimes V_B-V_A\otimes\Phi_BV_B\|_\rho|\\
\le&O(n^3)\varepsilon^{1/4}\|V_AF_A\otimes V_B-V_A\otimes V_BF_B-(\Phi_AV_A\otimes V_B-V_A\otimes\Phi_BV_B)\|_\rho\\
\le&O(n^3)\varepsilon^{1/4}\Big(\|V_AF_A\otimes V_B-\Phi_AV_A\otimes V_B\|_\rho+\|V_A\otimes V_BF_B-V_A\otimes\Phi_BV_B\|_\rho\Big)\\
=&O(n^3)\varepsilon^{1/4}\Big(\|V_AF_A-\Phi_AV_A\|_{\rho_A}+\|V_BF_B-\Phi_BV_B\|_{\rho_B}\Big)\le O(n^3)\varepsilon^{1/4}O(n^6)\varepsilon^{1/4}=O(n^9)\sqrt{\varepsilon}.
\end{aligned}$$

由公式（13）可知

$$\langle\widetilde{\psi}|\Phi_A\otimes\Phi_B|\widetilde{\psi}\rangle\ge 1-O(n^9)\sqrt{\varepsilon} \tag{14}$$

对于所有 $\Phi_A\otimes\Phi_B\in\{\varphi_A(X_i)^a\varphi_B(Z_i)^b\otimes\varphi_A(X_i)^a\varphi_B(Z_i)^b:\ a、b\in\{0,1\}、i\in[n]\}$。令 $d:=\dim(\mathrm{H}_A^{aux}\otimes\mathrm{H}_B^{aux})$，并为 $\mathrm{H}_A^{aux}\otimes\mathrm{H}_B^{aux}$ 选取标准正交基 $\{|\kappa_i\rangle\}_{i=1}^d$。于是我们可以写成$|\widetilde{\psi}\rangle=\sum_{j=1}^d\lambda_j|\psi_j\rangle\otimes|\kappa_j\rangle$，其中存在单位向量 $|\psi_j\rangle\in\mathbb{C}^{2^n}\otimes\mathbb{C}^{2^n}$ 和 $\lambda_j\in\mathbb{C}$，使得 $\sum_j|\lambda_j|^2=1$。

对于每个 $j \in [d]$，令 $\delta_j := 1 - \frac{1}{4n} \sum_{a、b \in \{0,1\}、i \in [n]} \psi_j | \Big(\sigma_X(e_i)^a \sigma_Z(e_i)^b \otimes \sigma_X(e_i)^a \sigma_Z(e_i)^b \Big) | \psi_j$。根据引理 4.8，有 $|\psi_j| \Phi^{\otimes n}$ EPR$|^2 \geq \overline{1} - n\delta_j$。式（14）意味着 $\sum_{j=1}^d |\lambda_j|^2 (1-\delta_j) \geq 1 - O(n^9)\sqrt{\varepsilon}$，换句话说，$\sum_j |\lambda_j|^2 \delta_j \leq O(n^9)\sqrt{\varepsilon}$。令 $|aux := \sum_{j=1}^d \lambda_j |\kappa_j \in \mathrm{H}_A^{aux} \otimes \mathrm{H}_B^{aux}$。于是

$$
\begin{aligned}
|\langle \widetilde{\psi} | \Phi_{\mathrm{EPR}}^{\otimes n}, aux \rangle| &= \sum_{j=1}^d |\lambda_j|^2 |\langle \psi_j | \Phi_{\mathrm{EPR}}^{\otimes n} \rangle| \geq \sum_{j=1}^d |\lambda_j|^2 |\langle \psi_j | \phi_{2^n} \rangle|^2 \\
&\geq \sum_{j=1}^d |\lambda_j|^2 (1 - n\delta_j) = 1 - n \sum_{j=1}^d |\lambda_j|^2 \delta_j \geq 1 - O(n^{10})\sqrt{\varepsilon}.
\end{aligned}
$$

由于任意复相位都可以吸收到 $|aux\rangle$中，我们不妨设$\widetilde{\ }\langle \psi | \Phi^{\otimes n}{}_{\mathrm{EPR}}\, aux \rangle \geq 0$。由此可得

$$
\| |\widetilde{\psi}\rangle - |\Phi_{\mathrm{EPR}}^{\otimes n}, aux\rangle \|^2 = 2 - 2\langle \widetilde{\psi} | \Phi_{\mathrm{EPR}}^{\otimes n}, aux \rangle \leq O(n^{10})\sqrt{\varepsilon}.
$$

那么对于任意 $g \in H(n)$，我们有

$$
\begin{aligned}
&\| (V_A \otimes V_B) \Big(f_A(g) \otimes \mathbb{1}_{\mathcal{H}_B} |\psi\rangle \Big) - \Big(\sigma(g) \otimes \mathbb{1}_{\mathbb{C}^{2^n}} |\Phi_{\mathrm{EPR}}^{\otimes n}\rangle \Big) \otimes |aux\rangle \| \\
\leq &\| \Big(V_A f_A(g) - \phi_A(g) V_A \Big) \otimes V_B |\psi\rangle \| + \| \phi_A(g) \otimes \mathbb{1}_{\widetilde{\mathcal{H}}_B} (|\widetilde{\psi}\rangle - |\Phi_{\mathrm{EPR}}^{\otimes n}, aux\rangle) \| \\
= &\| V_A f_A(g) - \phi_A(g) V_A \|_{\rho_A} + \| |\widetilde{\psi}\rangle - |\Phi_{\mathrm{EPR}}^{\otimes n}, aux\rangle \| \leq O(n^6)\varepsilon^{1/4} + O(n^5)\varepsilon^{1/4} \leq O(n^6)\varepsilon^{1/4}.
\end{aligned}
$$

我们得出，对于所有 $g \in H(n)$，$\|(V_A \otimes V_B) \Big(f_A(g) \otimes \mathbb{1}_{\mathcal{H}_B} |\psi\rangle \Big) - \Big(\sigma(g) \otimes \mathbb{1}_{\mathbb{C}^{2^n}} |\Phi^{\otimes n}{}_{\mathrm{EPR}}\rangle \Big) \otimes |aux\rangle \|^2 \leq O(n^{12})\sqrt{\varepsilon}$。

□

回忆一下，对于任意 $W \in \{X, Z\}^n$ 以及 $a \in \{0,1\}^n$，我们用 $\sigma_W(a)$ 表示泡利算子 $\otimes_{i=1}^n \sigma_{W_i}^{a_i}$ 的张量积。在 LWPBT 的典范完美策略中，Alice 在问题 $W(a)$ 上执行 $\sigma_W(a) \in \mathrm{I}_A$。由于 $|a| \leq 6$ 对于所有 $W(a) \in \mathrm{I}_A$，由定理 4.9 和定理 3.4 可立即得到：

推论4.10. 存在常数 $C_{\mathrm{lw}} > 0$ 使得以下结论成立。对于任意 $\varepsilon > 0, n \in \mathbb{N}$，以及针对 n量子比特 *LWPBT* 的策略 $S = (\tau^A, \tau^B, |\psi\rangle \in H_A \otimes H_B)$，其获胜概率为$1-\varepsilon$，存在等距映射 $V_A : H_A \to (\mathbb{C}^2)^{\otimes n} \otimes H_A^{aux}, V_B : H_B \to (\mathbb{C}^2)^{\otimes n} \otimes H_B^{aux}$以及一个单位向量$|aux\rangle \in H_A^{aux} \otimes H_B^{aux}$使得

$$
\| (V_A \otimes V_B) \Big(\tau^A(W(a)) \otimes Id_{\mathcal{H}_B} |\psi\rangle \Big) - \Big(\sigma_W(a) \otimes Id_{\mathbb{C}^{2^n}} |\Phi_{EPR}^{\otimes n}\rangle \Big) \otimes |aux\rangle \| \leq C_{\mathrm{lw}} n^6 \varepsilon^{1/4}
$$

对于所有 $W(a) \in I_A$。

4.3 相关自测试

我们了解到另外两种自测试，即 2-out-of-n CHSH 博弈 [CRSV18], 以及 2-out-of-n 魔方（MS）博弈 [MNY22], ，它们可以测试 n EPR 对，但只要求诚实玩家实现常数大小的泡利测量。更准确地说，2-out-of-n CHSH 博弈是针对 n EPR 对的自检，而 [MNY22] 中给出的博弈是在对易算子模型中研究的，并测试维数为 2^n的希尔伯特空间，尽管 2-out-of-n MS博弈的分析可以扩展到张量积模型，将其作为对 EPR 对的测试。2-out-of-n MS 具有大约$n^4\sqrt{\varepsilon}$ 的鲁棒性，而 2-out-of-n CHSH 博弈在测试该状态时具有 $n\sqrt{\varepsilon}$ 鲁棒性。

在我们的设置中，我们要求一种能够完美获胜的自检，并且还能够测试权重不超过 6 的泡利测量的任意编织。我们猜想，对于 2-out-of-n MS 的一个修改版本，也可以证明类似的自检性质，其中包括额外的一致性检查。我们相信，可以使用定理 4.1 中的群论方法来确认这些额外的自检性质，但这可能需要进行与第4.2节所给出的类似技术处- 理。LWPBT 和修改后的 2-out-of-n MS 都有 $poly(n)$ 许多问题和数量恒定的答案，并且具有 $poly(n)\sqrt{\varepsilon}$ 鲁棒性。

5 修正哈密顿量博弈

在本节中，我们展示对于某个局部哈密顿量 H，可以构造一个非局域博弈$\mathcal{G}(H)$，其获胜概率与 $\lambda_0(H)$的基态能量 H密切相关。我们的博弈基于 Grilo 引入的哈密顿量博弈 [Gri19], ，但为了实现零知识性质，我们进行了一些细微的重新配置。具体而言，我们不再像 [Gri19], 中那样使用泡利编织测试，而是针对不诚实量子证明者采用低权重 Pauli 编织测试，然后执行并行重复，以实现常数完备性-可靠性间隙。为了将 LWPBT 纳入我们修改后的哈密顿量测试中，我们考虑具有特定结构的哈密顿量：

定义5.1。 我们称一个哈密顿量 H 是 XZ型的，如果它可以分解为 $H = \frac{1}{m}\sum_{\ell=1}^{m}\gamma_\ell H_\ell$,其中每个 $\gamma_\ell \in [-1,1]$ 以及每一项 H_ℓ都是算子 σ_X， σ_Z或 σ_I的张量积。

接下来，我们定义相关的能量测试，该测试类似于 [Gri19]中所使用的能量测试。

定义 5.2 （能量测试）。 给定一个 XZ 型的 n 量子比特 6-局部哈密顿量$H = \frac{1}{m}\sum_{\ell=1}^{m}\gamma_\ell H_\ell$， 我们定义如下能量测试：

1. 验证者从 $\ell \in [m]$ 中均匀随机选取一项 H_ℓ，并从满足 $\sigma_W(r) = H_\ell$ 的配对 $\{(W,r) \in \{X,Z\}^n \times \{0,1\}^n$ 中均匀随机选取一对。*2.* 验证者向 *Alice* 发送 $W(r)$，并告知 *Bob* 参与者正在进行能量测试。*3. Alice* 回复单个值 $c \in \{-1,1\}$，*Bob* 回复 $2n$ 个比特 $a_1,\dots a_n, b_1,\dots b_n$。*4.* 接下来，验证者按如下方式计算比特串 d 。若 $r_i = 1$ 且 $W_i = X$，则取 $d_i = (-1)^{a_i}$ ；若 $r_i = 1$ 且 $W_i = Z$，则取 $d_i = (-1)^{b_i}$ ；其他情况则取 $d_i = 0$ 。*5.* 若 $c \cdot \prod_i d_i \neq sign(\gamma_l)$，验证者接受；否则以 $|\gamma_l|$ 的概率拒绝。结合 *LWPBT* 和上述能量测试，我们定义修正后的哈密顿量测试：

定义 5.3 （哈密顿量测试）。 设 $H = \frac{1}{m}\sum_{\ell=1}^{m}\gamma_\ell H_\ell$ 是一个 k-局部哈密顿量，属于 XZ-类型，并且设 $p \in (0,1)$ 。我们定义如下博弈 $\mathcal{G}$（H， p）：以概率 （$1-p$） 玩家进行第 *SectionSection 3*中介绍的 *LWPBT*；以概率 p 玩家进行定义 *5.2*中描述的能量测试。

我们将策略 $\mathcal{S}$ 用于 $\mathcal{G}(H,p)$ 称为半诚实策略，如果参与者在进行 LWPBT 时采用典范完美策略。因此，在半诚实策略中，Alice 和 Bob 持有 n EPR 对，而 Alice 必须在问题 $W(r)$ 上执行 $\sigma_W(r)$，因为她无法区分来自 LWPBT或能量测试的问题。我们还定义了诚实策略 $\mathcal{S}_h$ 用于 $\mathcal{G}(H,p)$ ，其中参与者在进行 LWPBT 时采用典范完美策略；在能量测试中，Bob 诚实地将 H 的基态隐形传态给 Alice，并向验证者提供隐形传态密钥。

下面我们分析在玩家采用半诚实策略的假设下，他们赢得整个博弈$\mathcal{G}(H,p)$ 的能力。

引理 5.4 (半诚实策略的下界)。 假设 $H = \frac{1}{m}\sum_{l=1}^{m}\gamma_l H_l$ 是一个 n量子比特6局部 *XZ* 哈密顿量，且 *Alice* 和 *Bob* 正在为 $G(H,p)$执行半诚实策略 S。那么

$$\omega(\mathcal{S}) \le \omega(\mathcal{S}_h) = 1 - p(\frac{1}{2m}\sum_{l}|\gamma_l| + \frac{1}{2}\lambda_0(H)).$$

证明。 假设玩家采用半诚实策略 $\mathcal{S} = (\tau^A, \tau^B, |\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B)$ 来参与$\mathcal{G}(H,p)$。令 $\tau := \mathrm{Tr}^{\mathcal{H}_B}(|\psi\rangle\langle\psi|)$。由于玩家在 LWPBT 中完美获胜，只有当他们参与的是能量测试实例时，才会输掉整个博弈。令 $a, b \in \{0,1\}^n$ 为 Bob 在能量测试中给出的答案，并令 $\rho := \sigma_X^b \sigma_Z^a \tau \sigma_Z^a \sigma_X^b$。

假设在能量测试的一轮中，验证者选取一个 $\ell \in [m]$，并为 Alice 选择一个 $W(r)$。如上所述，由于 Alice 无法区分来自 LWPBT 和能量测试的问题，她必须在自己的寄存器上执行 $\sigma_W(r) = H_\ell$。因此 $\mathbb{E}(c \cdot \prod_i d_i) = \mathrm{Tr}(H_\ell \sigma_X^b \sigma_Z^a \tau \sigma_Z^a \sigma_X^b) = \mathrm{Tr}(H_\ell \rho)$。令 p_ℓ 为 $c\prod_i d_i = sign(\gamma_\ell)$ 的概率。那么 $\mathbb{E}(c\prod_i d_i) = p_\ell sign(\gamma_\ell) - (1-p_\ell) sign(\gamma_\ell)$，换言之， $\gamma_\ell \mathbb{E}(c\prod_i d_i) = (2p_\ell - 1)|\gamma_\ell|$。这意味着验证者以如下概率拒绝

$$p_\ell|\gamma_\ell| = \frac{|\gamma_\ell| + \gamma_\ell \mathbb{E}(c\prod_i d_i)}{2} = \frac{|\gamma_\ell| + \gamma_\ell \mathrm{Tr}(H_\ell\rho)}{2}.$$

因此，通过 ave 遍历 $\ell \in [m]$，我们看到玩家以概率未通过能量测试

$$\frac{1}{m}\sum_{\ell\in[m]}\frac{|\gamma_\ell| + \gamma_\ell \mathrm{Tr}(H_\ell\rho)}{2} = \frac{1}{2m}\sum_{\ell\in[m]}|\gamma_\ell| + \frac{1}{2}\mathrm{Tr}(H\rho).$$

当且仅当 ρ 确实是 H 的基态密度矩阵时，该概率才会达到最小值；在这种情况下，赢得整个博弈的概率至多为

$$1 - p\Big(\frac{1}{2m}\sum_{\ell\in[m]}|\gamma_\ell| + \frac{1}{2}\lambda_0(H)\Big).$$

如果 Bob 在能量测试中传送基态并向验证者提供验证密钥，就可以达到这一概率。

□

引理 5.5。（不诚实策略的上界）设 $H = \frac{1}{m}\sum_{\ell=1}^{m}\gamma_\ell H_\ell$ 是一个 6-局部、 n-量子比特哈密顿量，属于 XZ-型。对于任意 $\eta \in (0,1)$，令 $p = \frac{4n^{-6}\eta^{3/4}}{(C_{\mathrm{lw}}+1)\,3^{3/4}}$，其中 C_{lw} 是推论*4.10*中给出的常数。那么

$$\omega^*\Big(\mathcal{G}(H,p)\Big) \le \omega(\mathcal{S}_h) + \eta,$$

其中 $\omega(\mathcal{S}_h) = 1 - p\Big(\frac{1}{2m}\sum_{\ell\in[m]}|\gamma_\ell| + \frac{1}{2}\lambda_0(H)\Big)$ 如引理 *5.5*。

证明。假设证明者在针对 G(H,p) 的策略 S $= (\tau^A, \tau^B, |\psi$下，以概率 $1-\varepsilon$ 赢得 LWPBT，并以概率 $\delta + 1 - \frac{\sum_\ell|\gamma_\ell|}{2m} - \lambda_0(H)$ 2 赢得能量测试。推论 4.10 表明 $\delta \le C_{\mathrm{lw}} n^6 \varepsilon^{1/4}$。那么对于 p: $= \frac{4n^{-6}\eta^{3/4}}{(C_{\mathrm{lw}}+1)3^{3/4}}$，其中 $\eta \in (0,1)$，我们有 $\eta + \varepsilon = \eta/3 + \eta/3 + \eta/3 + \varepsilon \ge 4(\frac{\eta^3\varepsilon}{3^3})^{1/4} = p(C_{\mathrm{lw}}+1)n^6\varepsilon^{1/4}$。由此可得

$$p\delta - (1-p)\varepsilon \le pCn^6\varepsilon^{1/4} + p\varepsilon - \varepsilon \le pC_{\mathrm{lw}}n^6\varepsilon^{1/4} + pn^6\varepsilon^{1/4} - \varepsilon = p(C_{\mathrm{lw}}+1)n^6\varepsilon^{1/4} - \varepsilon \le \eta.$$

因此，总体获胜概率为

$$\omega(\mathcal{S}) = (1-p)(1-\varepsilon) + p(\delta + 1 - \frac{\sum_\ell |\gamma_\ell|}{2m} - \frac{\lambda_0(H)}{2}) = \omega(\mathcal{S}_h) + p\delta - (1-p)\varepsilon \le \omega(\mathcal{S}_h) + \eta.$$

□

在本文的其余部分，给定一个 n量子比特、6-局部哈密顿量 H XZ型以及参数α和 β，满足 $\beta - \alpha \ge 1/poly(n)$，我们使用 $\mathcal{G}(H)$ 表示博弈 $\mathcal{G}(H,p)$，其中 $p = {}^{32n^{-6}}(\quad \beta-\alpha\ {}^{24})()$。

定理5.6。给定一个 n量子比特的6局部哈密顿量 $H = \frac{1}{m}\sum_{\ell=1}^{m}\gamma_\ell H_\ell$ 和参数 ${}^{27}\ C_{\mathrm{lw}}+1\ {}^{4}\ \alpha,\ \beta$ 其中$\beta - \alpha \ge 1/poly(n)$，令 ω_α （分别令 ω_β）表示 $G(H)$ 在$\lambda_0(H) \le \alpha$ （分别 $\lambda_0(H) \ge \beta$）下的最大获胜概率。则 $\omega_\alpha - \omega_\beta \ge 1/poly(n)$。

证明。设 $\eta := {}^{16}(\quad \beta-\alpha\ {}^{32})\ (\ )^{4}$，并令 $p := {}^{4n^{-6}\eta^{3/4}}(C_{\mathrm{lw}}+1)3^{3/4}$。则 $p = {}^{32n^{-6}}(\quad \beta-\alpha\ {}^{24})\ (\ )^{4}$，因此 $\mathsf{G}(H) = \mathsf{G}(H,p)$。由引理 5.4 和引理 5.5 可得 $\omega(\mathsf{S}_h) \le \omega^*\Big(\mathsf{G}(H,p)\Big) \le \omega(\mathsf{S}_h) + \eta$。这意味着 $\omega_\alpha \ge 1 - p(\frac{1}{2m}\sum_\ell|\gamma_\ell| + \frac{1}{2}\alpha)$ 且 $\omega_\beta \le 1 - p(\frac{1}{2m}\sum_\ell|\gamma_\ell| + \frac{1}{2}\beta) + \eta$。由于 $n^6(\beta-\alpha)^7 \le O(n^{-1})$，因此

$$\omega_\alpha - \omega_\beta \ge \frac{1}{2}p(\beta-\alpha) - \eta = \frac{16n^{-6}(\beta-\alpha)^{25}}{27(C_{\mathrm{lw}}+1)^4}(1 - n^6(\beta-\alpha)^7) \ge \frac{16n^{-6}(\beta-\alpha)^{25}}{27(C_{\mathrm{lw}}+1)^4} \ge \frac{1}{poly(n)}.$$

□

我们采用的间隙放大方法沿用了 [GSY19] 的方法：对完美完备性博弈的锚定版本进行并行重复。关键区别在于，我们的底层博弈不满足完美完备性。因此，我们将 Yuen 提出的阈值并行重复定理应用于这些博弈的锚定版本。

对于每个 $n \in \mathbb{N}$，令 $\mathsf{G}(H)$、w_α和 w_β如定理5.6所述。根据 [Yue16，定理 41]，，存在一个 $poly(n)$-可计算的变换，称为锚定，它将 $\mathsf{G}(H)$变换为一个双人博弈 $\mathsf{G}(H)_\perp$，其获胜概率为 $1 - {}^{1-w^*}(\mathsf{G}(H))\ 2$。因此，$w^*(\mathsf{G}(H)_\perp) = \begin{cases} 1-\varepsilon_\alpha & \lambda_0(H) \le \alpha \\ 1-\varepsilon_\beta & \lambda_0(H) \ge \beta \end{cases}$，其中 ε_α：$= 1 - w_\alpha$ 且 $\varepsilon_\beta := 1 - w_\beta$。接着，根据 [Yue16，定理 42]，，存在一个普适常数$C > 0$，使得对于所有整数 $m \ge 1$和 $\gamma \ge 0$，在博弈 $\mathsf{G}(H)_\perp^m$ 中，玩家获胜的博弈数超过 $\Big(w^*(\mathsf{G}(H)_\perp) + \gamma\Big)m$ 的概率至多为 $(1-\gamma^9/2)^{Cm}$。取 $\gamma := {}^{\varepsilon_\alpha-\varepsilon_\beta}_{4}$，并令 $m =$ 为 $\max\{4\gamma^{-2}, 2C\gamma^{-9}\}$。令 $\widehat{\mathsf{G}}(H) := \mathsf{G}(H)_\perp^m$ 为 $\mathsf{G}(H)$ 的 m 并行重复锚定版本。我们证明，这个非局域博弈具有常数完备性-可靠性间隙。

定理 5.7。令 $\widehat{\omega}_\alpha$（分别地，$\widehat{\omega}_\beta$）为在 $\lambda_0(H) \le \alpha$（分别地，$\lambda_0(H) \ge \beta$）时 $\widehat{G}(H)$ 的最大获胜概率。那么 $\widehat{\omega}_\alpha - \widehat{\omega}_\beta \ge 1/4$。

证明。如果 $\lambda_0(H) \ge \beta$，那么 $\widehat{\omega}_\beta \le (1 - \frac{\gamma^9}{2})^{Cm} \le (1-\frac{\gamma^9}{2})^{2/\gamma^9} < e^{-1} < 1/2$。现在假设 $\lambda_0(H) \le \alpha$。对于 $\mathsf{G}(H)_\perp$，一个最优策略 S的获胜概率为 $1 - \frac{\varepsilon_\alpha}{2}$。设 X为该策略 S^m 获胜的博弈次数这一随机变量。那么 $X \sim$服从 $\mathrm{Binomial}(m, 1-\frac{\varepsilon_\alpha}{2})$，因此 $\mathbb{E}X = m(1-\frac{\varepsilon_\alpha}{2})$ 且$\mathrm{Var}X = m\frac{\varepsilon_\alpha}{2}(1-\frac{\varepsilon_\alpha}{2})$。由于 $(1-\frac{\varepsilon_\alpha}{2}) - (1 - \frac{\varepsilon_\beta}{2} + \gamma) = \frac{\varepsilon_\beta - \varepsilon_\alpha}{2} - \gamma = \gamma$，我们得到

$$\begin{aligned} Pr(X \le (1 - \tfrac{\varepsilon_\beta}{2} + \gamma)m) &= Pr((1-\tfrac{\varepsilon_\alpha}{2})m - X \ge \gamma m) \\ &\le Pr(|X - \mathbb{E}X| \ge \gamma m) \\ &\le \frac{m(1-\frac{\varepsilon_\alpha}{2})\frac{\varepsilon_\alpha}{2}}{(\gamma m)^2} = \frac{1}{m\gamma^2} \le 1/4. \end{aligned}$$

This im 层 $\widehat{\omega}_\alpha \ge w(S^m) = 1 - Pr(X \le (1 - \frac{\varepsilon_\beta}{2} + \gamma)m) \ge 3/4$，因此定理得证 . □

6 零知识证明系统

在本节中，我们证明定义 5.3 中描述的博弈族构成一个统计零知识 MIP*[2, 1] 协议，可用于解决具有逆多项式完备性/可靠性间隙的 QMA 问题。首先，我们介绍该协议。

6.1 XZ-哈密顿量的历史态模拟

在介绍我们的 MIP* 协议并继续讨论零知识方面的结果之前，我们将重新表述一个最初由 Broadbent 和 Grilo [BG22]（引理 3.5）提出的结果，使其更适用于设备无关技术。

定理 6.1（历史态模拟）。对于（$L = L_{yes}, L_{no}$）中的任意语言 QMA 以及$s \in \mathbb{N}$，存在一族验证电路 $V_{(s)x} = U_T \dots U_1$，对于 L，该电路作用于大小为$p(|x|)$ 的见证和 $q(|x|)$ 个辅助量子比特上，使得存在一个多项式时间确定性算法$Sim_{V^{(s)}}$。该算法以实例 $x \in L$ 和一个满足 $|S| \leq 3s+2$ 的子集 $S \subseteq [T+p+q]$ 作为输入，然后输出一个 $|S|$-量子比特密度矩阵 $\rho(x, S)$ 的经典描述，并具有以下性质：

1. 若 $x \in L_{yes}$，则存在一个 $p(|x|)$ 量子比特见证 ψ^s，使得 $V_x^{(s)}$在 ψ^s 和 $\|\rho(x,S) - \mathrm{Tr}_S(\rho)\|_{tr} \leq negl(|x|)$上以至少 $1 - negl(n)$ 的概率接受，其中

$$\rho = \frac{1}{T+1} \sum_{t,t' \in [T+1]} |unary(t)\rangle\langle unary(t)| \otimes U_t \dots U_1(\psi^s \otimes |0\rangle\langle 0|^{\otimes q}) U_1^* \dots U_{t'}^*$$

是 $V_x^{(s)}$在见证 ψ^s上的历史态。

2. 令 H_i 为 $V_x^{(s)}$的电路到局部哈密顿量构造中的一项，并令 S_i 为 H_i 非平凡作用于其上的量子比特集合。则对所有$x \in L$，$\mathrm{Tr}(H_i \rho(x, S_i)) = 0$。

3. 电路到局部哈密顿量构造得到的哈密顿量 H 是一个 XZ 类型的6-局部哈密顿量。

证明。Broadbent 和 Grilo 使用由另一组物理门构造的可模拟码证明了前两点 [BG22]。简而言之，Broadbent 和 Grilo 提出了一种构造性方法；对于每个 $x \in L$，该方法都提供一种变换，将原始验证电路 V变换为一个可模拟的验证电路 $V_x^{(s)}$，该电路包含 4 个主要阶段：

(i) 验证者接收一个编码见证态，并检查所提供的见证是否已在相关编码 $\mathcal{C}$ 下正确编码；(ii) 创建辅助资源态 $|0\rangle$、$|T\rangle$ 并在$\mathcal{C}$ 下对其进行编码；(iii)在编码见证态上，使用横向Clifford门或 T-门的适当编码，对原始验证电路 V执行编码版本，其中使用 $|T\rangle$；(iv) 对计算的输出进行解码。

对于每个 c 常数 s 该CECC $\mathcal{C}$ 被取为 log$(3s+5)$-重拼接的 Steane 编码 .

定理 2.10 通过使用相同的编码$\mathcal{C}$ 并利用资源态 |托福利门⟩应用 3 量子比特托福利门得到；该资源态可由 $|000\rangle$ 利用 H 和 $\Lambda^2(X)$构造。我们

的结果随后可通过适当修改资源生成阶段(ii) 来创建辅助态 $|0\rangle$ 和 $|$托福利门$\rangle$的编码而得出。然后，将阶段(iii) 改为使用门集$\{H, \Lambda(X), \Lambda^2(X)\}$的编码来应用原始电路的编码。

要了解这种门集变化如何带来第三个结果，请注意，对于任意门 G ，我们有$\Lambda(G) = \frac{1}{2}(I + Z)$ $\otimes I + \frac{1}{2}(I - Z) \otimes G$。利用这一分解，我们可以轻易验证，门 $\Lambda(X)$ 和 $\Lambda^2(X)$ 都可以表示为 X 、Z和 I的张量积的实线性组合。 $H = \frac{1}{\sqrt{2}}(X + Z)$也同样如此。因此，在阶段（$ii$）和（$iii$）中使用的所有物理门，都由可以表示为 X和 Z的张量积的实线性组合的门构成。在阶段 i）和（ iv）中使用的物理门也同样如此。我们还将得到，所有这些门的阶数都是 2。最后，按照 Ji 的相同方法（引理 22 [Ji16]），我们得到 H 是 6-局部且属于 XZ 类型。

□

下面我们只需调用定理 6.1 针对 $s = 2$ 以实现我们的零知识协议。我们使用 V_x 来表示 $V_x^{(2)}$ 在本节剩余部分中。

6.2 用于 QMA 的双证明者零知识证明系统

设 $L = (L_{yes}, L_{no})$ 是 QMA 中的一个语言。图 5 描述了一个针对 L 的双证明者单轮交互证明系统，其完备性-可靠性间隙为常数。

$$x \xrightarrow{\text{定理 6.1}} V_x \xrightarrow{\text{circuit-to-Hamiltonian}} H_x \xrightarrow{\text{Definition 5.3}} \mathcal{G}_x := \mathcal{G}(H_x) \xrightarrow{\text{Theorem 5.7}} \widehat{\mathcal{G}}_x := \widehat{\mathcal{G}}(H_x)$$

图 5： x 是 $L \in$ QMA中的一个实例。 V_x 是一个 $poly(|x|)$规模的量子电路。 H_x 是一个 $poly(|x|)$量子比特的 6-局部$\widehat{}$ XZ类型哈密顿量。$\mathcal{G}_x$ 是一个非局域博弈，其问题长度为 $poly(|x|)$比特，答案长度为 $poly(|x|)$比特。

更具体地说，对于任意 $x \in L$，应用定理 6.1，结合 $s = 2$，可得到一个 $poly(|x|)$-大小的验证电路 V_x，而电路到哈密顿量构造会生成一个 $poly(|x|)$-量子比特$\widehat{}$6局部哈密顿量 H_x ，其类型为 XZ型。随后，我们可以按照第 *5* 节构造一个非局域博弈 G_x ，如第 5节所述。根据定理5.7，完备性-可靠性间隙为常数。从实例$\backsim x \in L$ 到非局域博弈 $\mathcal{G}_x$ 的映射是高效的，因为图 5 中描述的每一步都是高效的。

为了证明上述交互式证明系统针对 L 具有统计零知识性质，$\widehat{}$我们首先证明，对于任意恶意验证者 V和 $x \in L_{yes}$，存在一个概率多项式时间模拟器，可以从 $View(\widehat{V}(x), \mathcal{S}_h)$中进行采样，其中 $\mathcal{S}_h$ 是 $\mathcal{G}_x$ 在第 5节中定义的诚实策略。

引理 6.2。 假设对于某个语言 $L = (L_{yes}, L_{no})$ ，有 $x \in L_{yes}$ 属于 QMA。令 G_x 为图 *5* 中描述的相应非局域博弈，令 S_h 为第$\widehat{}$ 节中定义的 G_x 的诚实策略。对于任意恶意验证者 V，都存在一个概率多项式时间算法 $Sim_{\widehat{V}}$，其输出分布与 $View(\widehat{V}(x), S_h)$ 的距离可忽略，

证明。设 H_x 为相应的哈密顿量，并假设 H_x 作用于 n 个量子比特上（$n = poly(|x|)$）。回想一下，在 $\mathcal{S}_h$ 中，Alice 和 Bob 在共享的 n-EPR 对$|\Phi^{\otimes n}{}_{\text{EPR}}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ 上进行测量。Bob 还有一个额外的 n 量子比特寄存器 $\mathcal{H}_{B'}$ ，其中保存着 H_x 的基态 ρ 的副本。令 $\mathcal{H}_{A,i}$、$\mathcal{H}_{B,i}$ 和 $\mathcal{H}_{B',i}$ 分别表示 Alice 或 Bob 在各自寄存器上的第 i 个量子比特。

$\widehat{}$如第2.5节恶意验证者V 所讨论的，其首先抽取 q_1 Alice或 Bob 的所有可能问题集合上的某个分布来提出第一个问题。给定一个回答 r_1 第二个$\widehat{}$问题 q_2 是使用分布进行条件抽样的。由于 V 是概率多项式时间，模拟器 $Sim_{\widehat{V}}$ 也可以在使用相同随机性的情况下，从这些分布中进行抽样。对于如何有条件地产生回答，我们考虑以下几种情况。

如果问题 q_1 和 q_2 都不是能量测试请求，那么在诚实策略中，双方都将在其共享的 n-EPR 对上进行一次或多次泡利测量，因此模拟器可以高效地产生回答。这里玩家的顺序并不重要，因为模拟器可以先随机生成第一位玩家的回答 r_1，然后根据交互记录中之前的条目，计算第二位玩家适当的回答 r_2。

假设 q_1 是发送给 Bob 的能量测试请求。在诚实策略中，Bob 对 $\mathcal{H}_B \otimes \mathcal{H}_{B'}$执行 n 次贝尔测量。模拟器可以在 Bob 收到能量测试请求的条件下，通过均匀采样 $2n$ 个随机比特来生成回答 r_1：$(\alpha, \beta) = (\alpha_1, \cdots, \alpha_n, \beta_1, \cdots, \beta_n)$。在诚实策略中，Alice 此时应当在她的寄存器 $\mathcal{H}_A$ 上拥有 $\rho_{\alpha,\beta}$：$= \sigma_Z^{\beta}\sigma_X^{\alpha}\rho\sigma_X^{\alpha}\sigma_Z^{\beta}$，其中 σ_W^r表示 $\otimes_{i\in[n]}\sigma_W^{r_i}$对于 $W \in \{X, Z\}$ 以及 $r \in \{0,1\}^n$。

由此可知，q_2 必定是对 Alice 的测量请求。它可以是如下形式之一：对于某个 $W \in \{X, Z, I\}^n$ 和某个 $a \in \{0,1\}^n$，$\sigma_W(a)$ 满足 $|a| \leq 6$；或者 $\sigma_{XZ} \otimes \sigma_{ZX}(a)$ 满足 $|a| = 2$。若 S 是 Alice 的可观测量非平凡作用的量子比特集合，那么根据定理 6.1，存在一个多项式时间算法，可以输出一个密度矩阵 $\rho(x, S)$ 的描述，使其满足

$$\|\mathrm{Tr}_{\overline{S}}(\rho) - \rho(x, S)\|_{tr} \leq negl(n). \tag{15}$$

$Sim_{\widehat{V}}$随后可以使用对 Alice 在 S 的量子比特上进行诚实测量所得结果的近似值，将 r_2 附加到交互记录中，β。此近似值可通过 $\rho(x, S)$ 计算，因为

$$\mathrm{Tr}_{\overline{S}}(\sigma_Z^{\beta}\sigma_X^{\alpha}\rho\sigma_X^{\alpha}\sigma_Z^{\beta}) = \Big(\bigotimes_{i\in S}\sigma_Z^{b_i}\sigma_X^{a_i}\Big)\mathrm{Tr}_{\overline{S}}(\rho)\Big(\bigotimes_{i\in S}\sigma_Z^{b_i}\sigma_X^{ai}\Big).$$

最后，我们考虑 Alice 首先收到测量请求 q_1 并在收到回答 r_1 后，验证者向 Bob 发送针对 q_2的能量测试请求的情形。为了生成给 Alice 的回答，模拟器将首先生成一个均匀随机的回答 r_1。我们记 $\Phi_{q_1,\ r_1}$ 为依据 q_1 测量共享 EPR 对并得到结果 r_1后，在 $\mathcal{H}_A \otimes \mathcal{H}_B$ 上的测量后状态。在诚实策略下，整体共享态为

$$\tau_{q_1,r_1} := \Phi_{q_1,r_1} \otimes \rho \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_{B'},$$

而 Bob 将在量子寄存器 $\mathcal{H}_B \otimes \mathcal{H}_{B'}$上执行相互独立的贝尔测量。同样，我们记 S为 Alice 在收到问题 q_1 后进行测量的量子比特集合。于是有

$$\mathrm{Tr}_{\overline{S}}(\tau_{q_1,r_1}) = \mathrm{Tr}_{\overline{S}}(\Phi_{q_1,r_1}) \otimes \mathrm{Tr}_{\overline{S}}(\rho).$$

由方程（15）可得

$$\|\mathrm{Tr}_{\overline{S}}(\tau_{q_1,r_1}) - \mathrm{Tr}_{\overline{S}}(\Phi_{q_1,r_1}) \otimes \rho(x, S)\|_{tr} \leq negl(n).$$

因此，模拟器可以如下生成条件回答 $(\alpha, \beta) = (\alpha_i, \beta_i)_i$。首先，根据定理 6.1计算约化密度矩阵 $\rho(x, S)$。对于 $i \in S$，按照 $\mathrm{Tr}_S(\Phi_{q_1,r_1}) \otimes \rho(x, S)$上各种可能贝尔测量结果的概率，对 (α_i, β_i) 进行采样。对于剩余的$i \notin S$，模拟器可以均匀随机地采样数对(α_i, β_i)。

在上述所有情况下，都能保证模拟器的输出与.....仅有可忽略的差异，因此，$Sim_{\widehat{V}}$的输出与$View(x,\mathcal{S})$仅有可忽略的差异。 □

剩下要做的，就是论证图 5 所描述的、基于^放大后的博弈 $\mathcal{G}_x$ 的交互式协议是统计零知识的。

定理6.3。 图中描述的协议5 是统计零知识的，并且具有常数完备性-可靠性间隙。

证明。 常数完备性-可靠性间隙直接由定理 5.7得出。若要证明统计零知识，我们首先考虑博弈$\mathcal{G}_x$的锚定过程。我们可以通过为诚实策略中接收到问题 $\perp$ 的任一玩家固定一个输出选项，为$\mathcal{G}_x$ 的锚定版本指定一个诚实策略$\mathcal{S}_{h,\perp}$ 用于。然后，给定任意恶意验证者 $\widehat{V}(x)$，定理6.3 中给出的模拟器可以轻易修改为从一个与 $View(\widehat{V}(x),\ \mathcal{S}_{h,\perp})$仅有可忽略差异的分布中进行采样。

^对于阈值并行重复博弈$\mathcal{G}_x$，诚实策略 $\mathcal{S}_{h,\perp}^{m}$ 取为诚实策略的$\mathcal{S}_{h,\perp}$的 m重积。于是，正如 [GSY19]，中所述，由于协议只会查询每位参与者一次，因此可以通过按照上述引理中所用模拟器的 m重积进行采样，得到一个新的模拟器。

□

7 现成模型

本节将形式化定义 OTS 模型（第 7.1 节）。在第 7.2 节中，我们陈述主要的概念性定理，这些定理运用了本文主体部分中的所有技术性贡献。

7.1 模型的形式化描述

这里我们对 OTS 模型作形式化描述。该模型定义为 MIP* 的一种细化，其中弱化了完备性条件，允许证明者中只有一方是“全能的”，而另一方的功能受限，且其功能独立于问题实例。

现成设备。我们首先对现成设备族的定义作形式化描述。验证设备 $D=(|\psi\rangle,\{P_a^1\}_a,\ldots,\{P_a^q\}_a)$ 由希尔伯特空间 $\mathrm{K}_A\otimes\mathrm{K}_B$ 上的状态 $|\psi\rangle$ 以及 K_A 上的一组 POVM $\{P_a^1\}_a,\ldots,\{P_a^q\}_a$ 构成。回顾一下，非局域博弈的量子策略由第 2 节所述形式的元组 $\mathrm{S}=(\{E_a^x\}_{x,a},\{F_b^y\}_{y,b},|\phi\rangle\in\mathrm{H}_A\otimes\mathrm{H}_B)$ 确定。若某个量子策略 S 可以使用 D 实现，则称其满足以下三个条件：(i) 对某个希尔伯特空间 $\mathrm{K}_{B'}$，有 $\mathrm{H}_A=\mathrm{K}_A$ 且 $\mathrm{H}_B=\mathrm{K}_B\otimes\mathrm{K}_{B'}$。(ii) S 中作用于 H_A 的测量均包含在 D 中。(iii) S 中的共享态 $|\phi\rangle$ 可以分解为$|\phi\rangle=|\psi\rangle\otimes|\phi'\rangle$，其中 $|\psi\rangle$ 是 D 中的状态，而 $|\phi'\rangle$ 是某个辅助态，位于希尔伯特空间 $\mathrm{K}_{B'}$ 上。

注意，如果量子策略 $\mathcal{S}$ 可以通过验证设备 D实现，那么整个系统可分解为 $\mathcal{H}_A\otimes\mathcal{H}_B=\mathcal{K}_A\otimes\mathcal{K}_B\otimes\mathcal{K}_{B'}$。直观而言，我们将这一分解视为由一个设备与单个证明者共享的纠缠态 $|\psi\rangle$ 以及一个仅供证明者访问的辅助态 $|\phi'\rangle$ 组成。

给定一组验证设备 $\{D_n\}_{n\in\mathbb{N}}$，其中每个 D_n 由一个状态 $|\psi_n\rangle$和一系列 POVM 组成，若$\{D_n\}_{n\in\mathbb{N}}$ 是一个高效的现成设备族，则称其满足以下条件：存在一个多项式时间一致的量子电路族$\{Q_n\}_{n\in\mathbb{N}}$，使得 Q_n从全零态生成状态 $|\psi_n\rangle$，并且在输入 i 时，使用 D_n中的第 i个 POVM 测量 $|\psi_n\rangle$。

定义 7.1。一门承诺语言 $L=(L_{yes},\ L_{no})$ 具有一个现成设备（*OTS*）证明系统，当且仅当存在一个现成设备的高效族 $\{D_n\}_{n\in\mathbb{N}}$，以及一个可在多项式时间内计算的函数，该函数将实例 x 映射为非局域博弈 G_x 的描述，并满足以下条件：

1. 使用现成设备的完备性。对于任意具有 $|x|\le n$的 $x\in L_{yes}$，存在一个量子策略 S_x，该策略可以使用 D_n实现，从而获得 $\omega(G_x,\ S_x)\ge c$。

2. 可靠性。 对于任意 $x \in L_{no}$，我们有 $\omega^*(G_x) < s$。

我们使用 OTS 来表示所有语言 L 的类别，这些语言具有一个完备性与可靠性之间存在常数差距的 *OTS* 证明系统。

任何 OTS 证明系统都可描述为一种特殊的双玩家、单轮MIP* 证明系统，并对完备性条件施加了额外约束；如果某个 OTS 证明系统作为MIP* 证明系统具有统计零知识性质，我们就称它为统计零知识（详见定义 2.7）。

7.2 零知识与委托计算的应用

本节将证明，QMA 中的任意语言都存在一个统计零知识 OTS 证明系统。我们还将探讨如何缩减 OTS 模型，以提供用于可验证委托量子计算的协议。

定理 7.2。 对于 QMA 中的每个语言 L，都存在一个针对 L 的统计零知识 *OTS* 证明系统，且具有常数完备性和可靠性差距。

证明。 我们将使用该证明系统，它将实例 x 发送到博弈 $\mathcal{G}_x$，如图 5所示。利用第 3 节和第 4节中的刚性结果，我们已经证明了各个博弈G$_x$ 在第 5节中的完备性和可靠性。该博弈的零知识性质也已在第 6节得到证明。剩下的就是证明，该协议还满足定义 7.1中概述的、使用现成设备实现完备性的额外限制。也就是说，我们需要证明存在一个高效的现成设备族$\{D_n\}$，能够为所有是实例$\mathcal{S}_x$ 实现诚实策略 x。

对于每个 $L \in$ QMA，都存在一个多项式 f，使得对于所有大小为 $|x| = n$ 的 $x \in L$，相应的哈密顿量 H_x 至多作用于 $f(n)$ 个量子比特。接下来假设 $x \in L_{yes}$，且$|x| \leq n$。在博弈 G$_x$的诚实策略中，Alice 和 Bob 至多共享 $f(n)$ 对 EPR 对；此外，Bob 私下持有 H_x的基态 ρ。Alice 所需的测量始终对应于在共享 EPR 对的至多 6 个量子比特上进行的 σ_X或 σ_Z，或是在两个量子比特上进行的 $\sigma_X\sigma_Z \otimes \sigma_Z\sigma_X$。在 m 重并行重复锚定博弈 G$_x$的诚实策略 S$_x$ 中，玩家共享 $mf(n)$ 对 EPR 对；Alice 在至多 $6m$ 个量子比特上进行 σ_X 或 σ_Z 测量，或在 $2m$个量子比特上进行带有 $\sigma_X\sigma_Z \otimes \sigma_Z\sigma_X$的测量。由于 $m = poly(n)$，我们通过指定一个现成设备的高效族 $\{D_n\}$，从而满足所需的完备性条件；对于每个 n，验证设备 D_n 包含 $mf(n)$ 对 EPR 对，以及上述所有作用于至多 $6m$ 个量子比特的泡利测量。 □

在我们面向委托量子计算的应用中，我们考虑一种新颖的交互式协议，其中除了交换经典消息之外，服务器还可以向客户端发送如第 7.1 节中定义的不受信任的验证设备（见第 1 节）。在图 6 中，我们考虑这样一种情况：在第一个 “ 消息 ” 中，即设置阶段，证明者发送一个不受信任的验证设备，随后进行经典通信。

将这些观察与定理7.2结合起来，我们得到关于委托量子计算的以下结果。

定理 7.3。 对于每个语言 L 属于 有界错误量子多项式时间，都存在一个如图 *6* 所示的 L 统计零知识委托协议，具有常数完备性和可靠性差距。

定理7.3 成立在很大程度上是因为，它可以被视为定理 7.2在一个 BQP-完全问题中的特定应用。唯一额外的技术要求是

1. **设置阶段：** 客户端向服务器发送设置参数 $k \in \mathbb{N}$，服务器从现成设备的高效族$\{D_n\}_n$中提供一个验证设备 D_k。2. **计算选项：** 客户端向服务器发送电路 Q的经典描述，该电路满足$|Q| \leq k$。 ̂3. **可验证委托：** 客户端与服务器和设备 D_k 作为参与者进行一轮博弈$\mathcal{G}_Q$。当且仅当博弈获胜时，客户端才接受。

图 6：多项式时间经典客户端与多项式时间量子服务器之间的委托协议；服务器在设置阶段提供一个不受信任的验证设备。

这发生在步骤 3 中，在该步骤里，诚实的多项式时间量子证明者必须能够达到相应博弈的最优获胜概率。下面给出一个概要。

证明。（概要）我们可以将定义 2.2 中的 BQP 完全问题视为 QMA 中的一种语言。由此，我们可以应用图 5 中概述的高效映射，得到相应的博弈 ̂$\mathcal{G}_Q$。在这种情况下，底层哈密顿量的基态可以由多项式时间量子证明者制备。因此，如定理 7.2 的证明所示，我们可以定义所需的多项式时间一致族现成设备$\{D_n\}_{n\in\mathbb{N}}$，令 D_n 包含数量足够的 EPR 对，以及所需的泡利测量。此外，由于多项式时间量子证明者始终能够制备所需的基态，诚实服务器可以通过生成该状态，并在需要时将其隐形传态至验证设备，从而在步骤 3 中实现所需的完备性。我们还可以根据定理 7.2 的结果，得出上述委托协议继承了零知识性质。

□

References

[ABEM17] D. Aharonov、M. Ben-Or、E. Eban 和 U. Mahadev。量子计算的交互式证明。2017 年。arXiv:1704.04487 [quant-ph][ACGK19] S. Aaronson、A. Cojocaru、A. Gheorghiu 和 E. Kashefi。盲量子委托计算的复杂性理论限制。载于第 *46* 届自动机、语言与编程国际研讨会（*ICALP 2019*），第 6 号文章，2019 年。doi:10.4230/LIPIcs.ICALP.2019.6[BG22] A. Broadbent 和 A. B. Grilo。局部密度矩阵一致性的 QMA 困难性及其在量子零知识中的应用。*SIAM* 计算杂志，51(4):1400–1450，2022 年。doi:10.1137/21M140729X[BGKW88] M. Ben-Or、S. Goldwasser、J. Kilian 和 A. Widgerson。多证明者交互式证明：如何消除难解性假设。载于*STOC '88*：第二十届 *ACM* 计算理论研讨会论文集，第 113–131 页，1988 年。doi:10.1145/62212.62223

[BGS13] A. Broadbent、G.Gutoski 和 D. Stebila。量子一次性程序。载于《密码学进展——CRYPTO2013》，第2 卷，第344–360 页，2013年。doi:10.1007/978-3-642-40084-1_20[BJSW16] A. Broadbent、Z. Ji、F.Song 和 J.Watrous。QMA 的零知识证明系统。载于《2016 年第 57 届IEEE计算机科学基础年会》（FOCS2016），第31–40 页，2016年。doi:10.1109/FOCS.2016.13[BJSW20] A. Broadbent、Z. Ji、F. Song和 J. Watrous。QMA 的零知识证明系统。《SIAM 计算杂志》，49(2)：245–283，2020 年。doi:10.1137/18M1193530[BOGG+88] M.Ben-Or 等。一切可证明的命题都可以在零知识中得到证明。载于《密码学进展——CRYPTO'88》，第 37–56 页，1988 年。doi:10.1007/0-387-34799-2_4[Bro18] A. Broadbent。如何验证量子计算。《计算理论》，14(1)：1–37，2018年。doi:10.4086/toc.2018.v014a011[CFGS18] A. Chiesa、M.Forbes、T. Gur 和N.Spooner。即使在量子世界中，空间隔离也意味着零知识。载于《2018 年第 59 届 IEEE 计算机科学基础年会》（FOCS2018），第755–765 页，2018 年。doi:10.1109/FOCS.2018.00077[CGJV19] A. Coladangelo、A.B. Grilo、S. Jeffery和 T. Vidick。受控验证者：采用准线性资源的可验证委托量子计算新方案。载于《密码学进展——EUROCRYPT2019》，第 3 卷，第247–277 页，2019 年。doi:10.1007/978-3-030-17659-4_9[CHSH69] J. F. Clauser、M. A.Horne、A. Shimony 和R. A.Holt。检验局域隐变量理论的实验设想。《物理评论快报》，23(15)：880–884，1969年。doi:10.1103/PhysRevLett.23.880[CHTW04] R. Cleve、P. Høyer、B.Toner 和 J. Watrous。非局域策略的后果与局限。载于《第19届计算复杂性年会》（CCC2004），第 236–249 页，2004 年。doi:10.1109/CCC.2004.1313847[CL17] A. Chailloux和A.Leverrier。针对量子对手安全的 NP 相对论（或双证明者单轮）零知识协议。载于《密码学进展——EUROCRYPT2017》，第 3卷，第369–396 页，2017 年。doi:10.1007/978-3-319-56617-7_13[CMMN20] D. Cui、A. Mehta、H. Mousavi和 S. S. Nezhadi。CHSH 的推广与最优策略的代数结构。《Quantum》，4：346，2020 年。doi:10.22331/q-2020-10-21-346[Col17] A.Coladangelo。通过倾斜CHSH 和魔方游戏的副本对（倾斜）EPR 对进行并行自检。《量子信息与计算》，17(9&10)：831–865，2017 年。doi:10.26421/QIC17.9-10-6

[CRSV18] R. Chao、B. W. Reichardt、C. Sutherland 和 T. Vidick。使用少量测量检验大量纠缠。Quantum，2:92，2018。doi:10.22331/q-2018-09-03-92[CS23] C. Cr´epeau 和 J. Stuart。使用同态承诺方案的零知识多方交互证明。2023。arXiv:2304.09784 [quant-ph][CVZ19] A. Coladangelo、T. Vidick 和 T. Zhang。带预处理的 QMA 非交互式零知识论证。2019。arXiv:1911.07546 [quant-ph][FK17] J. F. Fitzsimons 和 E. Kashefi。无条件可验证的盲量子计算。Physical Review A，96(1):012303，2017。doi:10.1103/PhysRevA.96.012303[GH17] W. T. Gowers 和 O. Hatami。有限群近似表示的逆定理与稳定性定理。Sbornik: Mathematics，208(12):1784–1817，2017。doi:10.1070/sm8872[GMR89] S. Goldwasser、S. Micali 和 C. Rackoff。交互式证明系统的知识复杂性。SIAM Journal on Computing，18(1):186–208，1989。doi:10.1137/0218012[GMW91] O. Goldreich、S. Micali 和 A. Wigderson。除证明自身有效性外不泄露任何信息的证明，或 NP 中所有语言均有零知识证明系统。Journal of the ACM，38(3):690–728，1991。doi:10.1145/116825.116852[Gri19] A. B. Grilo。一个单轮量子计算可验证委托的简单协议。载于第 46 届国际自动机、语言与编程研讨会（ICALP 2019），文章编号 28，2019。doi:10.4230/LIPIcs.ICALP.2019.28[GSY19] A. B. Grilo、W. Slofstra 和 H. Yuen。量子多证明者交互式证明的完美零知识。载于 2019 年第 60 届 IEEE 计算机科学基础年会（FOCS 2019），第 611–635 页，2019。doi:10.1109/FOCS.2019.00044[Ji16] Z. Ji。量子证明的经典验证。载于 STOC 2016：第 48 届 ACM SIGACT 计算理论研讨会论文集，第 885–898 页，2016。doi:10.1145/2897518.2897634[Ji17] Z. Ji。量子多证明者交互式证明的压缩。载于 STOC 2017：第 49 届 ACM SIGACT 计算理论研讨会论文集，第 289–302 页，2017。doi:10.1145/3055399.3055441[JJUW11] R. Jain、Z. Ji、S. Upadhyay 和 J. Watrous。QIP = PSPACE。Journal of the ACM，58(6):30，2011。doi:10.1145/2049697.2049704

[JNV+20] Z. Ji、A. Natarajan、T. Vidick、J. Wright 和 H. Yuen。多方交互证明（纠缠）=RE。2020。arXiv:2001.04383 [quant-ph][Kil88] J. Kilian。以不经意传输为基础构建密码学。载于 STOC '88：第 20 届 ACM 计算理论研讨会论文集，第 20–31 页，1988。doi:10.1145/62212.62215[KM03] H. Kobayashi 和 K. Matsumoto。先验纠缠受限的量子多证明者交互式证明系统。Journal of Computer and System Sciences，66(3):429–450，2003。doi:10.1016/S0022-0000(03)00035-7[KSV02] A. Y. Kitaev、A. Shen 和 M. N. Vyalyi。经典与量子计算。American Mathematical Society，2002。doi:10.1090/gsm/047[Mah18] U. Mahadev。量子计算的经典验证。载于 2018 年第 59 届 IEEE 计算机科学基础年会（FOCS 2018），第 259–267 页，2018。doi:10.1109/FOCS.2018.00033[McK17] M. McKague。并行 CHSH 自测试。Quantum，1:1，2017。doi:10.22331/q-2017-04-25-1[Mer90] N. D. Mermin。主要无隐变量定理的简单统一形式。Physical Review Letters，65(27):3373–3376，1990。doi:10.1103/PhysRevLett.65.3373[MNP21] L. Manˇcinska、T. G. Nielsen 和 J. Prakash。拼接魔术博弈自检最大纠缠态。2021。arXiv:2105.10658 [quant-ph][MNY22] H. Mousavi、S. S. Nezhadi 和 H. Yuen。非局域博弈、压缩定理与算术层级。载于 STOC 2022：第 54 届 ACM SIGACT 计算理论研讨会论文集，第 1–11 页，2022。doi:10.1145/3519935.3519949[MPS21] L. Manˇcinska、J. Prakash 和 C. Schafhauser。针对无界维度状态与测量的常数规模鲁棒自测试。2021。arXiv:2103.01729 [quant-ph][MS23] L. Manˇcinska 和 S. Schmidt。自测试中的反例。Quantum，7:1051，2023。doi:10.22331/q-2023-07-11-1051[MY04] D. Mayers 和 A. Yao。量子设备自测试。Quantum Information & Computation，4(4):273–286，2004。doi:10.26421/QIC4.4-4[MYS12] M. McKague、T. H. Yang 和 V. Scarani。单态的鲁棒自测试。Journal of Physics A，45(45):455304，2012。doi:10.1088/1751-8113/45/45/455304

[NC00] M. A. Nielsen 和 I. L. Chuang。《量子计算与量子信息》。剑桥大学出版社，2000 年。[NV17] A. Natarajan 和 T. Vidick。用于稳健验证纠缠的量子线性测试。载于 STOC 2017：第 49 届 ACM SIGACT 计算理论研讨会论文集，第 1003–1015 页，2017 年。doi:10.1145/3055399.3055468[NV18] A. Natarajan 和 T. Vidick。量子态的低次测试，以及用于 QMA 的量子纠缠博弈 PCP。载于 2018 年第 59 届 IEEE 计算机科学基础年度研讨会（FOCS 2018），第 731–742 页，2018 年。doi:10.1109/FOCS.2018.00075[Per90] A. Peres。量子测量的不相容结果。《Physics Letters A》，151(3):107–108，1990 年。doi:10.1016/0375-9601(90)90172-K[RUV13] B. W. Reichardt、F. Unger 和 U. Vazirani。对量子系统的经典控制。《Nature》，496:456–460，2013 年。doi:10.1038/nature12035[RY22] G. Rosenthal 和 H. Yuen。用于合成量子态和酉算子的交互式证明。载于第 13 届理论计算机科学创新会议——ITCS 2022，文章编号 112，2022 年。doi:10.4230/LIPIcs.ITCS.2022.112[Slo16] W. Slofstra。Tsirelson 问题及一个关于源自非局域博弈的群的嵌入定理。2016 年。arXiv:1606.03140 [quant-ph][Slo19] W. Slofstra。量子关联集合并非闭集。《Forum of Mathematics, Pi》，7:e1:1–e1:41，2019 年。doi:10.1017/fmp.2018.3[Tsi93] B. S. Tsirelson。关于量子贝尔型不等式的一些结果与问题。《Hadronic Journal Supplement》，8:329–345，1993 年。[Vid18] T. Vidick。关于“用于稳健验证纠缠的量子线性测试”的阐述性笔记，2018 年。http://users.cms.caltech.edu/~vidick/notes/pauli_braiding_1.pdf[VZ20] T. Vidick 和 T. Zhang。量子计算的经典零知识论证。《Quantum》，4:266，2020 年。doi:10.22331/q-2020-05-14-266[Wat00] J. Watrous。有限群性质的简洁量子证明。载于第 41 届计算机科学基础年度研讨会（FOCS 2000），第 537–546 页，2000 年。doi:10.1109/SFCS.2000.892141[Wat03] J. Watrous。PSPACE 具有常数轮量子交互式证明系统。《Theoretical Computer Science》，292(3):575–588，2003 年。doi:10.1016/S0304-3975(01)00375-9

[Wat09] J. Watrous. 量子计算复杂性。载于复杂性与系统科学百科全书，第 7174–7201 页。Springer，2009 年。doi:10.1007/978-3-642-27737-5_428-3[WBMS16] X. Wu、J.-D. Bancal、M. McKague 和 V. Scarani。设备无关的两个单态并行自测试。《物理评论*A*》，93:062121，2016 年。doi:10.1103/PhysRevA.93.062121[Yue16] H. Yuen。博弈、协议与量子纠缠。博士论文，麻省理工学院，2016 年。https://dspace.mit.edu/handle/1721.1/107364