arXiv:2601.12874v1 [cs.CC] 19 Jan 2026

量子交互式预言机证明

Baocheng Sun* Thomas Vidick†

摘要

我们开始研究量子交互式预言机证明（qIOP）。这是一种量子概率可检验证明和量子交互式证明的推广，也是经典交互式预言机证明的量子类比。

在量子交互式预言机证明模型中，我们允许量子证明者与量子验证者之间进行多轮量子交互，但验证者对量子资源的访问受到限制。这包括对证明者消息的查询，以及验证者所应用的量子电路的复杂度。QMA 是否具有量子交互式预言机证明系统这一问题，是对量子 PCP 猜想的一种放宽。

W我们展示了以下两种 qIOP 的主要构造，二者均为无条件的 l:

- 我们构造了一个针对 QMA 的 qIOP，在该协议开始时，验证者与证明者共享多项式数量的 EPR 对，且验证者从证明者消息中只读取常数个量子比特。

- 我们为 QMA 提供了一种更强的 qIOP 构造，其中验证者不仅只读取常数个量子比特，而且总共只操作常数个量子比特，包括其私有寄存器中的量子比特。然而，在这种更强的设定下，通信复杂度会变为指数级。这留下了一个开放问题：是否存在具有多项式通信复杂度的 QMA 强 qIOP。

作为我们构造的关键组成部分，我们提出了一种新颖的单证明者多量子比特测试，它本身也可能具有独立的研究价值。

*baocheng.sun@weizmann.ac.il。魏茨曼科学研究所。

†thomas.vidick@epfl.ch。计算机与通信科学学院及量子科学与工程中心，洛桑联邦理工学院，以及魏茨曼科学研究所数学与计算机科学学院。

目录

1 引言 **1**

1.1 我们的表述.1 1.2 主要结果.2 1.3 开放问题.3 1.4 相关工作.4

2 技术概述 **5**

2.1 Clifford-哈密顿量问题.5 2.2 一般量子交互式预言机证明.6 2.3 强量子交互式预言机证明.7

3 组织结构 **12**

4 预备知识 **13**

4.1 Clifford-哈密顿量问题的间隙放大.14 4.2 可概率检验的邻近性证明.16 4.3 群稳定性.17

5 量子交互式预言机证明的表述 20

5.1 符号说明.20 5.2 带查询的量子信道.21 5.3 量子交互式预言机证明系统.22

6 Qu共享 EPR 对与经典通信的量子交互式预言机证明 **25**

6.1 交互式预言机证明模型中的承诺.25 6.2 共享 EPR 对的量子交互式预言机证明.27 6.3 技术性论断.31

7 多量子比特 测试 34

7.1 纠错码.34 7.2 诚实证明者策略.36 7.3 验证者策略.37 7.4 一般证明者操作.41 7.5 主定理.42

8 对诚实证明者具有对数深度的强量子交互式预言机证明 52

8.1 泡利基测量.54 8.2 能量测试和能量一致性测试.54 8.3 一般证明者操作.56 8.4 主定理.57

单量子比特测试 试 65

A.1 诚实证明者策略.65 A.2 验证者策略.66 A.3 主定理.67

1 引言

经典PCP定理 [ALM+98，AS98，Din06]是 20 世纪 90 年代初计算复杂性理论中最重要的突破之一。它的影响不仅体现在简洁密码学论证等实际应用上，也延伸至近似问题的困难性等基础领域 [FGL+91]，并深刻影响了编码理论的发展。

量子 PCP 定理的对应版本，即量子 PCP 猜想（qPCP）[AN02、AALV09], 数十年来一直是研究的主题。qPCP猜想对量子力学的基础具有重要影响 [AAV13], ，其与 NLTS（无低能平凡态）定理的关系 [FH14]便是一个例证。围绕 qPCP 猜想的研究既取得了令人鼓舞的成果 [ABN23] ，也得出了否定性结果 [BH13、NN24]。近期的一项突破 [ABN23] 证明了 NLTS 定理，增强了人们对 qPCP 猜想可行性的信心。然而，qPCP 猜想仍鲜有研究 [AAV13], 这促使人们开始关注由 qPCP 猜想引出的自然且限制较少的问题。

我们提出了 qPCP 猜想的一种放宽形式，类似于经典 PCP 推广为交互式预言机证明（IOP）的过程 [BCS16、RRR16]。具体而言，我们提出了量子交互式预言机证明（qIOP），并给出两种互不包含、各自采用不同技术方法的构造。我们对 qIOP 的表述建立在量子 PCP 猜想之上；该猜想以高效证明验证来定义 [AAV13]：对于 QMA 语言的任意实例，都存在一个多项式长度的量子证明，只需测量常数个量子比特即可验证。我们的方法扩展了证明系统框架，允许进行多轮交互，同时确保验证者总共只读取常数个量子比特。因此，qPCP 是量子交互式预言机证明的一种特例；将交互限制为单轮，就得到 qPCP。

作为 qPCP 的一种推广，qIOP 的存在为 qPCP 猜想的有效性提供了支持性证据。此外，qIOP 有望用于为 QMA语言开发量子简洁论证 [BCS16，KLVY23，BKL+22，GJMZ23，MNZ24]。

1.1 我们的表述

我们提出量子交互式预言机证明的若干变体。每种表述都满足：当所有计算和通信都限制为经典形式时，该模型便退化为标准的经典交互式预言机证明。具体而言，我们如下定义量子IOP系统和强量子IOP系统。

定义 1.1 (量子 IOP 系统；定义5.10的非正式版本)。 一个量子交互式预言机证明*(量子 IOP)* 系统，以函数 $q(n)$ 和 $l(n)$ 为参数： $\mathbb{Z}_+ \to \mathbb{Z}_+$由一个量子验证者 V 构成，并且对于任何大小为 n的输入，满足以下条件：

- 验证者与证明者交互的轮数至多为$\mathrm{poly}(n)$。
- 在每一轮中，证明者都会向验证者发送一条量子消息。消息长度可能因轮次而异。
- 在每一轮中，验证者：
  - 对其私有量子比特以及证明者消息的部分内容应用量子电路，其中包括当前轮次收到的量子比特以及从前一轮保留的量子比特，– 存储证明者消息寄存器的一部分，以供后续轮次使用。

- 每次交互后，验证者都会返还证明者量子消息的剩余部分（即未存储的部分），并可选择返还其自身私有量子寄存器的一部分。

- 协议结束时，验证者输出一个判定比特。

主要的复杂度参数包括：

- 查询复杂度 $q(n)$：验证者在所有轮次中访问的证明者消息中的量子比特总数。

- 通信复杂度 $l(n)$：所有轮次中证明者消息里的量子比特总数。

我们将这样的系统称为量子交互式预言机证明，条件是 $q(n)$ 有常数上界。[1]我们定义量子交互式预言机证明的以下变体量子交互式预言机证明：

- 如果验证者发回的私有寄存器必须是受限量子交互式预言机证明 经典的，则称该系统为受限量子交互式预言机证明。

- 如果验证者在每一轮都必须返回证明者的整个量子交互式预言机证明消息寄存器（即不存储消息的任何部分），则称其为强量子交互式预言机证明。

定义 1.2（承诺问题的量子交互式预言机证明系统，定义 5.14的非正式版本）。针对语言 $\mathcal{L}$，完备性为c：$\mathbb{Z}_+ \to [0,1]$ 且可靠性为 s： $\mathbb{Z}_+ \to [0,1]$ 的量子交互式预言机证明（量子 *IOP*）系统满足以下条件：

- 对于任意大小为 n 的是实例，都存在一个多项式时间证明者，使验证者以至少 $c(n)$ 的概率接受。

- 对于任意大小为 n 的否实例，对于所有证明者，验证者接受的概率至多为$s(n)$。

系统的完备性-可靠性间隙定义为 $c(n) - s(n)$。

注 1.3。 在正式定义中，我们采用定义 *5.1*中给出的查询概念，以精确量化查询复杂度和证明长度。此处的查询概念源自量子查询复杂度相关文献中使用的预言机模型。

注 1.4. 在经典情形下，每轮都读取证明者消息的常数轮 *IOP*，与仅在最后读取整个交互过程的 *IOP* 等价。此外，自适应交互式预言机证明与非自适应交互式预言机证明等价。然而，这些等价关系在量子情形下未必成立。

1.2 主要结果

下面给出我们两个主要结果的非正式表述。

定理1.5 (定理6.1的**非正式版本。**存在一个用于 QMA 的量子交互式预言机证明系统，其参数如下：查询复杂度为 $q(n) = O(1)$，通信复杂度为 $l(n) = \mathrm{poly}(n)$，且完备性-可靠性间隙为常数。

[1]在正式定义5.10中，我们将其称为 *general* 量子交互式预言机证明，以区别于受限变体和强变体。

注 1.6。在我们的构造中，唯一的量子通信发生在第一轮，此时验证者向证明者发送$\mathrm{poly}(n)$ *EPR* 对。证明者与验证者此后交换的所有消息都是经典的。

定理1.7 （定理 8.17 的非正式表述）。 存在一个用于 QMA 的强量子交互式预言机证明系统，其查询复杂度为 $q(n) = O(1)$，通信复杂度为 $l(n) = \exp(\mathrm{poly}(n))$，且完备性与可靠性之间的差距为常数。

对于这两个结果，交互轮数均为常数。我们在第 2 节进一步介绍每个结果所用的证明技术。简单来说，第一个协议基于对见证进行量子隐形传态，并恰当地使用邻近性概率可检验证明（PCPP），使验证者能够校正隐形传态掩码，同时只需向证明者查询常数个比特。（不过，验证者确实会在自己的私有空间中执行多项式规模的量子计算，该空间包含验证者持有的一半 EPR 对。）第二个协议基于多量子比特测试，将测量委托给证明者，并运用经典 PCP 技术，使验证者能够恢复能量测量结果。尽管验证者总共只操作常数个量子比特，多量子比特测试仍要求证明者向验证者发送指数规模的量子通信。然而，我们认为该测试本身也值得关注，或可成为后续改进的目标。

1.3 开放问题

在经典情形下，若公币交互式预言机证明的验证者消息长度为 $O(\log n)$-比特，则可以将其编译为 PCP。已知，若公币交互式预言机证明具有 polylog(n) 轮次、$O(1)$ 查询复杂度、完美完备性以及 $O(1/\mathrm{poly}(n))$ 可靠性，则意味着存在一个多项式长度 PCP [ABCY22]。量子 IOP（qIOP）与量子 PCP （ qPCP ）的联系，尚不如经典情形下那样清楚。事实上，我们甚至不知道强 qIOP 是否意味着存在指数规模的量子 PCP。因此，我们的 qIOP 构造并未让我们对量子 PCP 归约可能产生何种形式的局部哈密顿量，或这些归约本身，获得新的认识。这引出了关于这两个框架之间联系的以下问题：

问题 1。 **8.** 是否存在一种从量子 *IOP* 到量子 *PCP* 的黑盒变换 *?*

由于我们目前构造的强量子交互式预言机证明具有指数级通信复杂度，因此自然会提出以下问题：

问题 1。 **9.** 是否存在具有多项式通信复杂度的强量子交互式预言机证明？

此外，我们也很关注 qIOP 模型在密码学中的应用。在[GJMZ23], 中，作者在假设量子 PCP 存在的前提下，构造了一个针对 QMA 的量子通信简洁论证，其所需假设弱于单向函数（OWF）。这引出了以下问题：

问题 1.10。 是否存在基于弱于单向函数（*OWF*）的假设、且不依赖于量子 *PCP* 猜想得到肯定解答的委托量子计算协议？

另一种潜在的密码学应用如下：

问题 1.11. 我们能否对 *qIOP* 协议应用 *Fiat–Shamir* 变换，从而得到针对 *QMA* 的非交互简洁量子论证，或者得到查询复杂度为常数的针对 *QMA* 的非交互量子论证？

在构造强量子交互式预言机证明时，我们注意到验证者操作带有经典色彩。具体而言，在该协议中，验证者要么施加一个 Z 门，要么在 Z基下进行测量。这自然引出了一个问题：在仍允许高效的量子证明者说服量子验证者某个 QMA语言成立的同时，此类证明系统中的通信在多大程度上可以是经典的？这引出了以下问题：

问题1.12。 是否存在一种针对*QMA*语言的证明系统，其中通信完全是经典的，但证明者和验证者都是量子的？

1.4 相关工作

交互式预言机证明。 在经典领域，IOP在PCP定理得到证明后[BCS16、RRR16]之后出现。交互有助于缩短证明长度，主要借助一种称为交互式组合的工具。然而，我们的目标不是简化，而是创造尚不存在的东西。因此，经典IOP方面的经验只能提供有限的启示。尽管如此，我们的主要动机是勾勒出一条证明量子 PCP 猜想的可能路径：首先利用经典交互式预言机证明以及非局域博弈（见下文）研究中的见解，至少在初期避开传统qPCP研究中遇到的一些主要困难（例如不可克隆定理）。

有限量子能力验证者的QMA验证协议。 目前已有多种交互协议，可对QMA进行信息论安全验证，其中验证者的量子能力有限。这包括 [FK17、ABOEM17、FHM18], 参见 [GKK19] 中的综述。尽管这些协议基于这样一种验证者：其每轮执行的量子操作规模为常数（或对数），但所有协议都包含多项式数量的交互轮次。因此，验证者的总工作量，以及从证明者处接收并读取的量子通信总量，始终是多项式的。我们关注的是验证者的总常数级 工作量；但我们不限制验证者的量子存储器。因此，这些模型互不包含。我们没有借鉴这方面文献中的技术（除了将QMA语言归约到局域哈密顿量问题这一思路；该思路见于 [FHM18] ，如今已是相当经典的做法）。

QMA的指数长度经典PCP。尽管通过量子化经典PCP变换来推导 qPCP 是很自然的做法， [AAV13]却在一定程度上背离了这一思路，部分原因是 [BH13] 指出，“最‘自然’的变换在量子情形下可能会失效” [AAV13]。更具体地说，他们通过以下步骤证明了 QMA 存在指数长度经典PCP：$\mathsf{QMA} \subseteq \mathsf{PSPACE} = \mathsf{IP}$，以及从 IP 到指数长度经典PCP的自然变换。然而，由此得到的证明系统直接处理局部哈密顿量，而不是显式编码量子见证。因此，即使证明者拥有该见证，也无法利用它来提高效率。相比之下，对于我们的两种构造，诚实证明者策略都基于一种自然算法。对于定理 1.5 ，该算法是高效的（前提是有足够多份量子见证副本）。对于定理 1.7 ，该算法也是高效的，但需要以非常系统化的方式对指数多个泡利可观测量进行相干求值，而这种方式很容易并行化。

量子 PCP 的博弈版本。[NV16] 针对 XZ-哈密顿量问题提出了 qPCP 的“博弈版本”：多个证明者共享纠缠，并通过经典方式与验证者通信，在一个单轮协议中发送长度为常数的证明者消息。很自然地，人们会

以此类方法为出发点，但要将多证明者设置与单证明者设置联系起来，仍然面临挑战。

据我们所知，唯一一项建立此类联系的先前工作是 [Weh06], ，其证明了包含关系 $\oplus$MIP*[2] $\subseteq$QIP（2），从而无条件地将两名量子证明者“编译”为一名证明者。然而，他们的方法似乎仅限于测试 XOR 型关系，以及涉及恰好两条消息交换的协议。我们没有发现如何将其扩展到更复杂的双证明者协议。

较新的方法 [NZ23、MNZ24] 利用密码学技术压缩证明者，但这些方法依赖于计算假设，并对证明者的计算能力施加了并非证明系统固有的限制。更为关键的是， [NN24]指出 [NV16] 仅适用于 XZ-哈密顿量问题，而我们的目标是处理 QMA。迄今为止，尚无已知的适用于 QMA 的博弈版本 qPCP 构造 [NN24]。

尽管如此，我们对强量子交互式预言机证明的构造受到了 [NV16]中所发展的技术的启发。我们并非先为 QMA 构造博弈版本的 qPCP，再将其编译为 qPCP，而是改造了 [NV16] 中用于验证 XZ哈密顿量证明的量子比特测试技术，并将其扩展为单证明者协议，将其应用于 QMA 语言。

我们基于量子隐形传态构造了一个共享 EPR 对的量子交互式预言机证明。我们注意到， [Gri19] 中的协议同样基于量子隐形传态。事实上，我们的共享 EPR 对量子交互式预言机证明协议可以视为 [Gri19]中多证明者协议的单证明者对应版本。不过，在他们的设置中，两个证明者都不可信，验证者无法控制证明者执行的操作，因此需要额外的自测试。在我们的设置中，验证者实际上扮演了 [Gri19], 中一名证明者的角色；但由于验证者是诚实的量子验证者，无需证明这些量子比特。此外，由于验证者是诚实的，并且也充当测量量子比特的证明者，我们无需隐藏正在测量的是哪个哈密顿量项。

对易性测试。 在双证明者设置中，测试反对易关系需要复杂的构造，而测试对易性则是一种更基础且成熟的技术 [CGJV19]。归根结底，我们的单量子比特测试协议与 [CRSV17]中用于测试态依赖对易性的协议很接近。不过，在他们的设置中，已知每个量子比特本身都具有反对易性，主要问题在于不同量子比特是否彼此对易。

2 技术概述

在本文中，除非另有说明，我们使用可观测量 一词来指同时为厄米算子且平方等于恒等算符的算子。偶尔，我们也用可观测量 来指形式为 $O = \sum_i a_i P_i$ 的算子，其中 $a_i \in \mathbb{R}$，每个 P_i 都是一个正交投影，且 $\sum_i P_i = I$。符号 $O(a)$ 表示作用于所选量子比特上的泡利 $O \in \{X, Y, Z\}$ 算子的张量积，所选量子比特由比特串 a 指定：

$$O(a) = O^{a_1} \otimes O^{a_2} \otimes \cdots \otimes O^{a_n},$$

其中 $O^0 = I$ 是恒等算符， $O^1 = O$ 是泡利-O 矩阵。

2.1 克利福德哈密顿量问题

Clifford-哈密顿量问题由 [BJSW16]提出。这是局域哈密顿量问题的一个特例，其中每个局部项都具有以下形式 $C^\dagger(|0\rangle\langle 0|)^{\otimes 5}C$，其中 C 是一个元素

属于作用于 5个量子比特上的克利福德群。Clifford-哈密顿量问题旨在确定作为输入给出的克利福德哈密顿量的最低能量（即最小特征值），误差不超过与量子比特数量成反比的多项式量级。 [BJSW16], 通过改造标准的 Kitaev归约，证明了该问题是 QMA-完备的。由于我们所有的量子交互式预言机证明协议都旨在使完备性与可靠性之间达到常数间隙，我们首先展示如何放大 Clifford-哈密顿量问题，以局域性换取更大的间隙。

设 $H = \mathbb{E}[H_i]$ 是一个 Clifford 哈密顿量。这里，每个 H_i 都是一个 5-局域Clifford投影。放大后，哈密顿量变为

$$(1-2H)^{\otimes N} = \big(\mathbb{E}_i[1-2H_i]\big)^{\otimes N} = \mathbb{E}_{s_1,\ldots,s_N}\Big[\bigotimes_{j\in[N]}(1-2H_{s_j})\Big] .$$

这个放大后的哈密顿量由指数多个项组成；不过，我们可以高效地对其中一项进行采样。请注意，采样到的项不一定是局域的，而且通常不对应 Clifford 投影。

在许多情况下，验证泡利可观测量的测量结果比验证 Clifford 投影的测量结果容易得多。因此，我们希望将对 Clifford 投影的测量归约为对泡利可观测量的测量。请注意，量子态位于形式为 $C^\dagger(|0\rangle\langle 0|)^{\otimes 5}C$ 的 Clifford 投影中的含义是，应用 C后，所有 5 个量子比特都处于量子态 $|0\rangle$。我们不必一次测量所有量子比特，而可以逐个测量。此时，对原投影进行测量等价于针对每个 $j \in [5]$投影量子态，所用算符为：

$$C^\dagger\Big(I^{\otimes j-1}\otimes\frac{I+Z}{2}\otimes I^{\otimes(5-j)}\Big)C .$$

由于 Clifford门保持泡利群不变，这些项中的每一项都是投影到泡利可观测量的 $+1$特征子空间上的投影。通过使用这 5 个投影测量原始量子态，并对测量结果取逻辑与，我们就得到了一种仅使用泡利可观测量来估算放大后的克利福德哈密顿量能量的方法。

如果一个哈密顿量是*XZ*哈密顿量，即它是 XZ 项的加权和，且每一项都具有以下形式 $X(a)Z(b)$，其中 $a \wedge b = 0$，这意味着 a，$b \in \mathbb{F}_2^n$ 具有互不相交的支撑集。目前尚不清楚具有常数间隙的 XZ- 哈密顿量问题是否是 QMA 完全问题。[NN24] 提出了若干理由，说明在保持问题属于 QMA 的同时放大间隙可能具有挑战性。因此，我们主要研究克利福德哈密顿量问题。不过，有时讨论 XZ-哈密顿量实例会更方便；特别是，我们用于测量克利福德哈密顿量能量的方法，实质上会将 XZ 哈密顿量的测量作为一个子程序。

2.2 一般量子交互式预言机证明

我们的第一个构造基于量子隐形传态。请注意，我们得到的常数间隙哈密顿量问题，即放大的克利福德哈密顿量，并非局部问题。因此，证明者不能简单地将见证发送给验证者，再让验证者抽取并测量一个随机项，因为验证者的查询复杂度只有常数。回想一下，在 qIOP 的标准定义中，我们只计算验证者从证明者的消息中读取的量子比特数。如果验证者和证明者共享 EPR 对 [2]，且验证者测量自己的一半，则这次测量不计入

[2]共享 EPR 对也可以通过让验证者发送一条包含 EPR 对一半的第一条消息来建立。然而，在我们对量子交互式预言机证明所作的基于查询复杂度的定义中，验证者不允许向证明者发送长消息。验证者只接收证明者发来的消息、对其进行查询，然后再将其发回。如果验证者想向证明者传递信息，就必须借助证明者先前发送的消息，将其与自己的寄存器交换。因此，我们将协议定义为从共享 EPR 对开始。

查询复杂度。基于这一观察，我们设计了如下协议：证明者和验证者最初共享 EPR 对。随后，证明者执行量子隐形传态，并向验证者发送量子隐形传态过程中生成的经典一次性密码本的编码。由于哈密顿量中的每一项都是非局部的，验证者仍需以非局部方式读取一次性密码本，才能正确解读测量结果。幸运的是，一次性密码本是经典的，因此我们可以找到一个经典解，使证明者能够以可靠且简洁的方式，提供验证者所需的准确信息。

请注意，我们使用的一般量子交互式预言机证明的唯一特性是：由验证者的私有量子比特导出的验证者消息不要求是经典的；特别地，验证者可以发送任意量子态。相比之下，受限量子交互式预言机证明或强量子交互式预言机证明只允许经典验证者消息，但可以返回证明者的消息寄存器。在一般量子交互式预言机证明的设定中，验证者尤其可以在第一轮向证明者发送多项式数量的 EPR 对。

我们将展示如何估计非局域 XZ哈密顿量的能量；估计非局域 Clifford 哈密顿量能量的方法与此类似。对于 XZ哈密顿量，要估计该哈密顿量在给定量子态上的能量，我们可以随机抽取一个 XZ 项，并根据测量结果决定接受或拒绝。接受概率与能量成正比。由于量子隐形传态得到的量子态被一次性密码本加密，直接对其进行测量无法得到原始量子态上的正确结果。然而，在能够访问 OTP 的情况下，可以从加密态推断出对 XZ 项进行直接测量的结果：如果在加密态上测量 $X(a_i)Z(b_i)$ 得到 r，且加密掩码为 $X(p)Z(q)$，我们就知道在原始量子态上的测量将得到 $r + p \cdot b_i + q \cdot a_i$。（其中，$a_i$，$b_i$，$p$，$q$ 都是 n 位字符串，且运算均模 2 进行。）

请注意，我们需要测量的可观测量 $X(a_i)Z(b_i)$ 是非局部的。我们仍需弄清楚如何对一次性密码本（p，q）进行编码，使验证者能够计算出值 $p \cdot b_i + q \cdot a_i$。虽然哈达玛码可以实现这一点，但会导致指数长度的编码。在交互式场景中，验证者可以请求证明者的帮助，但不能直接将选定的 XZ 项（a_i，b_i）发送给证明者，因为这会让证明者有机会作弊。

其思路是让证明者先提交一次性密码本（p，q）的“承诺”，然后验证者才发送（a_i，b_i）。随后，证明者必须证明所承诺的值会产生正确的结果 $p \cdot b_i + q \cdot a_i$。为此，我们使用任意纠错码对该承诺进行编码，并通过邻近性 PCP 提供正确性证明。根据邻近性 PCP 的可靠性，如果该承诺与任何一个同某个有效（p，q）一致、且能产生所声称值的码字都相距很远，验证者将以高概率拒绝。

我们将其称为交互式预言机证明模型中的承诺。值得注意的是，密码学文献中也曾将类似技术用于其他目的 [LMS22，MNZ24]。

该协议的一个优点是通信完全是经典的。不过，由于需要预先使用 EPR 对，如何将其转化为适用于 QMA 的简洁论证仍不清楚。

2.3 强量子交互式预言机证明

总体思路。 此前许多用于验证 QMA 的协议都源自多证明者量子比特测试，我们也采用相同的方法。早期工作，例如 [NV16] 将 CHSH 和魔方博弈等单量子比特反对易博弈推广到多量子比特测试，并将这些结果应用于针对 XZ-哈密顿量问题的 qPCP 博弈版本 [NN24]。这些博弈版本涉及多个纠缠证明者与一位经典验证者交互，采用单轮协议，证明者发送的消息长度为常数。

理解 qIOP 构造的一种方式，是将其视为把多证明者多量子比特测试编译为单证明者多量子比特测试协议，随后便可用该协议估计对应于某个 QMA语言的哈密顿量的能量——这模仿了[NV16、Gri19]的技术。尽管这一目标已在计算假设下实现 [KLVY23、MNZ24],但此前从未以信息论的方式实现。

直接将非局域博弈中发给所有证明者的消息转换为 qIOP 设置中发给单个证明者的一条消息，可能会将原本发给其他证明者的查询泄露给这名单个 qIOP 证明者，从而向其明确提供问题，使其能够准确作答。经典地，对每个证明者针对每个可能问题的应答策略进行编码，可以编译一个 MIP，但消息大小会随问题规模呈指数级增长[BFL90]。然而，对于共享纠缠的量子证明者，证明者针对验证者不同问题的策略可能并不对易。因此，列举所有可能的测量结果并非易事，因为测量的执行顺序可能影响结果。

暂且搁置编译方法，为 QMA 设计 qIOP 的自然思路如下。首先，证明者向验证者发送一份量子见证的“承诺”，以防止证明者中途篡改它。随后，验证者在证明者的协助下对已承诺的量子态进行测量。在这一框架下，首要目标之一是设计这样一种承诺方案，使验证者能够以常数查询复杂度测量简单的可观测量，例如 Pauli $X(a)$ $a \in \mathbb{F}_2^n$和 $Z(b)$ $b \in \mathbb{F}_2^n$的张量积。这些算子常见于多量子比特测试中。

我们没有采用直接编译，而是从非局域博弈中汲取灵感来设计承诺过程。在我们的协议中，在第一轮，证明者将见证发送给验证者：先以纯化方式在 X 基下测量，再使用纠错码（具体而言，是哈达玛码）进行编码。在后续一轮中，见证会在 Z 基下测量，同样采用纯化方式，并以类似方式编码。这种“承诺”可以理解为：见证在 X基和 Z基下被销毁（对应两类问题），测量结果则使用纠错码编码。由于测量经过纯化，证明者能够（在所有量子比特都返还给他之后）从一个基切换到另一个基。

有趣的是，在我们的协议中，每一轮的问题都是固定的。尽管如此，到协议结束时，我们已经要求证明者分别根据 X 和 Z 提供答案，因此所有可能向证明者提出的问题都已涵盖。此外，在最后一轮，验证者确实需要从一个分布中抽取问题，因为需要不同的问题来定义不同的可观测量，以刻画证明者的行为。这些不同的可观测量为研究反对易关系提供了对象，而该关系是刻画证明者测量的关键。

单证明者单量子比特测试。 遵循 [Vid20], 中的表述，量子比特可以理解为一个能够以两种相互不兼容的方式进行观测的系统——更准确地说，它是一个配备了一对反对易可观测量的系统，这实质上对应于 X 和 Z 算子在同构意义下的存在。

我们设计了一个简单的协议，其中证明者与验证者进行多轮交互。最后，验证者向证明者发送一个经典比特，证明者再以一个经典比特作答。不失一般性地，在最后一轮中，证明者根据验证者的问题比特，在某个量子态上应用两种可观测量中的一种。我们证明，这两种可观测量在该量子态上反对易。要迫使证明者在某个 EPR 对的一半上测量反对易的可观测量（另一半由验证者持有），很容易做到

；但在这里，挑战在于评估证明者自行选择的量子态上的反对易性（即该量子态不受验证者或协议的约束）。

将这一结论与多证明者设置中的现有研究进行比较很有意思。在 [NV16], 中，作者使用了一种标准的非局域博弈，其中多证明者反对易博弈的鲁棒性同时涉及 EPR 对的鲁棒性，以及作用于 EPR 对上的反对易算子的鲁棒性。众所周知，这些鲁棒性结果足以构造针对 XZ哈密顿量的 PCP 博弈版本。为了在单证明者博弈中获得所需的 QMA 结果，有意义的反对易关系应满足什么条件？我们是否应该检验单个证明者是否持有 EPR 对？由于原始证明者作用于不同的希尔伯特空间，我们是否应该预期，压缩后，原本属于不同证明者的算子仍彼此对易？乍看之下，这两个问题的答案似乎都应该是肯定的。然而，这两者似乎都没有作为子程序出现在我们的最终协议中。直观而言，这说得通，因为在包含 EPR 对的非局域博弈中，作用于第一位证明者的算子等价于其转置作用于第二位证明者的算子。在这种情形下，EPR 对起到了桥梁作用。由于只有一位证明者，就不需要在他们之间搭桥；两位证明者都可以作用于同一组量子比特，而这些算子也就不再对易。

构造。我们的协议由三轮组成。

- 在第一轮中，诚实证明者发送其量子态在 Z基下的纯化测量。纯化测量的结果存储在寄存器R中。
- 验证者可以选择在寄存器R上施加相位翻转门（Z 门）、在计算基（Z 基）下测量，或什么也不做（施加恒等算子）。然后，验证者将寄存器R送回证明者。
- 在第二轮中，诚实证明者撤销在 Z 基下的纯化测量，并发送其量子态在 X 基下的纯化测量（位于同一个寄存器R中）。
- 验证者可以再次选择施加相位翻转门（ Z 门）、在 Z 基下测量，或什么也不做。
- 在第三轮中，验证者将R送回证明者，并附上一道一比特的问题，内容为“X”或“Z”。
- 证明者在 X 基下撤销纯化测量，并返回与验证者的问题相对应的测量结果。

请注意，对可观测量的纯化测量结果施加相位翻转门，等价于直接将可观测量本身作为门施加。对可观测量的纯化测量结果在计算基下进行测量，等价于直接对量子态测量该可观测量。

在该协议中，验证者从以下四种测试中均匀随机抽取一种，并与证明者一起执行：

1. **Z一致性测试：**验证者在第一轮进行测量，在第二轮不做任何操作，在第三轮向证明者发送“Z”，并且仅当第一轮的测量结果与证明者对第三轮“Z”查询给出的比特答案相符时才接受。

2. **X 一致性测试（标准）：** 验证者在第一轮不做任何操作，在第二轮进行测量，在第三轮向证明者发送“X”，并且仅当第二轮的测量结果与证明者对第三轮“X”查询给出的比特答案相符时才接受。

3. **X 一致性测试（翻转）：** 验证者在第一轮施加相位翻转，在第二轮进行测量，在第三轮向证明者发送“X”，并且当且仅当第二轮的测量结果与证明者对第三轮“X”查询的回答比特一致时接受。

4. **反对易测试：** 验证者在第一轮进行测量，在第二轮施加相位翻转，在第三轮向证明者发送“Z”，并且当且仅当第一轮的测量结果与证明者对第三轮“Z”查询的回答比特相反时接受。

如果我们将证明者在最后一轮施加的可观测量解释为酉算子，那么 Z 和 X 可以在最后一轮同时施加，且施加顺序可以不同。这些可观测量之间的反对易关系 $XZ = -ZX$ 正是我们要证明的命题。反对易测试已经给出了一个具有反对易关系形式的初始方程，而一致性测试则用于将该方程中的操作转移到最后一轮使用的可观测量上。实际上，可以将 ZX 和 XZ 视为一系列操作：Z 后接 X ，这是在 XZ的情况下。这些操作可以分布在交互的不同阶段中。例如，我们可以在第一轮和最后一轮都施加 Z 。另一个例子是，在第一轮施加相位翻转、在第二轮进行测量，这相当于先施加Z ，再施加 X。一致性测试确保了在不同轮次施加 Z 和 X 之间的关系。

前述操作说明，将一致性测试翻转后，可以用来诱导不同的可观测量序列。从非局域博弈的角度看，这项测试的重要性还有另一种解释。直观来说，如果不进行翻转，证明者只需选择一个初始态，并在该初始态下进行博弈。引入翻转后（验证者仅在所有测量之前进行翻转），证明者便不得不在多个初始态下进行博弈。通过将该协议与非局域博弈进行比较，我们可以得出若干有趣的观察结果。

与非局域博弈的比较。为说明其背后的直觉，我们给出一种基于非局域博弈单证明者变体的构造。由于我们尚未发现采用非局域博弈框架能带来任何特定优势，因此，关于量子 IOP 和强量子 IOP 的主要结果并非基于此处所述的非局域博弈测试。因此，我们省略其正式表述。

我们以幻方博弈为例进行说明，但该构造可以自然地推广到其他非局域博弈。

	c1	c2	c3
r1	(1) $I \otimes Z$	(2) $Z \otimes I$	(3) $Z \otimes Z$
r2	(4) $X \otimes I$	(5) $I \otimes X$	(6) $X \otimes X$
r3	(7) $X \otimes Z$	(8) $Z \otimes X$	(9) $Y \otimes Y$

该协议包含6轮次（12条消息），每一轮对应幻方中的一行（从上到下依次编号为 r1、r2、r3）或一列（从左到右依次编号为 c1、c2、c3）

游戏。轮次按固定顺序进行：r2、c3、r1、c2、r3、c1。[3] 每一轮中，诚实证明者会发送相关行或列的纯化测量（2 个量子比特，第三个可以推断得出）。验证者要么在 Z 基下测量，要么对部分量子比特施加 Z 门操作，或什么也不做，然后将量子比特发回。随后，诚实证明者撤销纯化测量。

交互结束时，验证者发送一个索引 $\{1,\dots,9\}$（对应幻方中的 9 个位置），证明者返回一个比特。唯一进行的测试是一致性检查：确保行与列的交点处保持一致，以及前 6 轮与最后一轮之间保持一致。这些测试还包括在进行两次一致性检查测量之前采用各种形式的翻转。由于翻转方式只有常数种，因此我们可以以常数概率执行每一种可能的测试。反对易关系体现在最后一轮中，具体来说，是位置 2（第一行的第二个元素）与位置 4（第二行的第一个元素）之间的关系。

直观而言，要求证明者依次测量所有行或所有列，会迫使其采用量子策略。实际上，证明者是在承诺回答所有可能的问题。请注意，由于这个游戏没有经典解，因此证明者不可能在单轮中对所有问题都作出正确回答。

令人惊讶的是，即使没有所有翻转测试，虽然可靠性得以保留，但该协议在鲁棒性方面仍有不足，因为它无法强制实现反对易关系。我们构造出了反例：它们仅使用对易算子，就能通过幻方测试的单证明者版本。然而，在所有这些反例中，初始态都由所用算子唯一确定。理解翻转测试的另一种视角，是将其与两个证明者之间一致性关系所发挥的作用进行比较。在多证明者设置中，一致性关系可用于切换操作所作用的玩家。这对于证明魔方博弈的鲁棒性至关重要。在确立 X 与 Z 之间的反对易关系后，这种“玩家切换”也发挥着重要作用。通过这种切换，可以推导出 Weyl–Heisenberg 群中元素之间的关系：目标是证明$X(a)Z(b)X(c)Z(d) = (-1)^{bc}X(a+c)Z(b+d)$，其中一个关键子目标是能够“翻转”中间算子 $Z(b)X(c)$。一致性检查用于实现“玩家切换”，进而使我们能够推导出 $X(a)Z(b)X(c)Z(d) - X(a)Z(b)X(c) \otimes Z(d) = 0$，从而能够在 $X(a)Z(b)X(c)$中翻转 $Z(b)X(c)$。

分析鲁棒性时面临的其他困难。请注意，在协议进行到中间时，诚实证明者不一定会应用纯化可观测量，也可能应用任意酉算子。这给我们带来了困难，因为我们更希望将证明者在中间轮次的操作表述为可观测量，即一个既是厄米算子、平方又等于恒等算子的算子，这样就可以直接将其与最后一轮的可观测量进行比较。此外，证明者可能会在下一轮交互之前对其量子态施加额外的酉算子，从而有可能作弊。不过，这已经涵盖了证明者可能拥有的全部灵活性。

为了解决这些问题，我们可以将验证者诚实执行的测量或相位翻转门重新诠释为证明者操作的一部分，将其吸收到证明者的操作中，并将其视为证明者的可观测量。尽管证明者仍可能在轮次之间施加额外的幺正变换，但这

[3]虽然并不严格要求特定的顺序，但并非所有排列都可行。这个顺序是通过演绎得出的。具体而言，我们需要保留下列顺序：包含位置 4 的行的索引必须首先出现，接着是包含位置 9（第三行的第三个元素）的列的索引，然后是包含位置 2 的行的索引。同样，包含位置 2 的列的索引应首先出现，接着是包含位置 9 的行的索引，然后是包含位置 4 的列的索引。按照这一顺序，我们便能将数对 (2, 4 4, 2 9) 转换为一个中间含有 的表达式，并最终转换为 ( )。

不会对我们的分析产生显著影响。

多量子比特测试。 我们沿用 [NV16] 中的标准方法，将单量子比特测试扩展为多量子比特测试。具体而言，在每一轮中，证明者都会向验证者发送其见证在该轮对应基底下的测量结果：第一轮使用 Z 基，第二轮使用 X 基，第三轮则根据验证者的问题采取相应操作。证明者始终以哈达玛编码的形式回复纯化测量结果。尽管证明者的时间复杂度为指数级，但仍可使用具有任意扇出的受控非门，通过对数深度电路实现。

测试克利福德哈密顿量的能量。 为了估计可观测量 $X(a)Z(b)Y(c)$，我们可以利用量子比特测试的第一轮和第二轮。测量一个可观测量等价于将其受控版本作为酉算子施加，其中控制量子比特初始化为 $|+\rangle$ 态，随后在 X 基下测量控制量子比特。在我们的设置中，验证者在第一轮的 $b+c$ 位置执行一个受控非门，并在第二轮的 $a+c$ 位置再执行一个受控非门，同时在控制量子比特上额外施加 c 次相位门。此过程使我们能够测试克利福德哈密顿量的能量。

使通信量达到多项式级别的挑战。 请注意，我们描述的构造具有指数级通信复杂度。在每一轮中，无论是测量形如 $X(a)$ 还是 $Z(b)$ 的可观测量，证明者都必须同时发送所有 $a, b \in \mathbb{F}_2^n$ 的测量结果，因此无法预知验证者在该轮会读取哪个特定位置。

我们尝试遵循 [dlS22] 的方法，将协议长度缩减至多项式级别。我们没有像 λ-偏置集合那样采用 [dlS22]，而是选择使用经典局部可测试码。作出这一选择是因为，尽管可以检验证明者是否确实发送了某个 λ-偏置集合与某个字符串之间内积的叠加态（即预期的纯化测量结果），但这种检验相当复杂。

此外，在 [dlS22] 的设置中，使用任何纠错码都会得到类似结果。然而，他们的分析所要求的一个关键性质是，证明者的状态必须是完全混合态。这一假设对于确保表示 $\pi(a)X = U(a)XU(a)^\dagger$ 构成酉表示至关重要，而这也是应用 Poincar´e 不等式的必要条件。在多证明者设置中，这一性质自然成立，因为可以假设证明者以 EPR 对 [4] 起始。然而，在我们的设置中，单个证明者可以选择任意初始态，因此这一假设不再成立。

3 组织结构

在第4 节中，我们将介绍全文所需的记号和约定，并定义 Clifford-哈密顿量问题，说明如何放大间隙。第5节将正式定义量子交互式预言机证明（qIOP）及其变体。第7 节将讨论扩展到多量子比特测试，并以此为基础，在第8 节介绍强量子交互式预言机证明的构造。附录A 介绍我们对单量子比特测试的方法。虽然这一节与主要结果没有直接关联，但它进一步阐述了此前提出的单证明者设置下量子比特测试背后的思路。

[4] 这是因为该游戏是一个同步的游戏 me.

致谢。T.V. 获得美国空军科学研究办公室（AFOSR）FA9550-22-1-0391 号资助，以及瑞士教育、研究与创新国务秘书处（SERI）的支持。本研究的部分工作是在 T.V. 于以色列魏茨曼科学研究所工作期间完成的，当时他获得了新科学家中心的研究资助。B.S. 获得魏茨曼科学学院的奖学金。作者谨向 Zvika Brakerski 教授致谢，感谢他参与有益的讨论。

4 预备知识

本节介绍本文中使用的记号和约定，以确保表述清晰且一致。

寄存器和空间的记号。

- **寄存器：**我们用无衬线字体的大写字母（如 X、Y、Z）表示量子寄存器。
- **希尔伯特空间：**我们用花体大写字母（如 $\mathcal{X}$、$\mathcal{Y}$、$\mathcal{Z}$）表示与相应寄存器关联的复希尔伯特空间。
- **量子信道：**我们用黑板粗体字母（如 $\mathbb{P}$、$\mathbb{Q}$）或大写希腊字母（如Φ、Ψ）表示量子信道。
- **算法：** 用大写等宽字母（如 A、B、C）表示算法。

受控酉变换。 为简化表述，我们引入受控酉操作的记号。

定义 4.1 (受控酉变换**)**。 设P 为一个寄存器， U_{P} 为作用于其上的酉算子。设R 为一个单量子比特寄存器。当R 中的量子比特为 $|1\rangle$时，受控酉变换 $C(U_{\mathsf{P}},\mathsf{R})$ 将 U_{P} 作用于该寄存器：

$$C(U_{\mathsf{P}},\mathsf{R}) = \begin{pmatrix} I_{\mathsf{P}} & 0 \\ 0 & U_{\mathsf{P}} \end{pmatrix}$$

更一般地，对于维数为 d 的寄存器R'以及 $i \in [d]$，当寄存器R 中的量子比特为 $|i\rangle$时，受控酉变换 $C(U_{\mathsf{P}},\mathsf{R}\ i)$将 U_{P} 作用于该寄存器：

$$C(U_{\mathsf{P}},\mathsf{R},i) = \mathrm{diag}(\underbrace{I_{\mathsf{P}},\ldots,I_{\mathsf{P}}}_{i-1},U_{\mathsf{P}},\underbrace{I_{\mathsf{P}},\ldots,I_{\mathsf{P}}}_{d-i})$$

纯化测量。 我们定义纯化测量，以模拟对可观测量进行测量并将结果存储在寄存器中。

定义 4.2 (纯化测量**)**。 设P、R 为寄存器， O_{P} 为一个分解为$O = \sum_{i=1}^{r} a_i P_i$的可观测量，其中每个 P_i 都是正交投影，并且$I = \sum_i P_i$。执行纯化测量并将结果存储在R 中的酉算子为：

$$P(O_{\mathsf{P}},\mathsf{R}) = \sum_{i=1}^{r} P_{i,\mathsf{P}} \cdot (X(a_i))_{\mathsf{R}}$$

注意，应用 $P(O_{\mathsf{P}},\mathsf{R})$，然后测量 R，等同于直接测量 O_{P} 并将结果存储在 R 中。

EPR基。 我们如下定义 EPR 基:

定义 义 4.3 (EPR基)。 设 $|\varphi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$。*EPR* 基量子态为 *e:*

$$
\begin{aligned}
|E_{00}\rangle &= \left|\varphi^+\right\rangle\!\left\langle\varphi^+\right|, \\
|E_{10}\rangle &= (Z\otimes I)\left|\varphi^+\right\rangle\!\left\langle\varphi^+\right|(Z\otimes I), \\
|E_{01}\rangle &= (X\otimes I)\left|\varphi^+\right\rangle\!\left\langle\varphi^+\right|(X\otimes I), \\
|E_{11}\rangle &= (ZX\otimes I)\left|\varphi^+\right\rangle\!\left\langle\varphi^+\right|(XZ\otimes I).
\end{aligned}
$$

子寄存器和子串。 我们引入用于访问子寄存器和子串的记号:

定义 4.4。 设 $\mathsf{A} = (\mathsf{A}_1, \ldots, \mathsf{A}_n)$ 为一个寄存器元组，并且 $S = \{s_1, \ldots, s_k\} \subset [n]$ 满足 $s_1 < \cdots < s_k$。定义 $\mathsf{A}_S = (\mathsf{A}_{s_1}, \ldots, \mathsf{A}_{s_k})$。

定义 4.5。 设 n、$m \in \mathbb{Z}_+$、$w \in \mathbb{F}_2^n$、$\mathsf{T} = (\mathsf{T}_i)^{i\in[n]}$，以及 $s = (s_1, \ldots, s_m) \in [n]^m$。定义:

$$
w(s) = (w_{s_1}, \ldots, w_{s_m}), \quad \mathsf{T}(s) = (\mathsf{T}_{s_j})_{j\in[m]}\ .
$$

相对于一个量子态的内积。

定义 4.6. 对于半正定算子 σ，定义:

$$
\langle A, B\rangle_\sigma = \mathrm{Tr}(A^\dagger B\sigma), \quad \|A\|_\sigma^2 = \mathrm{Tr}(A^\dagger A\sigma)\ .
$$

4.1 Clifford-哈密顿量问题的间隙放大

Clifford-哈密顿量问题由以下文献提出: [BJSW16]。克利福德哈密顿量是一种局部哈密顿量，其每个局部项都具有 $C^\dagger(|0\rangle\langle 0|)^{\otimes 5}C$的形式，其中 C 是五重克利福德群中的一个元素。在选择要进行放大的哈密顿量问题时，我们关注两个关键参数: 能隙和哈密顿量的 ℓ_1-范数。-范数指将哈密顿量分解为可观测量线性组合时，各系数绝对值之和。在Kitaev时钟构造中，YES 和 NO 实例的最小能量都非常接近 0，因此不适合作为间隙放大的起点。放大的标准方法是先平移哈密顿量 H，例如将其替换为 $I - H$。然而，这种平移会使 ℓ_1-范数增至 1 以上；反复进行时，范数可能会呈指数级增长。

在实际应用中，由于我们最终要测量可观测量，因此只需确保平移后哈密顿量成为可观测量之和。这样，在放大（即重复）之前，ℓ_1-范数自然为 1。使用克利福德哈密顿量项的一大优势在于，它们是投影P，因此可以将它们平移至 $1 - 2P$，从而得到可观测量。然后，我们就可以通过重复来放大间隙。

注意

$$
C^\dagger(|0\rangle\langle 0|)^{\otimes 5}C = \prod_{j\in[5]} C^\dagger \cdot \left(I^{\otimes j-1} \otimes \frac{I+Z}{2} \otimes I^{\otimes(5-j)}\right) \cdot C,
$$

这可能表明，我们也可以将 Clifford 投影直接转化为一系列 XZ 哈密顿量。这或许意味着我们现在可以测量 XZ 哈密顿量。然而，这种转化无法保持 ℓ_1 范数。放大后，情况会变得更糟: 范数为 1 的 Clifford 哈密顿量可能会被转化为一系列范数呈指数级增大的 XZ 哈密顿量。结果是，尽管放大增大了谱隙,

范数的指数级膨胀会导致有效间隙呈指数级缩小，从而使放大失效。

以下定义描述了 QMA 完备构造中使用的一种特定类型的局部哈密顿量项。每一项都投影到一组量子比特上的经克利福德变换的全零态，同时在其余量子比特上作用为恒等算子。

定义 4.7 (克利福德哈密顿量投影)。 若哈密顿量（厄米矩阵） H 在量子比特集合 S 上非平凡作用为 $C^\dagger \left|0^{|S|}\right\rangle\!\left\langle 0^{|S|}\right| C$，其中 C 是 $|S|$重克利福德群的一个元素，则称其为克利福德哈密顿量投影。当且仅当满足上述条件时，称 H 为克利福德哈密顿量投影。更具体地说，

$$H = (C^\dagger |0^{|S|}\rangle\langle 0^{|S|}|C)_S \otimes I_{[n]-S}.$$

此定义将上述投影推广到由多个此类投影组成的完整哈密顿量。对它们取平均，可确保 H 的谱介于 0 和 1 之间。

定义 4.8 (克利福德哈密顿量)。 若哈密顿量 $H \in \mathbb{C}^{2^n} \otimes \mathbb{C}^{2^n}$ 是由多项式数量 $m = \mathrm{poly}(n)$ 个克利福德哈密顿量投影项 H_i取均匀平均得到的，则称其为克利福德哈密顿量。也就是说，

$$H = \frac{1}{m} \sum_{i \in [m]} H_i \ .$$

此外，如果每个 H_i 至多对 k 个量子比特产生非平凡作用，则 H 是 k-局部的。

该问题询问给定局部克利福德哈密顿量的基态能量是低于 $a(n)$ 还是高于 $b(n)$，并承诺两者之一成立。

定义 4.9 （局部克利福德哈密顿量问题）。 设 $k \in \mathbb{Z}^+$，并设 a、b：$\mathbb{Z}^+ \to \mathbb{R}^+$ 为单调不减函数，使得 $\forall n \in \mathbb{Z}^+$、$a(n) < b(n)$。局部克利福德哈密顿量问题$\mathcal{LCH}(k, a, b)$ 是由下列内容定义的承诺问题 (S_{yes}, S_{no})：

- S_{yes}：满足 $\lambda_{\min}(H) \leq a(n)$ 的 k-局部克利福德哈密顿量 $H \in \mathbb{C}^{2^n} \otimes \mathbb{C}^{2^n}$ 的集合，
- S_{no}：满足 $\lambda_{\min}(H) \geq b(n)$ 的 k-局部克利福德哈密顿量 $H \in \mathbb{C}^{2^n} \otimes \mathbb{C}^{2^n}$ 的集合。

这个定理来自 [BJSW16]，表明对于 5 局部项和多项式小的完备性-可靠性间隙，局部克利福德哈密顿量问题是 QMA 完全的。它为研究 QMA 提供了一个具体且结构化的哈密顿量族。

定理 4.10 ([BJSW16]中的定理 2）。存在多项式 p 和 q，使得该问题

$$\mathcal{LCH}(5, 2^{-p(n)}, 1/q(n))$$

是 *QMA* 完全的。

这个引理介绍了一种间隙放大技术，可增大克利福德哈密顿量问题的 YES 实例与 NO 实例之间的谱隙。具体而言，变换 $H' = (1-2H)^{\otimes N}$ 会使间隙呈指数级增大。然而，这会以破坏哈密顿量的局域性结构为代价。该证明利用了厄米算子的谱性质，以及其张量幂的乘法特性。

引理 4.11 （Clifford-哈密顿量问题的间隙放大）。 设 $(S_{yes}, S_{no}) = \mathcal{LCH}(k, a, b)$满足 $a, b \in (0, 0.1)$。设 $H \in S_{yes} \cup S_{no}$，并定义 $H' = (1-2H)^{\otimes N}$其中某个奇数 $N \in \mathbb{Z}^+$。那么：

1. 若 $H \in S_{yes}$，则 $\lambda_{\max}(H') \geq (1-2a)^N$。

2. 如果 $H \in S_{no}$，那么 $\lambda_{\max}(H') \leq (1-2b)^N$。

此外，设 p、q 如定理 4.10 中所述。对于 $k=5$、$a=2^{-p(n)}$、$b=1/q(n)$，以及 $N=q^2(n)$，存在一个多项式 s使得：

1. 如果 $H \in S_{yes}$，那么 $\lambda_{\max}(H') \geq 1-2^{-s(n)}$。

2. 如果 $H \in S_{no}$，那么 $\lambda_{\max}(H') \leq 2^{-s(n)}$。

证明。如果 $H \in S_{yes}$，那么

$$\lambda_{\max}(H') \geq (1-2a)^N \geq 1-2aN \geq 1-2^{-s(n)} .$$

如果 $H \in S_{no}$，那么

$$\lambda_{\max}(H') \leq (1-2b)^N = (1-2b)^{1/(2b)\cdot 2bN} \geq 1-2^{-s(n)} .$$

□

4.2 可概率检验的邻近性证明

本节回顾可概率检验的邻近性证明（PCPP），该概念由 [BGH+04] 引入，以及其在规范 $\mathcal{P}$-完全问题 CircuitValue中的应用。这些概念在我们的演绎中发挥着核心作用。

定义 4.12（[BGH+04]）。我们将 $\mathcal{P}$-完全语言 Circuit Value 定义为 $\text{CktVal} = \{(C,w) : C(w) = 1\}$，其中 C 是一个布尔电路，w 是一个输入字符串。对于对语言$L \subseteq \{0,1\}^* \times \{0,1\}^*$，我们定义 $L(x) = \{y : (x,y) \in L\}$。

下面的定义形式化了一种证明系统，在该系统中，验证者无需读取整个输入，就能高效地检查给定输入是否接近有效输入。

定义 4.13（邻近性的 PCP（PCPP），[BGH+04]）。设 s，δ：$\mathbb{Z}^+ \to [0,1]$ 为函数。若验证者 V 是对语言对 L 的可概率检验的邻近性证明（*PCPP*）系统，且接近参数为 δ、可靠性误差为 s，则对于每一对字符串 (x, y)，以下条件成立：

- 完备性：若$(x,y) \in L$，则存在一个证明字符串 π，使得 $V(x)$ 以概率1接受预言机 $y \circ \pi$。
- 可靠性：若 y 与 $L(x)$相距 $\delta(|x|)$-远，则对于每个 π，验证者 $V(x)$ 以严格小于 $s(|x|)$的概率接受预言机$y \circ \pi$。

如果未明确指定 s 和 δ，则假设它们是区间(0,1)内的常数。

以下定理由 [BGH+04]提出，证明 Circuit Value 问题存在一个 PCPP。

定理 4.14 ([BGH+04])。存在一个常数 $\delta_0 \in (0,1)$，使得对于所有 $n \in \mathbb{Z}^+$ 和所有$\delta < \delta_0$，语言 Circuit Value 具有邻近性 *PCP*（针对大小为 n 的电路），其参数如下：

- 随机性复杂度 $O(\log n)$，
- 查询复杂度 $O(1)$，
- 完美完备性，且
- 可靠性误差 $1-\Omega(\delta)$ 对应接近参数 δ。

4.3 群稳定性

本节将回顾一些数学工具和基础结果，这些内容将在我们的整个分析过程中使用。我们不会直接照搬现有文献中的内容，要么是因为相关结果并未被明确表述，要么是因为它们无法完全满足我们的要求。首先，我们介绍 σ-加权的希尔伯特–施密特正半定厄米型和半范数；借助它们，我们可以在存在量子态的情况下研究近似表示和算子比较。随后，我们回顾 Gowers 和 Hatami 关于泡利群近似表示的一个基本稳定性结果，该结果将作为我们多量子比特测试的核心分析工具。

我们定义关于半正定算子 σ 的半正定厄米型和半范数如下。类似的定义已见于 [Vid11] 以及大量关于非局域博弈的文献中。

定义 4.15。 对于半正定算子 σ，定义：

$$\langle A, B\rangle_\sigma = \mathrm{Tr}(A^\dagger B\sigma), \quad \|A\|_\sigma^2 = \mathrm{Tr}(A^\dagger A\sigma).$$

以下一些有用性质是众所周知的。

引理 4.16。 设 σ 是一个半正定算子。那么对于任意算子 A、B：

$$\begin{aligned}\|A\|_\sigma^2 &\geq 0,\\ \|A+B\|_\sigma^2 &\leq 2\|A\|_\sigma^2 + 2\|B\|_\sigma^2,\\ \|AB\|_\sigma^2 &\leq \|A\|^2 \cdot \|B\|_\sigma^2,\end{aligned}$$

且如果 $C^\dagger C = I$，那么

$$\langle CA, CB\rangle_\sigma = \langle A, B\rangle_\sigma.$$

证明。 第一项和最后一项由定义可得。对于第二项，

$$\begin{aligned}\|A+B\|_\sigma^2 &= \mathrm{tr}((A+B)^\dagger(A+B)\sigma)\\ &= 2\mathrm{tr}(A^\dagger A\sigma) + 2\mathrm{tr}(B^\dagger B\sigma) - \mathrm{tr}((A-B)^\dagger(A-B)\sigma)\\ &\leq 2\|A\|_\sigma^2 + 2\|B\|_\sigma^2 .\end{aligned}$$

对于第三项，

$$\begin{aligned}\|AB\|_\sigma^2 &= \mathrm{tr}(A^\dagger AB\sigma B^\dagger)\\ &\leq \|A^\dagger A\| \cdot \mathrm{tr}(B\sigma B^\dagger)\\ &= \|A\|^2 \cdot \|B\|_\sigma^2.\end{aligned}$$

□

接下来回顾 σ-半范数的三角不等式，参见例如 [NW19，事实 4。28]。

引理 4.17（σ-半范数的三角不等式）。 设 σ 是一个半正定算子。那么对于任意算子 A 和 B，

$$\|A+B\|_\sigma \leq \|A\|_\sigma + \|B\|_\sigma.$$

现在，我们介绍几个定义，它们对于群表示和群的近似表示很有用。

定义 4.18 (酉群)。 将 $U(\mathbb{C}^d)$ 定义为酉矩阵群。

定义 4.19 （近似表示）。 给定有限群 G、维数 $d \geq 1$, $\varepsilon \geq 0$，以及一个迹为 1 的 d 维半正定矩阵 σ，一个 $(\varepsilon, \sigma, D_1, D_2)$-表示是一个函数 $f\colon G \to U(\mathbb{C}^d)$，满足：

$$\mathbb{E}_{x\sim D_1, y\sim D_2} \Re\left(\langle f(xy), f(x)f(y)\rangle_\sigma\right) \geq 1-\varepsilon.$$

现在我们陈述 Gowers 和 Hatami 提出的稳定性定理。该定理使我们能够得出结论：泡利群的近似表示在等距映射意义下与泡利群本身接近。我们针对 Weyl-Heisenberg 群，以及满足 $f(-x) = -f(x)$、$f(1) = I$ 的近似表示来具体陈述该定理。这是因为我们不仅希望近似表示接近 Weyl-Heisenberg 群的某个表示，还希望它对应于典范表示 $\pm X(a)Z(b)$。条件 $f(-x) = -f(x)$ 和 $f(1) = I$ 用于唯一确定这个表示。 [MNZ24] 的工作以不同方式处理了这一问题：他们首先得到 Weyl-Heisenberg 群的一个一般表示，然后说明如何分离出典范表示 $\pm X(a)Z(b)$。他们也没有将结果明确表述为定理。因此，尽管该证明广为人知，我们仍给出自己的版本，以强调表示论的视角。

定理 4.20 （Gowers-Hatami 稳定性定理， [GH17]）。 设 $\mathcal{P}_n$ 表示 n-量子比特 *Weyl–Heisenberg* 群，并设 $f\colon \mathcal{P}_n \to U(\mathbb{C}^d)$ 是一个 $(\varepsilon, \sigma,$ 均匀$(\mathcal{P}_n)$ $\mu)$-表示，满足： $\mathcal{P}_n$:

$$f(-x) = -f(x), \quad f(1) = I.$$

那么存在 $d' \geq d$、一个等距映射 $V\colon \mathbb{C}^d \to \mathbb{C}^{d'}$，以及一个表示 $g\colon \mathcal{P}_n \to U(\mathbb{C}^{d'})$，使得 $g(x) = \rho(x) \otimes I$，并且

$$\mathbb{E}_{x\sim\mu} \|f(x) - V^\dagger g(x) V\|_\sigma^2 \leq \Theta(\varepsilon),$$

其中 $\rho(\pm X(a)Z(b)) = \pm X(a)Z(b)$。

证明。 注意， $N = |\mathcal{P}_n| = 2\cdot 4^n$ 是唯一非一维的不可约表示$\rho(\pm X(a)Z(b)) = \pm X(a)Z(b)$，其维数为 $d_0 = 2^n$。

定义 V 如下：对于 $u \in \mathbb{C}^d$,

$$V(u) = \sqrt{\frac{N}{2d_0}} \cdot \mathop{\mathbb{E}}_{x\in\mathcal{P}_n} f(x)u \otimes \rho(x).$$

V 是一个等距映射：对于任意 u, $v \in \mathbb{C}^d$,

$$\begin{aligned}
u^\dagger V^\dagger V v &= \operatorname{tr}((Vu)^\dagger V v) \\
&= \frac{N}{2d_0} \cdot \operatorname{tr}\Big(\mathop{\mathbb{E}}_{x,y\in\mathcal{P}_n} u^\dagger f(x)^\dagger f(y) v \otimes \rho(x)^\dagger \rho(y)\Big) \\
&= \frac{N}{2d_0} \cdot \Big(\mathop{\mathbb{E}}_{x,y\in\mathcal{P}_n} u^\dagger f(x)^\dagger f(y) v \cdot \operatorname{tr}(\rho(x^{-1}y))\Big) \\
&= \frac{1}{2d_0}\Big(\mathop{\mathbb{E}}_{x\in\mathcal{P}_n} u^\dagger f(x)^\dagger f(x) v \cdot \operatorname{tr}(\rho(I)) + \mathop{\mathbb{E}}_{x\in\mathcal{P}_n} u^\dagger f(x)^\dagger f(-x) v \cdot \operatorname{tr}(\rho(-I))\Big) \\
&= u^\dagger v\ .
\end{aligned}$$

令，对于 $v \in \mathbb{C}^d$, $O \in \mathbb{C}^{d_0\times d_0}$,

$$(g(x))(v \otimes O) = v \otimes O\rho(x^{-1})\ .$$

注意， $g(-I) = -I$。在 $\mathcal{P}_n$ 的所有不可约表示中，唯一将 $-I$ 映射到 $-I$ 的是 ρ。那么，对于任意 $u,\ v \in \mathbb{C}^d$,

$$\begin{aligned}
u^*V^*g(x)Vv &= \mathrm{tr}((Vu)^*g(x)Vu) \\
&= \frac{N}{2d_0} \cdot \mathrm{tr}(\mathop{\mathbb{E}}_{z,y\in\mathcal{P}_n} u^\dagger f(z)^\dagger f(y)v \otimes \rho(z)^\dagger\rho(y)\rho(x^{-1})) \\
&= \frac{N}{2d_0} \cdot \mathop{\mathbb{E}}_{z,y\in\mathcal{P}_n} u^\dagger f(z)^\dagger f(y)v \cdot \mathrm{tr}(\rho(z)^\dagger\rho(y)\rho(x^{-1})) \\
&= \frac{1}{2d_0} \cdot (\mathop{\mathbb{E}}_{z\in\mathcal{P}_n} u^\dagger f(z)^\dagger f(zx)v \cdot \mathrm{tr}(I) + \mathop{\mathbb{E}}_{z\in\mathcal{P}_n} u^\dagger f(z)^\dagger f(-zx)v \cdot \mathrm{tr}(-I)) \\
&= \mathop{\mathbb{E}}_{z\in\mathcal{P}_n} u^\dagger f(z)^\dagger f(zx)v\ .
\end{aligned}$$

因此，

$$\begin{aligned}
\mathop{\mathbb{E}}_{x\sim\mu} \Re(\langle f(x), V^*g(x)V\rangle_\sigma) &= \mathop{\mathbb{E}}_{x\sim\mu,z\in_R\mathcal{P}_n} \Re(\mathrm{tr}(f(x)^\dagger f(z)^\dagger f(zx)\sigma)) \\
&= \mathop{\mathbb{E}}_{x\sim\mu,z\in_R\mathcal{P}_n} \Re(\mathrm{tr}(f(zx)^\dagger f(z)f(x)\sigma)) \\
&= \mathop{\mathbb{E}}_{x\sim\mu,z\in_R\mathcal{P}_n} \Re(\langle f(z)^\dagger f(zx), f(x)\rangle_\sigma) \\
&= \mathop{\mathbb{E}}_{x\sim\mu,z\in_R\mathcal{P}_n} \Re(\langle f(zx), f(z)f(x)\rangle_\sigma) \\
&\geq 1-\varepsilon\ .
\end{aligned}$$

因此，

$$\begin{aligned}
&\mathop{\mathbb{E}}_{x\sim\mu} \|f(x) - V^\dagger g(x)V\|_\sigma^2 \\
&= \mathop{\mathbb{E}}_{x\sim\mu} \mathrm{tr}((f(x)^\dagger - V^\dagger g(x)^\dagger V)(f(x) - V^\dagger g(x)V)\sigma) \\
&= 2 - 2\Re(\mathop{\mathbb{E}}_{x\sim\mu} \mathrm{tr}(f(x)^\dagger \cdot V^\dagger g(x)V)\sigma) \\
&\leq \Theta(\varepsilon)\ .
\end{aligned}$$

□

注 4.21。该定理的原始版本将傅里叶变换推广到了矩阵值函数和非阿贝尔群。值得注意的是，我们证明了，对于 *Weyl-Heisenberg* 群的任意近似表示，唯一的非一维不可约表示总是贡献一个显著的分量。

注 4.22。我们采用了 *[Vid20]*, 中的方法，而切换分布的想法由 *[MNZ24]*提出。不过，我们可以修改能量一致性测试，直接验证单个可观测量（例如 X（a）、 Y（b） 或 Z（c））的正确性。通过使用自校正，我们可以强制保证每个单独的 a、 b 和 c 的正确性，从而避免切换分布的需要。

下面的定理建立在上述结果之上，为我们的多量子比特测试提供了一个核心技术工具。

定理 *4.23*（多量子比特测试的鲁棒性）。设 $n, d \in \mathbb{Z}_+$, $\delta \in (0, 1)$，且 $\sigma \in \mathbb{C}^d \otimes \mathbb{C}^d$。设 μ_1 是定义在 $0, 1^n$上的分布。采样 $(b, a) \sim \mu_1$，然后从 $0, 1^n$中均匀随机采样 r。定义 μ_2 为 $(b + r, a)$的分布。设 $\rho(\pm X(a)Z(b)) = \pm X(a)Z(b)$。设 $f_X, f_Z : \{0, 1\}^n \to U(\mathbb{C}^d)$ 满足：

- $f_X(a)^2 = f_Z(b)^2 = I,\ f_X(a)^\dagger = f_X(a),\ f_Z(b)^\dagger = f_Z(b)$ *for all* $a, b \in \{0,1\}^n$,
- $f_X(a)f_X(b) = f_X(a+b),\ f_Z(a)f_Z(b) = f_Z(a+b)$, *for all* $a, b \in \{0,1\}^n$,
- $\mathbb{E}_{(b,a)\sim\mu_1} \| f_Z(b)f_X(a) - (-1)^{a\cdot b} f_X(a)f_Z(b) \|_\sigma^2 \le \delta$,
- $\mathbb{E}_{(b,a)\sim\mu_2} \| f_Z(b)f_X(a) - (-1)^{a\cdot b} f_X(a)f_Z(b) \|_\sigma^2 \le \delta$,

那么存在 $d' \ge d$、一个等距映射 $V : \mathbb{C}^d \to \mathbb{C}^{d'}$以及一个表示 $g : \mathcal{P}_n \to U(\mathbb{C}^{d'})$，使得 $g(x) = \rho(x) \otimes I$，并且

$$\mathbb{E}_{(b,a)\sim\mu_1} \| f_X(a)f_Z(b) - V^\dagger g(X(a)Z(b))V \|_\sigma^2 \le \Theta(\delta)\ .$$

证明。利用 $\mathcal{P}_n$ 中的任意元素都存在唯一的 $\pm X(a)Z(b)$ 形式的代表元这一点，对于 $a,\ b \in \{0,1\}^n$，我们定义 $f(\pm X(a)Z(b)) = \pm f_X(a)f_Z(b)$。接下来，我们需要验证 f 是一个近似表示。注意

$$\begin{aligned}
& f_X(a_0)f_Z(b_0)f_X(a_1)f_Z(b_1) - (-1)^{b_0\cdot a_1} f_X(a_0+a_1)f_Z(b_0+b_1) \\
= \ & f_X(a_0)f_Z(b_0)f_X(a_1)f_Z(b_1) - (-1)^{b_1\cdot a_1} f_X(a_0)f_Z(b_0)f_Z(b_1)f_X(a_1) \\
& + (-1)^{b_1\cdot a_1} f_X(a_0)f_Z(b_0)f_Z(b_1)f_X(a_1) - (-1)^{b_1\cdot a_1} f_X(a_0)f_Z(b_0+b_1)f_X(a_1) \\
& + (-1)^{b_1\cdot a_1} f_X(a_0)f_Z(b_0+b_1)f_X(a_1) - (-1)^{b_0\cdot a_1} f_X(a_0)f_X(a_1)f_Z(b_0+b_1) \\
& + (-1)^{b_0\cdot a_1} f_X(a_0)f_X(a_1)f_Z(b_0+b_1) - (-1)^{b_0\cdot a_1} f_X(a_0+a_1)f_Z(b_0+b_1)\ .
\end{aligned}$$

因此

$$\mathop{\mathbb{E}}_{(b_0,a_0)\sim Uniform(\mathcal{P}_n),(b_1,a_1)\sim\mu_1} \| f_X(a_0)f_Z(b_0)f_X(a_1)f_Z(b_1) - (-1)^{b_0\cdot a_1} f_X(a_0+a_1)f_Z(b_0+b_1) \|_\rho^2 \le \Theta(\delta)\ .$$

□

5 量子交互式预言机证明的形式化

本节将对量子交互式预言机证明（QIOP）的模型进行形式化。QIOP 是经典 IOP 的量子类比，验证者仅具有有限的量子访问权限。我们首先说明基本记号，然后介绍查询以及带查询的量子信道等基本概念和原语。接着，我们定义 qIOP 系统，并介绍用于刻画不同资源约束的变体。

5.1 记号

我们用无衬线字体 A、X 等表示量子寄存器，并用花体字母 $\mathcal{A}$、$\mathcal{X}$ 等表示相应的复希尔伯特空间。我们用 $L(\mathcal{H})$ 表示 $\mathcal{H}$ 上的线性算子，并用 $C(\mathcal{H})$ 表示 $\mathcal{H}$ 上的量子信道集合，即 $L(\mathcal{H})$ 上完全正且保迹的线性映射。

我们用 $d(\mathsf{A})$ 表示寄存器 A 的维度，并将满足 $d(\mathsf{A}) = 1$ 的寄存器称为平凡的。如果 A 是维度为 d_A 的寄存器，我们通过如下定义其上的计算基测量信道 $\mathbb{M}_\mathsf{A} \in C(\mathcal{A})$:

$$\mathbb{M}_\mathsf{A} = \sum_{i=1}^{d_A} \mathbb{M}_\mathsf{A}^i, \quad \mathbb{M}_\mathsf{A}^i(\rho_\mathsf{A}) = |i\rangle\langle i|\, \rho_\mathsf{A}\, |i\rangle\langle i|\ .$$

该信道对量子寄存器的标准基测量进行建模。

5.2 带查询的量子信道

查询信道是我们用于在 qIOP 中对量子访问进行建模的核心基本操作。

定义 *5.1*（查询）。设 $W = (W_1, \ldots, W_n)$、$R = (R_1, \ldots, R_m)$ 和 R' 均为量子比特寄存器。设 $k \in [n]$ 和 $\{s_1, \ldots, s_k\} \subseteq [n]$。设 $S = (W_{s_1}, \ldots, W_{s_k})$ 是 W 的子寄存器。那么，具有输入寄存器 R 和输出寄存器 R' 、作用于 S 上的查询信道，是一种仅作用于寄存器 S 和 R，并将 S 映射到 S、将 R 映射到 R'的量子信道。此外， Φ 的查询集合定义为$\{s_1, \ldots, s_k\}$。

带查询的量子信道由一次查询操作调用构成。具体而言，该信道首先选择一个查询集合 $\{s_1, \ldots, s_k\}$（通过测量），然后对寄存器 S 和 R 应用查询信道。这种结构模拟了通过预言机式访问进行的计算，其中查询模拟了与预言机进行的一轮交互。

定义 *5.2*（带查询的量子信道）。设 k、W、R 和 R' 如定义 *5.1* 所述。设 $I = (R_1, \ldots, R^{k\cdot\lceil\log(n)\rceil})$ 是 R 的一个子寄存器。我们将 W 称为见证寄存器，将 R 称为参考寄存器，并将 R' 称为后处理参考寄存器。令 S_s 表示由 $s = (s_1, \ldots, s_k) \in [n]^k$索引的子寄存器 $(W_{s_1}, \ldots, W_{s_k})$。对于每个 s，令 $\Phi_{\mathsf{RS}_s,s}$ 为寄存器 S_s 上的一个查询信道，其输入寄存器为 R，输出寄存器为 R'，如定义 *5.1* 所述。

若量子信道 Λ 可分解为如下形式，则称其为带查询的量子信道：

$$\Lambda = (\sum_s \Phi_{\mathsf{RS}_s,s} \otimes \mathbb{M}_{\mathsf{I}}^s) \circ \Psi,$$

其中 $\Psi \in C(\mathcal{R})$ 是一个量子信道。

定义 5.3。对于信道 Ψ，我们用 $t(\Psi)$表示其时间复杂度，即实现 Ψ所需的基本门数量的最小值。[5] 我们经常滥用记号，用 $t(\Psi)$ 表示信道 Ψ时间复杂度的一个上界。

复杂度参数。对于一个带查询的量子信道，我们为其关联以下参数：

- 证明**长度**为 $l(\Lambda) = n$。
- 查询**复杂度**为 $q(\Lambda) = k$。
- 时间**复杂度**为 $t(\Lambda)$。

以下定义对带查询的量子算法这一概念作出形式化表述。具体而言，它将此类算法建模为由一个经典多项式时间算法指定，该算法输出一个带查询的量子信道。

定义 5.4 (带查询的量子算法**)**。若算法 A 是带查询的量子算法，则 A 是一个经典多项式时间算法，它在给定输入 $x \in \{0,1\}^*$时输出一个带查询的量子信道的描述。令 $\mathbb{A}_x$ 表示由 $A(x)$生成的量子信道。

A 的复杂度由三个参数刻画：证明长度 $l(n)$、查询复杂度$q(n)$以及时间复杂度 $t(n)$。对于任意长度为 n 的输入 x，每个参数都定义为通道 $\mathbb{A}_x$ 所使用的相应资源的上界。

此外，我们用 $A(x, \rho_{\mathsf{W}})$ 表示 $\mathbb{A}_x(\rho_{\mathsf{W}} \otimes |0\rangle\langle 0|_{\mathsf{R}})$。我们用 $A(x)$ 表示 $\mathbb{A}_x(|0\rangle\langle 0|_{\mathsf{W}} \otimes |0\rangle\langle 0|_{\mathsf{R}})$。最后，我们用 $\mathbb{A}_x$ 的见证寄存器表示 $A(x)$的见证寄存器。

[5]为此，我们 假设已固定某个由单量子比特门和双量子比特门组成的有限通用门集 d.

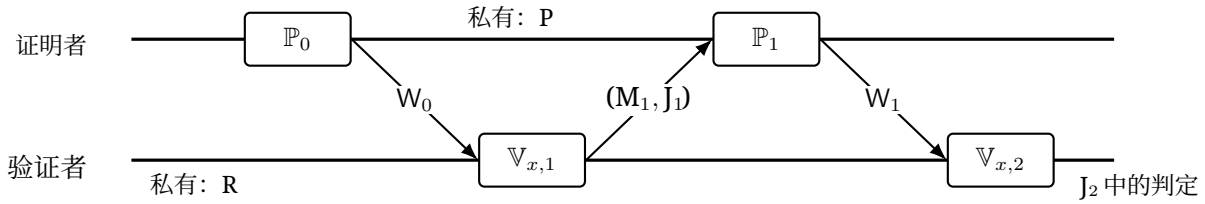


图 1：一个 $m = 3$-消息量子交互式证明的示例。

5.3 量子交互式预言机证明系统

在全面介绍量子交互式预言机证明系统之前，我们先使用前一小节引入的记号来表述著名的量子 PCP 猜想，并以此作为指导性示例，帮助阐明这些定义。

定义 5.5（量子概率可检验证明系统）。对于承诺问题 (S_{yes}, S_{no})，量子概率可检验证明系统是一个带查询的量子算法 V，满足：

1. 高效性：V 具有多项式时间复杂度。
2. 完备性：对于任意 $x \in S_{yes}$，存在一个量子态 ρ，使得 $\Pr[V(x) = 1] \geq \frac{2}{3}$。
3. 可靠性：对于任意 $x \in S_{no}$ 和任意量子态 ρ，$\Pr[V(x) = 1] \leq \frac{1}{3}$。

定义 5.6（量子概率可检验证明）。令 $l, q : \mathbb{Z}_+ \to \mathbb{Z}_+$。定义 $\mathcal{QPCP}(l, q)$ 为证明长度为 l 且查询复杂度为 q 的量子概率可检验证明系统所涵盖的承诺问题集合 (S_{yes}, S_{no})。

备注 5.7。我们的定义与量子 *PCP* 的标准（非自适应）定义一致 *[AAV13, GJMZ23, BHW24]*。

猜想 5.8（qPCP猜想）。$\mathrm{QMA} \subseteq \mathcal{QPCP}(\text{poly } O(1))$

我们现在引入量子交互式预言机证明（qIOP）系统的核心定义，它是经典交互式预言机证明系统的量子类比。

qIOP 系统由一系列算法 $V_1, \ldots, V_n$ 组成，其中每个 V_i 都是带查询的量子算法。验证者和证明者以初始态 $|0\rangle$ 开始。在交互过程中，验证者可以读取和修改证明者的消息寄存器，以此回应证明者的消息。验证者还可以保留证明者消息寄存器的一部分，并在后续轮次的交互中将其返回。验证者受到若干复杂度限制，而恶意证明者则被假定为计算能力不受限制。可靠性和完备性的定义与经典交互式证明系统中的定义类似。此外，验证者始终可以向证明者发送经典消息。

我们首先回顾量子交互式证明的定义，然后给出量子交互式预言机证明的定义。3 消息情形的示意见图1 。

定义 5.9（量子交互式证明系统）。设 $m \in \mathbb{Z}_+$ 为消息总数，并设 $h = \lfloor m/2 + 1 \rfloor$。一个具有 m 条消息的量子交互式预言机证明系统由一组带查询的量子算法组成，其形式为 $V = (V_1, V_2, \ldots, V_h)$。元组 $\mathbb{V}_x = (\mathbb{V}_{x,1}, \ldots, \mathbb{V}_{x,h})$ 表示算法 V_i 在输入 x 上生成的带查询的量子信道。每个量子信道 $\mathbb{V}_{x,i}$（$i \in [h]$）作用于（量子）见证寄存器 (W_{i-1}, W'_{i-1}) 和（量子）参考寄存器

R，并返回一个消息寄存器 （J_i、M_i），其中 J_i 是经典的，而 M_i 是量子的，同时还返回私有寄存器 （W'_i、R）。[6] 总而言之，验证者信道 $\mathbb{V}_x$、i 对寄存器的作用如下：

$$\big((\mathsf{W}_{i-1},\mathsf{W}'_{i-1}),\mathsf{R}\big)\longrightarrow\big((\mathsf{M}_i,\mathsf{J}_i),(\mathsf{W}'_i,\mathsf{R})\big)\,.$$

若 m 为奇数，定义索引集合 $I=\{0,\ldots,h-1\}$；若 m 为偶数，则令 $I=\{1,\ldots,h-1\}$。证明者策略由一组量子信道 $\{\mathbb{P}_i\}_{i\in I}$ 和量子寄存器 P 指定，其中每个 $\mathbb{P}_i$ 按如下方式作用于这些寄存器：

$$((\mathsf{M}_i,\mathsf{J}_i),\mathsf{P})\longrightarrow(\mathsf{W}_i,\mathsf{P}).$$

将寄存器 J_h 在 $\mathbb{V}_{x,h}$ 的输出中的第一个（经典）比特视为验证者的最终判定，即接受或拒绝。令 $\omega(\mathbb{V}_x)$ 表示由 $\mathbb{V}_x$ 定义的交互式博弈的值。也就是说，$\omega(\mathbb{V}_x)$ 是 $\mathbb{V}_x$ 在所有可能的证明者策略 $\{\mathbb{P}_i\}_{i\in I}$ 中的最大接受概率。

必须满足以下性质：

- 一致性： 除非另有说明，否则我们将W_i、W'_i、R、M_i 初始化为 $|0\rangle$，而P可以初始化为任意量子态。寄存器J_i 初始化为全零字符串。
- 高效性： 每个验证者算法 V_i 都必须能够在多项式时间内实现，并具有定义 5.4 中所定义的多项式时间复杂度。

在下一个定义中，我们给出量子交互式预言机证明的一般模型。在该模型中，验证者可以生成任意量子态并发送给证明者，而不局限于只发送来自证明者消息的寄存器。在此定义中，我们用 $\mathbf{M}'_i$ 表示验证者在第 i 轮生成的消息寄存器。验证者在第 i 轮的完整消息寄存器（记为 $\mathbf{M}_i$）包含 $\mathbf{M}'_i$ 以及在当前轮和前几轮中从证明者处接收的一些寄存器。

在后面的章节中，我们会给出一个相对“简单”的一般量子交互式预言机证明构造，以说明此定义可能过于宽松，无法导出有意义或有趣的结果。因此，我们随后引入一个限制更严格的定义，要求 $\mathbf{M}'_i$寄存器是平凡的。

定义 5.10 (一般量子交互式预言机证明系统)。 设 $m\in\mathbb{Z}_+$。一个 m-消息一般量子交互式预言机证明系统由一个 m-消息量子交互式证明系统 V 构成，其满足与定义 5.9相同的结构，但寄存器结构作如下修改。

与之前一样，在第 i 轮，对于 $i\in[h]$ 其中 $h=\lfloor m/2+1\rfloor$，验证者从证明者处接收量子消息寄存器 W_{i-1} 。此外，验证者还持有一个寄存器W'_{i-1} ，用于存储证明者先前接收的消息（的一部分），以及一个寄存器 R ，作为其私有（参考）寄存器。寄存器 W'_{i-1} 分解为

$$\mathsf{W}'_{i-1}=(\mathsf{W}'_{0,i-1},\mathsf{W}'_{1,i-1},\ldots,\mathsf{W}'_{i-2,i-1})\,,$$

其中，$\mathsf{W}'_{j,i-1}$ 表示证明者第 j 条消息（即 $\mathsf{W}j$）中迄今尚未发回给证明者的部分。

对于每个 $\mathsf{W}'_{j,\,i-1}$，验证者在第 i 轮向证明者发送一个子寄存器 $\mathsf{N}_{j,\,i}$ ，并将剩余部分保留为 $\mathsf{W}'_{j,\,i}$。此外，验证者还生成一个量子消息寄存器 M'_i 以及

[6]对于当前定义而言，不需要寄存器 W'_i ，不失一般性地可假设它们是平凡的。我们保留这些寄存器是为了将来的一致性。

一个经典消息寄存器 J_i 。验证者将完整的消息寄存器 $(\mathsf{M}_i,\mathsf{J}_i)$ 发回给证明者，其中

$$\mathsf{M}_i = (\mathsf{M}'_i, (\mathsf{N}_{0,i}, \mathsf{N}_{1,i}, \ldots, \mathsf{N}_{i-1,i})).$$

最后，我们定义该协议的以下资源界：

- 证明长度：验证者 V 的证明长度为 l： $\mathbb{Z}_+ \to \mathbb{Z}_+$，如果

$$l(n) \geq \sum_{i\in[n]} l_i(n),$$

其中 $l_i(n)$ 是 V_i的证明长度。

- 查询复杂度：验证者 V 的查询复杂度为 q： $\mathbb{Z}_+ \to \mathbb{Z}_+$，如果

$$q(n) \geq \sum_{i\in[n]} q_i(n),$$

其中 $q_i(n)$ 是 V_i的查询复杂度。

备注 5.11。 由于 $\mathbb{V}_{x,\ i}$ 具有见证寄存器 W_{i-1},W'_{i-1}，因此，$\mathbb{V}_{x,\ i}$ 中的门所触及的任何量子寄存器都会计入查询复杂度。

定义 5.12（受限量子交互式预言机证明系统）。 一个包含 m 条消息的受限量子交互式预言机证明系统由一个包含 m 条消息的一般量子交互式预言机证明系统组成，并满足：对于每个 i，M'_i 都是平凡量子寄存器。

定义 5.13（强量子交互式预言机证明系统）。 一个 m条消息的强量子交互式预言机证明系统由一个 m条消息的量子交互式预言机证明系统组成，并满足（使用定义 *5.9* 和定义 *5.12*中的记号）：对于每个 $i \in [h]$，M'_i 是平凡的（验证者不发送新的量子消息），且 $\mathsf{N}_{i-1,\ i}$ =W_{i-1} （所有证明者的量子消息都发回给证明者）。因此，M_i =W_{i-1}，W'_{i-1} 始终是平凡的，并且 $\mathbb{V}_{x,\ i}$仅具有见证寄存器W_{i-1} 。

定义 5.14（针对承诺问题的量子交互式预言机证明系统）。 设 $m \in \mathbb{Z}_+$为消息总数。一个针对承诺问题 m条消息的受限量子交互式预言机证明系统（分别为一般量子交互式预言机证明系统、强量子交互式预言机证明系统）（S_{yes}、 S_{no}）满足以下条件，其中 ω（$\mathbb{V}_x$）按定义 *5.12* （分别按定义 *5.10*、定义 *5.13*）定义。

- 完备性：存在一个常数 $c \in (0, 1]$，使得对所有 $x \in S_{yes}$，最大接受概率 $\omega(\mathbb{V}_x) \geq c$。也就是说，存在一种诚实证明者策略，使验证者以至少 c 的概率接受每个是实例。

- 可靠性：存在一个常数 $s \in [0, c)$，使得对所有 $x \in S_{no}$，最大接受概率 $\omega(\mathbb{V}_x) \leq s$。也就是说，任何证明者策略都无法使验证者以大于 s 的概率接受否实例。

我们定义三类量子交互式预言机证明系统。类 $\mathcal{QIOP}(r,\ l,\ q)$ 由所有满足以下条件的承诺问题构成：它们存在一种 r-消息受限量子交互式预言机证明（qIOP）系统，其证明长度上界为 l (n)，查询复杂度上界为 $q(n)$。这里，查询复杂度表示验证者在所有轮次中访问证明者消息内量子比特的总数。

定义 5.15（量子交互式预言机证明）。设 r, l, q： $\mathbb{Z}_+ \to \mathbb{Z}_+$。令 $\mathcal{QIOP}(r, l, q)$（分别为 $\mathcal{GQIOP}(r, l, q)$、$\mathcal{SQIOP}(r, l, q)$）表示满足以下条件的承诺问题(S_{yes}, S_{no})：它具有一种 r-消息受限（分别为一般、强）量子交互式预言机证明系统，其证明长度为l，查询复杂度为 q。

这些模型均假设验证者为多项式时间，并允许量子证明者拥有不受计算能力限制。交互轮数上限为 $r(n)$，且始终取为常数。这些复杂度类有助于刻画验证者可以访问或处理多少量子信息。

6 具有共享 EPR 对和经典通信的量子交互式预言机证明

在我们的第一个构造中，验证者制备 EPR 对，并将每对中的一半发送给证明者，从而建立共享纠缠。

本节将着手证明以下定理。

定理 6.1。QMA $\subseteq \mathcal{GQIOP}(O(1), \text{poly } O(1)$。

6.1 交互式预言机证明模型中的承诺

在交互式预言机证明情形中，验证者利用证明者的计算能力来计算输入的某些函数。在我们所讨论的特定情形中，证明者持有一个验证者无法直接访问的字符串，而验证者持有一个证明者并不知道的电路。该字符串与电路的组合决定输入是否属于该语言。显而易见的解决方案存在问题：如果验证者只是将电路发送给证明者，证明者就可以在另一个输入上计算，而不是在最初给定的输入上计算，从而作弊。交互式预言机承诺提供了一种解决方案，允许证明者在开始时承诺其输入。之后，验证者发送电路，而该承诺确保证明者在已承诺的输入上诚实地进行计算。

在以下定义中，第一个要求确保交互采用交互式预言机的形式，而第二个要求证明者能够承诺任意字符串并执行任意计算。（请注意，以下定义针对经典情形。）

定义6.2 (交互式预言机承诺**)**。交互式预言机承诺方案由一个经典概率多项式时间交互机 V 和一个函数 D： $\mathbb{F}_2^* \to \mathbb{F}_2^*$ 组成，满足以下条件：

1. 验证者的查询复杂度是一个常数。

2. 存在一个诚实多项式时间证明者 P，使得对于任意 n、任意 $s \in \mathbb{F}_2^n$、任意大小为 $\text{poly}(n)$ 且输出为单比特的电路 C，以及任意 $\varepsilon \in (0,1)$，在 $P(s)$ 与 $V(C, \varepsilon)$ 交互结束时，验证者以概率 1 输出 $C(s)$。此外，P 与 V 之间的通信复杂度为$\text{poly}(n)$。

3. 可靠性：对于任何具有单比特输出的多项式规模电路 C、任何 $\varepsilon \in (0,1)$，以及任何证明者 P，令 m 为交互结束时证明者的第一条消息，

$$\Pr[V(C, \varepsilon) \text{ outputs } C(D(m)) \text{ or rejects}] \geq 1 - \varepsilon .$$

注记 6.3。对于诚实证明者，第一条消息 m是承诺，并满足 $D(m) = s$。此外， $Im(D) = \mathbb{F}_2^*$。

我们将使用针对 Circuit Value 问题的邻近性概率可检验证明（PCPP）以及具有多项式码率、常数相对距离和高效编码与解码的纠错码族，构造一个交互式预言机承诺（IOC）协议。

首先，我们回顾一个关于纠错码存在性的基本结果。这些码构成了我们协议中证明者承诺的基础。

定义 6.4（纠错码的码字测试器）。设 $C \subseteq \mathbb{F}_2^n$ 为二进制纠错码。针对 C 的确定性测试器 是一个经典算法 T： $\mathbb{F}_2^n \to \{0,1\}$，满足

$$T(x) = \begin{cases} 1 & if\ x \in C, \\ 0 & otherwise. \end{cases}$$

也就是说，当且仅当一个字符串是 C中的有效码字时， T 才接受该字符串。

定理 6.5（纠错码， [SS96]）。存在具有多项式码率、常数相对距离以及确定性多项式时间编码与解码算法的线性纠错码族，同时还存在一个用于检查码字归属的确定性多项式时间测试器。

现在我们来描述交互式预言机承诺协议中证明者的结构。证明者使用其消息的码字编码来承诺一个值，随后通过与验证者交互来证明该值的一致性。

定义 6.6（交互式预言机承诺协议中证明者的构造）。

- 证明者的第一步：证明者向验证者发送一个字符串 $E(s)$，其中 E 是定理 *6.5* 中所述码的编码函数。
- 验证者的第一步：验证者向证明者发送一个布尔电路 C 的描述。
- 证明者的第二步：证明者以字符串 $C(s) \circ w$作出回应，其中 w 是一个见证，使得定理 *4.14* 中的验证者在以输入 $E(s) \circ w$ 调用时，接受预言机 $x = C(D(\cdot)) + C(s) + 1$。
- 验证者的第二步：验证者决定是否接受；如果接受，则产生一个输出。

接下来，我们描述交互式预言机承诺协议中验证者的行为。验证者使用 PCPP 验证器检查证明者的消息与某个码字的接近程度，并验证所声称的输出是否正确。

定义 6.7（交互式预言机承诺协议中验证者的构造）。

- 证明者的第一步：证明者向验证者发送一个字符串 m。
- 验证者的第一步：验证者向证明者发送一个布尔电路 C 的描述。
- 证明者的第二步：证明者向验证者发送字符串 $r \circ w$。

- 验证者的第二步：验证者接受并输出 r 当且仅当定理*4.14*中的验证者运行固定次数时，每次对输入

$$x = \big(C(D(\cdot)) + r + 1\big) \wedge T(\cdot),$$

带有隐式输入 $y = m$ 和证明 $\pi = w$，其中 D 是解码电路，而 T 是定理*6.5*中的码测试器

以下引理指出，上述定义的协议满足交互式预言机承诺的要求。具体而言，验证者满足完备性和可靠性要求。

引理 6.8。定义*6.7* 中描述的验证者满足交互式预言机承诺的要求。

证明。根据定义6.7、定理6.5和定理4.14，验证者的查询复杂度为常数。

完备性：根据定理6.5 和定理4.14，如果证明者是诚实的，并提供有效编码和见证，验证者将以概率 1 接受。此外，证明者与验证者之间的通信复杂度关于输入规模是多项式的。

可靠性：设 $S = \{t \mid C(D(t)) = r \wedge T(t) = 1\}$。如果 $\mathsf{dist}(m, S) > \delta$，那么 $\Pr[\mathtt{V}(C, \varepsilon)$ 接受$] \leq \varepsilon$，因此，

$$\Pr[\mathtt{V}(C, \varepsilon) \text{ either outputs } C(D(m)) \text{ or rejects}] \geq 1 - \varepsilon.$$

如果 $\mathsf{dist}(m, S) \leq \delta$，那么存在 s，使得 $C(s) = r$，且 $\mathsf{dist}(m, E(s)) \leq \delta$。因此，$D(m) = s$，且 $C(D(m)) = r$，验证者将要么接受并给出正确输出，要么拒绝。因此，

$$\Pr[\text{the verifier } \mathtt{V}(C, \varepsilon) \text{ either outputs } C(D(m)) \text{ or rejects}] = 1.$$

□

6.2 使用共享 EPR 对的量子交互式预言机证明

定理 6.9 (定理 6.1的重述)。 $\mathsf{QMA} \subseteq \mathcal{GQIOP}(3,$多项式 $O(1))$。

我们先定义定理 6.1证明中使用的验证者和证明者。随后，我们将着手证明该定理。

一种简单的方法是让证明者将见证的 N 个副本量子隐形传态给验证者，同时发送量子隐形传态所需的相应一次性密码本。然后，验证者测量其持有的 EPR 对的一半，利用收到的一次性密码本进行相应的校正，并根据测量结果决定是否接受。请注意，验证者持有的 EPR 对的另一半存储在私有寄存器中，因此不会增加查询复杂度。

在接下来的构造中，证明者和验证者遵循一个受这一朴素方法启发的协议。然而，证明者不直接传输一次性密码本，而是使用承诺方案对其进行承诺。随后，验证者利用其提取承诺值函数的能力，恢复校正测量结果所需的信息。

在协议开始时，验证者持有寄存器 R′，证明者持有寄存器 R，使得 RR′ 上的联合量子态由共享 EPR 对组成。

定义 *6.10*（定理 *6.1* 的诚实证明者策略）。设 p、q 如定理 *4.10* 中所述，且设 s、N 如引理 *4.11* 中所述。设 $H = \frac{1}{m}\sum_{i\in[m]} H_i \in \mathbb{C}^{2^n} \otimes \mathbb{C}^{2^n}$ 为一个 *5*-局部克利福德哈密顿量，满足 $m =$*poly*(n)，且满足以下条件之一：$\lambda_{\min}(H) \leq 2^{-p(n)}$ 或 $\lambda_{\min}(H) \geq 1/q(n)$。

令 RR' 为初始化为最大纠缠态的量子寄存器：

$$\frac{1}{\sqrt{2^{nN}}}\sum_{i=0}^{2^{nN}-1}|i\rangle_{\mathsf{R}}|i\rangle_{\mathsf{R}'}\ .$$

- 证明者持有寄存器 $\mathsf{W}_i=(\mathsf{W}_{i,1},\mathsf{W}_{i,2},\ldots,\mathsf{W}_{i,n})$，用于 $i\in[N]$。令 $|\varphi\rangle$ 为 $1-2H$最大特征值对应的本征态。证明者制备 N 份 $|\varphi\rangle$，并将它们存储在寄存器 W_i中。

- 对于每个 $i\in[N]$ 和 $j\in[n]$，证明者在 *EPR*基中测量联合系统 $\mathsf{W}_{i,j}\mathsf{R}_{(i-1)*n+j}$，如定义 *4.3*中所定义，并将测量结果存储在 $(s_{0,i,j},s_{1,i,j})$中。
- 令

$$s=(s_{k,i,j})_{(k,i,j)\in\{0,1\}\times[N]\times[n]}\ .$$

随后，证明者使用 作为输入，参与定义 *6.2*中所述的交互式预言机承诺协议。

定义 6.11 (定理6.1的验证者策略)。 在与定义 *6.10*相同的设置假设下，验证者执行以下操作：

- 对于每个 $i\in[N]$，验证者独立且均匀地随机采样 $l_i\in[m]$。
- 对于每个 $i\in[m]$，令 $H_i=\left(C_i^{\dagger}\left(|0\rangle\langle 0|\right)^{\otimes 5}C_i\right)\otimes I$。对于 $j\in[5]$，定义

$$O_{i,j}=\left(C_i^{\dagger}\cdot(I^{\otimes j-1}\otimes Z\otimes I^{\otimes(5-j)})\cdot C_i\right)\otimes I,$$

并令

$$O_{i,j}=(-1)^{d_{i,j}}X(a_{i,j})Z(b_{i,j})Y(c_{i,j})$$

为其在引理 *6.13*中的泡利表示。

- 对于每个 $i\in[N]$，验证者测量寄存器

$$\mathsf{R}'_i=(\mathsf{R}'_{(i-1)*n+1},\ldots,\mathsf{R}'_{(i-1)*n+n})$$

使用 *th* 可观测量 $O_{l_i,\ j}$ 从 $j=1$ 到 5，并将测量结果存储在 $r_{i,\ j}$.

- 验证者构造布尔电路：

$$C(x)=\bigoplus_{i\in[N]}\left(1\oplus\bigvee_{j\in[5]}\left(r_{l_i,j}\oplus a_{l_i,j}x_{0,i}\oplus b_{l_i,j}x_{1,i}\oplus c_{l_i,j}x_{1,i}\oplus c_{l_i,j}x_{0,i}\right)\right),$$

其中 $x=(x_{k,\ i,\ j})_{k\in\{0,1\},\ i\in[N],\ j\in[n]}$。

- 验证者使用定义*6.2* 中的交互式预言机承诺协议，所用电路为C，并且 $\varepsilon=0.001$。

- 当且仅当交互式预言机承诺协议接受且其输出为0时，验证者接受。

注释 6.12。 请注意，在我们的构造中，验证者在第一轮发送 *EPR* 对的一半后，所有剩余通信都是经典的。如果我们改为假设验证者和证明者在开始时就共享 *EPR* 对，那么该协议将完全是经典的。

定理 *6.1* 的证明。 设 V 为定义 6.11中的验证者。我们将证明 V 是一个具有 Nn-共享 EPR 对的三消息非自适应量子经典交互式预言机证明系统，参数为$\mathcal{LCH}(5, 2^{-p(n)}, 1/q(n))$，因此

$$\mathcal{LCH}(5, 2^{-p(n)}, 1/q(n)) \in \mathsf{GQIOP}(3, \mathrm{poly}, O(1), \mathrm{poly}).$$

根据定理4.10， $\mathcal{LCH}(5, 2^{-p(n)}, 1/q(n))$ 是QMA-完全的。因此，

$$\mathsf{QMA} \subseteq \mathsf{GQIOP}(3, \mathrm{poly}, O(1), \mathrm{poly}) .$$

根据定义6.10、定义6.11和定义5.12， V 是一致的，具有多项式时间复杂度，具有高效性，证明长度为 $\mathrm{poly}(n)$，查询复杂度为 $O(1)$。此外，完备性和可靠性性质如下。

完备性： 令r'_i 为在$1-2H_{l_i}$下测量 $|\varphi\rangle$所得分布对应的随机变量。通过量子隐形传态，在收到 s_0， s_1后，验证者的状态为$X(s_1)Z(s_0)\,|\varphi\rangle^{\otimes N}$。根据引理6.16、定义6.10和定义6.11，给定 l_1， l_2， $\cdots$， l_N， s_0， s_1，

$$\Pr\left[C((s_0,s_1)) = 0 \mid l_1, l_2, \cdots, l_N, s_0, s_1\right] = \Pr\left[\bigoplus_{i\in[N]} r'_i = 0\right] . \tag{1}$$

因此，根据引理6.17，我们可以得出

$$\begin{aligned}
\omega(V) =\ & \Pr[\text{Verifier accepts}] \\
=\ & \sum_{l_1,l_2,\cdots,l_N\in[m]} \Pr[l_1,l_2,\cdots,l_N]\cdot\Pr[\text{Verifier accepts} \mid l_1,l_2,\cdots,l_N] \\
=\ & \sum_{l_1,l_2,\cdots,l_N\in[m],s_0,s_1\in\mathbb{F}_2^{Nn}} \frac{1}{m^N}\Pr[s_0,s_1]\cdot\Pr[\text{Verifier accepts} \mid l_1,l_2,\cdots,l_N,s_0,s_1] \\
=\ & \sum_{l_1,l_2,\cdots,l_N\in[m],s_0,s_1\in\mathbb{F}_2^{Nn}} \frac{1}{m^N}\cdot(\frac{1}{2^{Nn}})^2\cdot\Pr[C((s_0,s_1))=0 \mid l_1,l_2,\cdots,l_N,s_0,s_1] \\
=\ & \sum_{l_1,l_2,\cdots,l_N\in[m]} \frac{1}{m^N}\cdot\Pr[\bigoplus_{i\in[N]} r'_i = 0] \\
=\ & \sum_{l_1,l_2,\cdots,l_N\in[m]} \frac{1}{m^N}\cdot\Pr[\text{The outcome of measuring } |\varphi\rangle^{\otimes N} \text{ under } \bigotimes_{i\in[N]}(1-2H_{l_i}) \text{ is } 0] \\
=\ & \sum_{l_1,l_2,\cdots,l_N\in[m]} \frac{1}{m^N}\cdot\langle\varphi|^{\otimes N}\,\frac{I+\bigotimes_{i\in[N]}(1-2H_{l_i})}{2}\,|\varphi\rangle^{\otimes N} \\
=\ & \langle\varphi|^{\otimes N}\,\frac{I+(1-2H)^{\otimes N}}{2}\,|\varphi\rangle^{\otimes N} \\
=\ & \frac{1}{2}+\frac{(\langle\varphi|\,(1-2H)\,|\varphi\rangle)^N}{2} \\
\geq\ & 1-\Theta(2^{-s(n)}) ,
\end{aligned}$$

其中，第四步由交互式预言机承诺的完备性得出。

可靠性： 设证明者在交互式预言机承诺中发送的第一条消息为M，并设 $(s_0,\ s_1)$ 满足 $D(M) = (s_0, s_1)$。不失一般性，整个量子

态在证明者发送该消息之后为

$$\frac{1}{\sqrt{2^{nN}}}\sum_{i=0}^{2^{nN}-1}\left(UP_M\left|0\right\rangle_{\mathsf{W}}\left|i\right\rangle_{\mathsf{R}}\right)\left|i\right\rangle_{\mathsf{R}'},$$

其中 W 是任意寄存器，U 是作用于 WR 上的任意酉算子，且 $\{P_M\}_{M\in\mathbb{F}_2^h}$ 是作用于 WR 上的任意正交投影测量，其中 $h=|E(1^{2Nn})|$ 是定理 6.5 中各码的编码电路的输出长度。

对于 $i\in[N]$，定义一个正交投影

$$Q_i^{(1)}=C_{l_i}^{\dagger}\bigotimes_{j\in[5]}\frac{I+(-1)^{a_{l_i,j}s_{0,i}+b_{l_i,j}s_{1,i}+c_{l_i,j}(s_{0,i}+s_{1,i})}Z}{2}C_{l_i},\qquad Q_i^{(0)}=I-Q_i^{(1)}.$$

注意到

$$X(s_1)Z(s_0)Q_i^{(j)}=\left(\frac{1}{2}+(-1)^j\left(\frac{1}{2}-H_{l_i}\right)\right)X(s_1)Z(s_0).$$

验证者接受的概率可如下界定：

$$\begin{aligned}\omega(V)=&\ \Pr[\text{Verifier accepts}]\\=&\sum_{l_1,l_2,\cdots,l_N\in[m]}\Pr[l_1,l_2,\cdots,l_N]\cdot\Pr[\text{Verifier accepts}\mid l_1,l_2,\cdots,l_N]\\=&\sum_{l_1,l_2,\cdots,l_N\in[m],M\in\mathbb{F}_2^h}\frac{1}{m^N}\Pr[M]\cdot\Pr[\text{Verifier accepts}\mid l_1,l_2,\cdots,l_N,M].\end{aligned}$$

根据交互式预言机承诺的可靠性，

Pr[交互式预言机承诺中的验证者要么输出 $C(s_0,\ s_1)$，要么拒绝] $\geq 1-\varepsilon$.因此，

$$\begin{aligned}&\Pr[\text{Verifier accepts}\mid l_1,l_2,\cdots,l_N,M]\\&=\Pr[\text{Verifier in interactive oracle commitment accepts and outputs }0\mid l_1,l_2,\cdots,l_N,M]\\&\leq\max\left\{\Pr[C(s_0,s_1)=0\mid l_1,l_2,\cdots,l_N,M]\ ,\ \varepsilon\right\}.\end{aligned}$$

Let

$$r_i=1\oplus\bigvee_{j\in[5]}\left(r_{l_i,j}\oplus a_{l_i,j}s_{0,i}\oplus b_{l_i,j}s_{1,i}\oplus c_{l_i,j}s_{1,i}\oplus c_{l_i,j}s_{0,i}\right).$$

那么，

$$\Pr[C(s_0,s_1)=0\mid l_1,l_2,\cdots,l_N,M]=\sum_{\oplus_{i\in[N]}r_i=0}\Pr[r_1,r_2,\cdots,r_N\mid l_1,l_2,\cdots,l_N,M].$$

此外，我们有

$$\begin{aligned}&\Pr[r_1,r_2,\cdots,r_N\mid l_1,l_2,\cdots,l_N,M]\cdot\Pr[M]\\=&\frac{1}{2^{nN}}\left\|\sum_{i=0}^{2^{nN}-1}\left(UP_M\left|0\right\rangle_{\mathsf{W}}\left|i\right\rangle_{\mathsf{R}}\right)\prod_{j=1}^{N}Q_j^{(r_j)}\left|i\right\rangle_{\mathsf{R}'}\right\|^2\end{aligned}$$

$$= \frac{1}{2^{nN}} \Big\| \sum_{i=0}^{2^{nN}-1} (UP_M |0\rangle_{\mathsf{W}} |i\rangle_{\mathsf{R}})(X(s_1)Z(s_0))_{\mathsf{R}'} \prod_{j=1}^{N} Q_j^{(r_j)} |i\rangle_{\mathsf{R}'} \Big\|^2$$

$$= \frac{1}{2^{nN}} \Big\| \sum_{i=0}^{2^{nN}-1} (UP_M |0\rangle_{\mathsf{W}} |i\rangle_{\mathsf{R}}) \prod_{j=1}^{N} (\frac{1}{2} + (-1)^{r_j}(\frac{1}{2} - H_{l_j}))X(s_1)Z(s_0) |i\rangle_{\mathsf{R}'} \Big\|^2.$$

我们用 ρ 表示

$$\frac{1}{2^{nN}} \sum_{M\in\mathbb{F}_2^h} \sum_{i=0}^{2^{nN}-1} (UP_M |0\rangle_{\mathsf{W}} |i\rangle_{\mathsf{R}})X(s_1)Z(s_0) |i\rangle_{\mathsf{R}'} \sum_{l=0}^{2^{nN}-1} (\langle 0|_{\mathsf{W}} \langle l|_{\mathsf{R}} P_M U^\dagger) \langle l|_{\mathsf{R}'} X(s_1)Z(s_0).$$

注意,

$$\begin{aligned}
\mathrm{tr}(\rho) &= \frac{1}{2^{nN}} \sum_M \mathrm{tr}\Big(\sum_{i=0}^{2^{nN}-1} (\langle 0|_{\mathsf{W}} \langle i|_{\mathsf{R}} P_M |0\rangle_{\mathsf{W}} |i\rangle_{\mathsf{R}}) \Big) \\
&= \frac{1}{2^{nN}} \mathrm{tr}\Big(\sum_{i=0}^{2^{nN}-1} (\langle 0|_{\mathsf{W}} \langle i|_{\mathsf{R}} I |0\rangle_{\mathsf{W}} |i\rangle_{\mathsf{R}}) \Big) \\
&= 1.
\end{aligned}$$

由于 ρ 是一个量子态,

$$\begin{aligned}
\omega(V) &\le \varepsilon + \sum_{l_1,l_2,\cdots,l_N\in[m],M\in\mathbb{F}_2^h} \frac{1}{m^N} \Pr[M] \cdot \sum_{\oplus_{i\in[N]} r_i = 0} \Pr[r_1, r_2, \cdots, r_N \mid l_1, l_2, \cdots, l_N, M] \\
&= \varepsilon + \sum_{l_1,l_2,\cdots,l_N\in[m],\oplus_{i\in[N]} r_i = 0} \frac{1}{m^N} \mathrm{tr}[\prod_{j=1}^{N} (\frac{1}{2} + (-1)^{r_j}(\frac{1}{2} - H_{l_j}))\rho] \\
&= \varepsilon + \sum_{l_1,l_2,\cdots,l_N\in[m]} \frac{1}{m^N} \mathrm{tr}[\frac{I + \otimes_{i\in[N]}(1-2H_{l_i})}{2}\rho] \\
&= \varepsilon + \mathrm{tr}[\frac{I + (1-2H)^{\otimes N}}{2}\rho] \\
&\le \frac{1}{2} + \varepsilon + \frac{1}{2} \cdot 2^{-s(n)}.
\end{aligned}$$

□

6.3 技术性论断

引理 6.13。 对于任意 $k \in \mathbb{Z}_+$ 以及 k 重克利福德群 C 中的任意元素，都存在 $a, b, c \in \mathbb{F}_2^k, d \in \mathbb{F}_2$, 使得

$$C^\dagger (Z \otimes \underbrace{I \otimes I \otimes \cdots \otimes I}_{k-1}) C = (-1)^d X(a)Z(b)Y(c) \tag{2}$$

和 $a \wedge b = b \wedge c = c \wedge a = 0$。我们称$(-1)^d X(a)Z(b)Y(c)$ 为 $C^\dagger (Z \otimes \underbrace{I \otimes I \otimes \cdots \otimes I}_{k-1}) C$的泡利表示。

证明。由于$Z\otimes I\otimes \underbrace{I\otimes\cdots\otimes I}_{k-1}$是 k重泡利群的一个元素，而 C 是k k重克利福德群的一个元素，因此 $C^\dagger(Z\otimes I\otimes I\otimes\cdots\otimes I)C$是 k重泡利群的一个元素。设

$$C^\dagger(Z\otimes \underbrace{I\otimes I\otimes\cdots\otimes I}_{k-1})C=(-1)^d\mathbf{i}^e X(a)Z(b)Y(c)$$

其中 $a,\ b,\ c\in\mathbb{F}_2^k,\ d,\ e\in\mathbb{F}_2$ 以及 $a\wedge b=b\wedge c=c\wedge a=0$。

因为

$$\begin{aligned}(-1)^d\mathbf{i}^e X(a)Z(b)Y(c)&=C^\dagger(Z\otimes \underbrace{I\otimes I\otimes\cdots\otimes I}_{k-1})C\\&=(C^\dagger(Z\otimes \underbrace{I\otimes I\otimes\cdots\otimes I}_{k-1})C)^\dagger\\&=((-1)^d\mathbf{i}^e X(a)Z(b)Y(c))^\dagger,\end{aligned}$$

因此 $e=0$。 □

引理 6.14。 设 A、B 为矩阵。对于 $x\in\mathbb{F}_2$、 $\frac{I+(-1)^x A}{2}B=B\frac{I+(-1)^{x+1}A}{2}$若 $\{A,B\}=0$、$\frac{I+(-1)^x A}{2}B=B\frac{I+(-1)^x A}{2}$若 $[A,B]=0$。

证明。 **第 1 部分：** 因为 $AB=-BA$,

$$\frac{I+(-1)^x A}{2}B=B\frac{I+(-1)^{x+1}A}{2}.$$

第 2 部分： 因为 $AB=BA$,

$$\frac{I+(-1)^x A}{2}B=B\frac{I+(-1)^x A}{2}.$$

□

引理 6.15。 对于任意满足 $O_i^2=I$ 的可观测量 O_i，

$$\frac{I+\bigotimes_{i\in[N]}O_i}{2}=\sum_{\bigoplus_{i\in[N]}r_i=0}\bigotimes_{i\in[N]}\frac{(I+(-1)^{r_i}O_i)}{2}$$

证明。 该引理由此得出

$$\sum_{\bigoplus_{i\in[N]}r_i=0}\bigotimes_{i\in[N]}\frac{(I+(-1)^{r_i}O_i)}{2}+\sum_{\bigoplus_{i\in[N]}r_i=1}\bigotimes_{i\in[N]}\frac{(I+(-1)^{r_i}O_i)}{2}=I.$$

and

$$\sum_{\bigoplus_{i\in[N]}r_i=0}\bigotimes_{i\in[N]}\frac{(I+(-1)^{r_i}O_i)}{2}-\sum_{\bigoplus_{i\in[N]}r_i=1}\bigotimes_{i\in[N]}\frac{(I+(-1)^{r_i}O_i)}{2}=\bigotimes_{i\in[N]}O_i.$$

□

引理 6.16。 设 C 是5重克利福德群中的一个元素。设 $|\varphi\rangle$ 是一个量子态。设r' 是按照 $1-2C^\dagger(|0\rangle\langle 0|)^{\otimes 5}C$对 $|\varphi\rangle$ 进行测量所得分布对应的随机变量。设

$$O_j = (C^\dagger \underbrace{I\otimes I\cdots\otimes I}_{j-1}\otimes Z\otimes \underbrace{I\otimes I\cdots\otimes I}_{5-j} C)\otimes I,$$

并令

$$O_j = (-1)^{d_j} X(a_j)Z(b_j)Y(c_j)$$

为 O_j在引理 6.13中定义的泡利表示。令 $s_0,\ s_1 \in_R \mathbb{F}_2^n$。令 $(r_1,\ r_2,\ \cdots,\ r_5)$ 为随机变量，其分布与在 O_j 下，将 $j=1$ 至 $j=5$ 依次进行测量时，对 $Z(s_0)X(s_1)|\varphi\rangle$所得的测量结果的分布相同。令 $r = 1\oplus \bigvee_{j\in[5]}($ $r_j\oplus a_j s_0\oplus b_j s_1\oplus c_j s_1\oplus c_j s_0)$。

那么，随机变量 r 和 r' 具有相同分布。

证明。 r' 的分布可表示为 $\Pr[r'=1] = \langle\varphi|H|\varphi\rangle$。

令 $r''_j = a_j s_0\oplus b_j s_1\oplus c_j s_1\oplus c_j s_0$。由于 $r = 1\oplus\bigvee_{j\in[5]}(r_j\oplus r''_j)$，$r$ 的分布可表示为

$$\Pr[r=1] = \|\prod_{j=1}^{5}\frac{I+(-1)^{r''_j}O_{6-j}}{2}\cdot X(s_1)Z(s_0)|\varphi\rangle\|^2.$$

注意到 $O_j = (-1)^{d_j}X(a_j)Z(b_j)Y(c_j)$，由引理 6.14，可得对于 $j\in[m]$,

$$\frac{I+(-1)^{r''_j}O_j}{2}\cdot X(s_1)Z(s_0) = X(s_1)Z(s_0)\cdot\frac{I+O_j}{2}$$

因此,

$$\begin{aligned}
\Pr[r=1] &= \|\prod_{j=1}^{5}\frac{I+(-1)^{r''_j}O_{6-j}}{2}\cdot X(s_1)Z(s_0)|\varphi\rangle\|^2\\
&= \|X(s_1)Z(s_0)\prod_{j=1}^{5}\frac{I+O_{6-j}}{2}\cdot|\varphi\rangle\|^2\\
&= \|\prod_{j=1}^{5}\frac{I+O_{6-j}}{2}\cdot|\varphi\rangle\|^2\\
&= \langle\varphi|\prod_{j=1}^{5}C^\dagger\underbrace{I\otimes I\cdots\otimes I}_{5-j}\otimes Z^+\otimes\underbrace{I\otimes I\cdots\otimes I}_{j-1}C|\varphi\rangle\\
&= \langle\varphi|H|\varphi\rangle.
\end{aligned}$$

□

引理 6.17。 设 O_i 对于 $i\in[m]$ 是可观测量。设 $H = \frac{1}{m}\sum_{i\in[m]}O_i$。设 $|\varphi\rangle$ 是一个量子态。设 $l_i\in[m]$ 对于 $i\in[N]$。设 r'_i 是一个随机变量，其分布与在 O_{l_i} 下测量 $|\varphi\rangle$ 所得的分布相同。那么，

$$\Pr[\bigoplus_{i\in[N]} r'_i = 0] = \Pr[\textit{The outcome of measuring } |\varphi\rangle^{\otimes N} \textit{ under } \bigotimes_{i\in[N]} O_{l_i} \textit{ is } 0] \tag{3}$$

证明。 这是因为

$$\Pr[\bigoplus_{i\in[N]} r'_i = 0] = \sum_{\bigoplus_{i\in[N]} r'_i=0} \prod_{i\in[N]} \langle\varphi| \frac{(I+(-1)^{r'_i}O_{l_i})}{2} |\varphi\rangle ,$$

and

$$\Pr[\text{The outcome of measuring } |\varphi\rangle^{\otimes N} \text{ under } \bigotimes_{i\in[N]} (1-2H_{l_i}) \text{ is } 0] = \langle\varphi|^{\otimes N} \frac{I+\bigotimes_{i\in[N]} O_{l_i}}{2} |\varphi\rangle^{\otimes N} .$$

结论由引理6.15得出。 □

7 多量子比特测试

在本节中，我们考虑扩展泡利矩阵 $X(g)$ $Z(g)$。我们设计了一种协议，迫使证明者的策略与这些矩阵保持一致。具体而言，使用这些矩阵的诚实证明者能够成功通过该协议。反过来，任何以足够高的概率成功的证明者，在 $|g|$ 为奇数时必须呈现近似反对易关系，而在 $|g|$为偶数时必须呈现近似对易关系，这与 $Z(g)$ 和 $X(g)$ 之间的关系类似。由于该测试是第2.3节中概述的单量子比特测试的推广，我们建议读者先复习该节。

7.1 纠错码

本节回顾一类特定纠错码的性质，这类纠错码在我们的构造中发挥着核心作用。虽然我们重点讨论哈达玛码，但我们的大多数论证也适用于满足若干基本性质的任意码，例如局部可测试性和自纠错。这些性质对于构造能够抵御错误、且只需有限访问所传输数据即可进行验证的交互式证明系统至关重要。

定理 7.1 （局部可测试且可自纠正的码）。 哈达玛码族 $\{C_k\}$ 满足以下性质：

1. 该码的码率为 $r = 1/\exp(k)$ ，相对距离为 $d = \Theta(1)$。

2. 它是一个生成矩阵为 $G_k \in \mathbb{F}_2^{n(k)\times k}$ 的线性码，其中 $n(k)$ 表示编码消息的长度与消息长度之间的函数关系 k。

3. 该码具有确定性的编码和解码算法，分别记为 E和 D。

此外，存在 $\varepsilon \in (0,0.001)$、 κ、 $\kappa' \in (0,1)$ 和 q_L、 $q_S \in \mathbb{Z}_+$ ，使得 t:

1. 局部测试： 对于所有 n，码 C_n 都是 κ-局部可测试的，查询复杂度为 q_L。也就是说，存在一个非自适应概率多项式时间预言机机 L ，其查询复杂度为 q_L，使得：

   (a) 对于任意 $k \in \mathbb{Z}_+$ 和 $x \in \mathbb{F}_2^k$，

   $$\Pr[L^{E(x)}(1^k) = 1] = 1.$$

(b) 对于任意 $k \in \mathbb{Z}_+$ 和 $w \in \mathbb{F}_2^{n(k)}$，

$$\Pr[L^w(1^k) = 1] \leq 1 - \kappa \cdot \mathrm{dist}(w, C_n).$$

2. 自校正：对于所有 n，码 C_n 具有查询复杂度 q_S的自校正性。存在一个非自适应概率多项式时间预言机机 S，其查询复杂度为 q_S，使得对于任意 $k \in \mathbb{Z}_+$ 和任意满足下式的 $w \in \mathbb{F}_2^{n(k)}$

$$\mathrm{dist}(w, C_n) < \kappa' \cdot d/2,$$

对所有 $p \in [n(k)]$，均有

$$\Pr[S^w(1^k, p) = (E \circ D(w))_p] \geq 1 - \varepsilon.$$

注释 7.2。对于 $i \in \{0,1\}^k$，令 $n(i) \in \mathbb{Z}$ 表示其二进制表示为 i的整数。那么，G_k 的第 $n(i)$ 行等于 i，即 $G_{k,\ n(i),\ \cdot} = i$。

We 现在定义测试与校正过程的随机性相关视图 s.

定义 7.3 (局部测试器与自校正器的随机性相关评估)。令 $\{C_n\}$ 为定理*7.1*中定义的码。

- 将 $L^w(1^k;\ r)$ 定义为 $L^w(1^k)$ 在使用随机性 $r \in \mathbb{F}_2^{l_L}$时的输出，其中 l_L 是 L的随机性复杂度。
- 将 $S^w(1^k, p; r)$ 定义为使用随机性 $r \in \mathbb{F}_2^{l_S}$时，$S^w(1^k, p)$ 的输出，其中 l_S是 S的随机性复杂度。

接下来，我们定义酉操作，在量子寄存器上模拟解码、局部测试和自校正功能。这些操作将用于我们的量子协议构造中。

定义 7.4 (酉解码算子)。设 D 为定理 *7.1*中的解码算法。对于 $k \in \mathbb{Z}_+$, $w \in \mathbb{F}_2^{n(k)}$ 和 $a \in \mathbb{F}_2^k$，定义解码酉算子

$$D_C(|a\rangle |w\rangle) = |a \oplus D(w)\rangle |w\rangle .$$

定义 7.5 (酉有效性测试算子)。设 L 如定义 *7.3*所述。对于 $k \in \mathbb{Z}_+$,$w \in \mathbb{F}_2^{n(k)}$，$r \in \mathbb{F}^{l_L}{}_{(k)\ 2}$ 以及所有 $a \in \mathbb{F}_2$，定义

$$L(|a\rangle |w\rangle |r\rangle) = \left|a \oplus L^w(1^k; r)\right\rangle |w\rangle |r\rangle .$$

定义 7.6 （酉自校正算子）。令 S 如定义 *7.3* 中所述。对于 $k \in \mathbb{Z}_+$、$w \in \mathbb{F}_2^{n(k)}$、$r \in \mathbb{F}^{l_S}{}_{(k)\ 2}$、$a \in \mathbb{F}_2$ 以及 $p \in [n(k)]$，，定义

$$S_p(|a\rangle |w\rangle |r\rangle) = \left|a \oplus S^w(1^k, p; r)\right\rangle |w\rangle |r\rangle .$$

7.2 诚实证明者的策略

诚实证明者与验证者进行三轮交互。我们首先描述证明者在前两轮中的操作，并将第三轮单独处理。

在第一轮中，诚实证明者对处于 Z 基底的 k量子比特见证执行纯化测量，并使用哈达玛码对 k 比特测量结果进行编码。随后，他将得到的量子态发送给验证者。收到验证者发回的同一寄存器后，证明者执行相同操作的逆操作。

在第二轮中，证明者再次对见证执行纯化测量，这次使用 X 基底，并用哈达玛码对结果进行编码。与第一轮一样，证明者将量子态发送给验证者，之后收到发回的寄存器时再执行逆过程。

在第三轮中，验证者发送一个指示基底（X 或 Z）的比特，诚实证明者对处于相应基底的见证执行纯化测量，并使用哈达玛码对结果进行编码。

现在，我们更精确地定义证明者在前两轮中的操作。这些轮次遵循一个由可观测量 O 参数化的通用模板。诚实证明者使用不同的 O 值：第一轮中使用 $O_a = Z(a)\ a \in \mathbb{F}_2^k$，第二轮中使用 $O_b = X(b)\ b \in \mathbb{F}_2^k$。现在，我们定义诚实证明者在前两轮中所执行操作的模板。该模板的具体实现将在后文描述。

定义 7.7（诚实证明者操作的模板）。 设 k、$n \in \mathbb{Z}_+$。设 P 为一个包含 k 个量子比特的寄存器，R $=$（Rj）$_{j\in[n]}$ 为一个包含 n 个量子比特的寄存器。P、R 最初由证明者持有。对于 $j \in [n]$，设 O_j为寄存器 P 上的可观测量。

- 证明者的第一步： 证明者应用以下酉算子

$$\prod_{p\in[n]} P(O_{p,\mathsf{P}}, \mathsf{R}_p).$$

  证明者将寄存器 R发送给验证者。

- 验证者的第一步： 验证者从证明者处接收寄存器 R 。验证者将寄存器R发送给证明者。

- 证明者的第二步： 证明者从验证者处接收寄存器 R 。证明者应用以下酉算子

$$(\prod_{p\in[n]} P(O_{p,\mathsf{P}}, \mathsf{R}_p))^{-1}.$$

注7.8 . 当我们实现模板时， O_j和 $j \in [n]$ 总是彼此对易 $r.$

接下来，我们描述诚实证明者在最后一轮的操作：

定义 7.9（最后一轮中诚实证明者的操作）。 设 $k, n \in \mathbb{Z}_+$。设 P 为一个包含 k 个量子比特的寄存器，R $=$ (Rj)$_{j\in[n]}$ 为一个包含 n 个量子比特的寄存器。P、R 最初由证明者持有。对于 $q' \in [2], j \in [n]$，令 $O_{q',j}$ 为寄存器 P 上的可观测量。

- 验证者向证明者发送 $q' \in [2]$。

- 诚实证明者按照定义 7.7 进行操作，其中 $O_p = O_{q',\ p}$ 对于 $p \in [n]$。

注 7.10。 当我们实现该模板时，对于 $q' \in [2], j_1, j_2 \in [n]$, $O_{q',\ j_1}$ 始终与 $O_{q',\ j_2}$对易。

注 7.11。 请注意，定义 7.7 中证明者的第二步对于定义7.9并非必要。但为便于说明，我们保留了这一步。在本节中，最后几轮的其他定义也同样如此。因此，我们的协议实质上包含 6 条消息，而非 7 条消息。

现在我们总结一下诚实证明者的操作：

定义 7.12 (多量子比特测试，诚实证明者)。 设 k, $n \in \mathbb{Z}_+$。设 $G_k = [g_1, g_2, \cdots, g_n]^T \in \mathbb{F}_2^n \otimes \mathbb{F}_2^k$ 如定义 7.3 所述。设 P 为一个包含 k 个量子比特的寄存器，R 为一个包含 n 个量子比特的寄存器。 P，R 最初由证明者持有，并初始化为 $|0\rangle$。

诚实证明者的操作定义如下：

- 诚实证明者将见证准备在寄存器 P 中。
- 诚实证明者按照定义 7.7 进行，其中 $O_p = Z(g_p)$ 对应 $p \in [n]$。
- 诚实证明者按照定义 7.7 进行，其中 $O_p = X(g_p)$ 对应 $p \in [n]$。
- 诚实证明者按照定义 7.9 进行，其中 $O_{1,\ p} = Z(g_p) O_{2,\ p} = X(g_p)$ 对应 $p \in [n]$。

7.3 验证者策略

接下来我们介绍验证者的操作。为便于说明，我们先对在自校正量子比特上施加 Z 门的过程进行抽象。

定义 7.13 (验证者的纯化形式，带自校正的读出)。 设 S_p 如定义 7.6所述。设 R $=(\mathsf{R}j)_{j\in[n]}$ 是一个含有 n 个量子比特的寄存器。设 S 是一个寄存器。定义

$$\widetilde{O}_{p,\mathsf{SRT_S}} = S^{\dagger}_{p,\mathsf{SRT_S}} \cdot Z_{\mathsf{S}} \cdot S_{p,\mathsf{SRT_S}}.$$

注7.14。 此处， S_p 对存储在寄存器 R位置p处的码字进行自校正，并将自校正后的结果存储在寄存器 S中。为执行自校正，该算法需要一些经典随机性，这些随机性存储在 $\mathsf{T_S}$中。因此，存储在 $\mathsf{T_S}$ 中的量子态是全-$|+\rangle$ 态。请注意，尽管我们以这种方式描述该算法，但在实际执行中，验证者会采样经典随机性。

在前两轮中，验证者可以通过多种方式回应证明者消息。稍后我们将说明验证者在整个协议中如何选择回应。在以下定义中，M， F， m， f可视为模板的输入。 M表示是否进行测量。 m 表示测量哪个寄存器。 F 表示是否进行翻转。 f 表示翻转哪个寄存器。

定义 7.15 (前两轮一致性检查中验证者操作的模板)。 设 R $=(\mathsf{R}j)_{j\in[n]}$ 为一个寄存器。设 S 为验证者持有的寄存器，初始值为$|0\rangle$。设 $\mathsf{T_S}$ 为验证者持有的寄存器，初始值为 $H^{\otimes l_{\mathsf{S}}}|0\rangle$，其中 l_{S} 的定义见定义 7.3。设 M， $F \in \{0,1\}$， m， $f \in [n]$。

- 证明者的第一步： 证明者向验证者发送寄存器 R。
- 验证者的第一步：验证者从证明者处接收寄存器 R 。如果 $F = 1$，验证者测量 Ts，然后验证者应用 $O_{f,\ \mathsf{SRTs}}$。如果 $M = 1$，验证者测量 $\widetilde{\mathsf{Ts}}$。然后，验证者测量 $O_{m,\ \mathsf{SRTs}}$ 并输出测量结果 r。验证者将寄存器 R发送给证明者。
- 证明者的第二步：证明者从验证者处接收寄存器 R 。

接下来，我们描述验证者在最后一轮中的操作：

定义 7.16 （验证者在最后一轮进行一致性检查时的操作）。令 $q' \in [2]$，$m \in [n]$。

- 验证者将 q' 发送给证明者。
- 验证者按照定义 *7.15* 进行操作，其中 $M = 1$，$F = 0$，$m = m$，$f = 0$。

现在，我们介绍验证者在多量子比特测试中的操作。验证者有两类检查：一致性检查和反对易检查。我们先介绍一致性检查。在这项检查中，验证者检查前两轮与最后一轮之间的一致性。更具体地说，验证者检查最后一轮的答案是否与前几轮的答案相符。

定义 7.17 (多量子比特测试，一致性检查)。设 D 是 $[n]$ 上的一个分布。设$\mathsf{R} = (\mathsf{R}j)_{j\in[n]}$ 为一个寄存器。设 S 为验证者持有并以 $|0\rangle$ 初始化的寄存器。设 $\mathsf{Ts}_{,\mathsf{i}}$（对 $i \in [3]$ ），为验证者持有并以 $H^{\otimes l_{\mathsf{S}}} |0\rangle$ 初始化的寄存器。验证者的操作定义如下：

- 验证者抽取 $u \in_R [2]$，设置 $M_u = 1$，并对 $i \neq u, i \in [2]$ 设置 $M_i = 0$ 。
- 如果 $M_1 = 1$，验证者将 $F_i = 0$ 设为 $i \in [2]$。如果 $M_2 = 1$，验证者将 $F_1 \in_R \mathbb{F}_2$设为 $F_2 = 0$。
- 验证者采样 f_1和 $f_2 \sim D$。
- 验证者重复定义 *7.15* 中的验证者操作两次。在第 i次中，验证者按照定义 *7.15* 执行，其中 $M = M_i$、$F = F_i$、$m = f_i$、$f = f_i$；如果 $M_i = 1$ ，则将 r_i 设为输出。
- 最后，验证者按照定义 *7.16* 执行，其中 $q' = u$、$m = f_u$。令 r' 为验证者的输出。
- 当且仅当 $r_u = r'$ 时，验证者接受。

接下来，我们介绍反对易测试。验证者会检查与中间应用的 X 相对应的一致性：第一轮的测量结果为 Z ，最后一轮的测量结果为 Z 。

定义 7.18 （多量子比特测试，反对易测试）。令 D 为 $[n]$ 上的一个分布。令 $G_k = [g_1, g_2, \cdots, g_n]^T \in \mathbb{F}_2^n \otimes \mathbb{F}_2^k$如定义 *7.3* 中所定义。令 $\mathsf{R} = (\mathsf{R}j)_{j\in[n]}$ 为一个寄存器。令S 为验证者持有并以 $|0\rangle$ 初始化的寄存器。令 $\mathsf{Ts}_{,\mathsf{i}}$ *for* $i \in [3]$ 为验证者持有并以 $H^{\otimes l_{\mathsf{S}}} |0\rangle$ 初始化的寄存器。验证者的操作定义如下：

- 验证者设置 $M_1 = 1, F_1 = 0, M_2 = 0, F_2 = 1$。
- 验证者采样 $(f_1, f_2) \sim D$。
- 验证者重复定义 *7.15* 中的验证者操作2 次。在第 i次，验证者按照定义 *7.15* 进行操作，其中 $M = M_i$， $F = F_i$， $m = f_i$， $f = f_i$，若 $M_i = 1$，则令 r_i 为输出。
- 最后，验证者按照定义 *7.16* 进行操作，其中 $q' = 1$， $m = f_1$。令 r' 为验证者的输出。
- 当且仅当 $r_1 = r' \oplus (g_{f_1} \cdot g_{f_2})$ 时，验证者接受。

最后，我们定义有效性检查，用于检查证明者是否确实向验证者发送了一个纠错码的实例。

定义 7.19 （验证者有效性检查的模板）。令 R $=$（Rj）$_{j\in[n]}$ 为一个寄存器。令L 为一个由验证者持有且初始化为 $|0\rangle$的寄存器。令 $\mathsf{T_L}$ 为一个由验证者持有且初始化为 $H^{\otimes l_\mathsf{L}}|0\rangle$的寄存器。令 $\mathsf{T_S}$ 为一个由验证者持有且初始化为 $H^{\otimes l_\mathsf{S}}|0\rangle$的寄存器。令 $t \in \{0,1\}, F \in \{0,1\}, f \in [n]$。

- 证明者的第一步：证明者将寄存器 R发送给验证者。
- 验证者的第一步：验证者从证明者处接收寄存器 R 。如果 $F = 1$，~验证者测量Ts，然后应用 $O_{f,\mathsf{SRTs}}$。
  - 如果 $t = 0$，验证者将寄存器 R发送给证明者。– 如果 $t = 1$，验证者测量$\mathsf{T_L}$，然后验证者应用 $L_{\mathsf{LRT_L}}$ 并测量 Z_L，输出测量结果 r。验证者将寄存器 R发送给证明者。
- 证明者的第二步：证明者从验证者处接收寄存器 R $r.$

接下来，我们描述验证者在最后一轮中的操作：

定义 7.20 （最后一轮中的验证者有效性检查）。令 $t \in \{0,1\}$。令 $q' \in [2]$。

- 验证者向证明者发送 q' 。
- 验证者按照定义 *7.19* 执行，参数为 $t = t$、 $F = 0$、 $f = 0$。

现在我们明确有效性检查过程中使用的验证者参数。

定义 7.21 （多量子比特测试，有效性检查）。设 D 是 $[n]$上的一个分布。设 R $=$(Rj)$_{j\in[n]}$ 是一个寄存器。设 S、L 是由验证者持有并初始化为 $|0\rangle$的寄存器。设 Ts,i ***for*** $i \in [3]$ 是由验证者持有并初始化为 $H^{\otimes l_\mathsf{S}}|0\rangle$的寄存器。设 TL,i ***for*** $i \in [3]$ 是由验证者持有并初始化为 $H^{\otimes l_\mathsf{L}}|0\rangle$的寄存器。验证者操作定义如下：

- 验证者抽样得到 $u \in_R [3]$。验证者设置 $t_u = 1$ 和 $t_i = 0$ ，其中 $i \neq u$、 $i \in [3]$。
- 验证者为 $i \in [u-1]$采样 $F_i \in_R \{0,1\}$ 。验证者为 $i \geq u$设置 $F_i = 0$ 。
- 验证者采样 f_1、 $f_2 \sim D$。
- 验证者抽取 $q' \in_R [2]$。

- 验证者重复执行定义 7.19 中的验证者操作两次。在第 i次中，验证者按照定义 7.19 进行操作，其中 $t = t_i$， $F = F_i$， $f = f_i$ 并且如果 $t_i = 1$ 将 r_i 设为输出。

- 最后，验证者按照定义 7.20 中的方式操作，其中 $t = t_3$， $q' = q'$ 并且如果 $t_3 = 1$ 则将 r_3设为输出。

- 验证者接受当且仅当 $r_u = 1$。

在描述验证者在多量子比特测试中的操作之前，我们先介绍验证者在测试期间使用的分布。

定义 7.22 （多量子比特测试的验证者分布）。 设 p， q 如定理 4.10所述，并设 s， N如引理 4.11所述。设 $H = \frac{1}{m}\sum_{i\in[m]} H_i \in \mathbb{C}^{2^n} \otimes \mathbb{C}^{2^n}$ 是一个 5-局部 Clifford 哈密顿量，其中 $m = \mathrm{poly}(n)$，并且 $\lambda_{\min}(H) \leq 2^{-p(n)}$ 或 $\lambda_{\min}(H) \geq 1/q(n)$。

对于每个 $i \in [m]$，令

$$H_i = \left(C_i^\dagger (|0\rangle\langle 0|)^{\otimes 5} C_i\right) \otimes I,$$
$$O_{i,j} = \left(C_i^\dagger (I^{\otimes(j-1)} \otimes Z \otimes I^{\otimes(5-j)}) C_i\right) \otimes I.$$

每个$O_{i,\ j}$ 都具有泡利表示

$$O_{i,j} = (-1)^{d_{i,j}} X(a_{i,j}) Z(b_{i,j}) Y(c_{i,j}),$$

如引理 6.13中所述。令 $t \in \mathbb{F}_2^{5N}$和 $l \in [m]^N$。定义

$$O(t,l) = \bigotimes_{i\in[N]} \prod_{j\in[5]} O_{l_i,j}^{t_{i,j}},$$

其泡利表示为：

$$O(t,l) = (-1)^{d(t,l)} X(a(t,l)) Z(b(t,l)) Y(c(t,l)).$$

定义测试中使用的测量分布如下：

- 对每个 $i \in [N]$，采样 $t \in_R \mathbb{F}_2^{5N}$、 $r \in_R \mathbb{F}_2^{Nn}$ 和 $l_i \in_R [m]$ 。
- 定义 μ_1 为以下数对上的分布 $(b(t,l) + c(t,l)\ a(t,l) + c(t,l))$。
- 定义 μ_2 为以下数对上的分布 $(b(t,l) + c(t,l) + r, a(t,l) + c(t,l))$。

现在我们把所有内容整合起来，并定义多量子比特测试中验证者的操作。

定义 7.23 (多量子比特测试，验证者)。 设 R 为一个寄存器。验证者的操作定义如下：

1. 以概率 $1/6$，验证者按照定义 7.17 进行操作，取 $D = \mu_1$；*2.* 以概率 $1/6$，验证者按照定义 7.18 进行操作，取 $D = \mu_1$；*3.* 以概率 $1/6$，验证者按照定义 7.21 进行操作，取 $D = \mu_1$；*4.* 以概率 $1/6$，验证者按照定义 7.17 进行操作，取 $D = \mu_2$；*5.* 以概率 $1/6$，验证者按照定义 7.18 进行操作，取 $D = \mu_2$，

6. 以概率 $1/6$，验证者按照定义 7.21 进行，其中 $D = \mu_2$，

7.4 一般证明者的操作

在陈述本节的主定理之前，我们先介绍一般证明者操作。

定义 7.24 （规范证明者操作）。 设 P 是一个寄存器，R 是一个包含 n 个量子比特的寄存器。P、R 最初由证明者持有，并初始化为 $|0\rangle$。对于 $q' \in [2]$，令 $U'_{q'}$ 为一个酉算子。对于 $i \in [2]$，令 U_i 为一个酉算子。

规范证明者在前两轮中的操作定义如下：在第 i 轮，

- 证明者的第一步： 证明者施加酉算子 $U_{i,\ \mathsf{PR}}$。证明者将寄存器R发送给验证者。
- 验证者的第一步： 验证者从证明者处接收寄存器 R 。验证者将寄存器R发送给证明者。
- 证明者的第二步：证明者从验证者处接收寄存器 R 。

最后一轮中规范证明者的操作定义如下：

- 验证者的第一步：验证者向证明者发送 $q' \in [2]$ 。
- 证明者的第一步：证明者施加酉算子 $U'_{q',\ \mathsf{PR}}$。证明者将寄存器R发送给验证者。
- 验证者的第一步：验证者从证明者处接收寄存器 R 。验证者向证明者发送寄存器R。
- 证明者的第二步：证明者从验证者处接收寄存器 R 。

注释 7.25。 注意，任何证明者操作都可以纯化为上述所述的规范证明者操作。

为便于表述，我们引入证明者和验证者的纯化形式与干净形式。

定义 7.26 （证明者的纯化形式）。 设 P、S、$\mathsf{T_S}$ 为一个寄存器，R 为一个包含 n 个量子比特的寄存器。对于 $q' \in [2]$，令 $U'_{q'}$ 为一个酉算子。对于 $a \in \mathbb{F}_2^k$，将最后一轮中的证明者的厄米形式定义为：

$$\widetilde{O}'_{q',j,\mathsf{SRT_S}} = (U'_{q',\mathsf{PR}})^\dagger \cdot \widetilde{O}_{j,\mathsf{SRT_S}} \cdot U'_{q',\mathsf{PR}}.$$

注释 7.27。 验证者的纯化形式定义于定义 7.13中。

定义 7.28 （验证者的干净形式）。 设 P、D 为一个寄存器，R 为一个包含 n 个量子比特的寄存器。令D_C 按照定义 7.4进行定义。对于 $a \in \mathbb{F}_2^k$，将前两轮中的验证者的厄米形式定义为：

$$O_{\mathsf{DR}}(a) = D^\dagger_{C,\mathsf{DR}} Z_{\mathsf{D}}(a) D_{C,\mathsf{DR}}.$$

注释 7.29。 酉算子 D_C 对寄存器 R 中存储的量子态进行解码，并将其存储在寄存器 D中。整体算子实际上直接将 $Z(a)$ 作用于由经典纠错码保护的量子态上。

定义 7.30 (证明者的干净形式)。 设 P、D 为一个寄存器，R 为一个含有 n 量子比特的寄存器。对于$q' \in [2]$，令$U'_{q'}$ 为一个酉算子。对于 $a \in \mathbb{F}_2^k$，定义最后一轮中证明者的厄米形式如下：

$$O'_{q',\mathsf{DPR}}(a) = (U'_{q',\mathsf{PR}})^\dagger O_{\mathsf{DR}}(a) U'_{q',\mathsf{PR}}.$$

为便于表述，我们引入转移作用。

定义 7.31 (转移作用)。 令 U_i 对于 $i \in [2]$ 的定义如定义 7.24所示。对于 $i < j$，定义从 i到 j 的转移作用如下：

$$U_{i\to j} = U_j \cdots U_{i+2} U_{i+1}.$$

定义 7.32 (纯化形式中的带翻转的转移作用)。 令 U_i 对于 $i \in [2]$ 的定义如定义 7.24所示。对于 $F \in \{0,1\}^2$， $f \in [n]^2$，定义纯化形式中的带翻转的转移作用如下：

$$\begin{aligned}
\widetilde{U}_{1,F,f,\mathsf{SPRT_S}} &= \widetilde{O}^{F_1}_{f_1,\mathsf{SRT_S}} U_1, \\
\widetilde{U}_{2,F,f,\mathsf{SPRT_S}} &= \widetilde{O}^{F_2}_{f_2,\mathsf{SPRT_S}} U_2 \cdot \widetilde{U}_{1,F,f,\mathsf{SPRT_S}}.
\end{aligned}$$

定义 7.33 (干净形式中的带翻转的转移作用)。 令 $G_k = [g_1, g_2, \cdots, g_n]^T \in \mathbb{F}_2^n \otimes \mathbb{F}_2^k$ 的定义如定义 7.3所示。令 U_i 对于 $i \in [2]$ 的定义如定义 7.24所示。对于$F \in \{0,1\}^2$， $f \in [n]^2$，定义干净形式中的带翻转的转移作用如下：

$$\begin{aligned}
U_{1,F,f} &= O(g_{f_1})^{F_1} U_1, \\
U_{2,F,f} &= O(g_{f_2})^{F_2} U_2 \cdot U_{1,F,f}.
\end{aligned}$$

7.5 主定理

现在，我们在本节中陈述主定理。

定理 7.　34 (多量子比特测试)。 设 V 为定义 7.23 中定义的验证者，则：

1. 完备性： V 以概率 1 接受定义 7.12 中的证明者。

2. 可靠性： 设 P 为定义 7.24 中定义的证明者。设 $O'_1(\cdot)$ $O'_2(\cdot)$ 按定义 7.30 定义。若 V 以大于 P 的概率接受 $1-\delta$，则 $O'_1(a)$ $O'_2(b)$ 在该量子态下满足近似反对易/对易关系

$$\rho = U_{0\to 2} \left|000\right\rangle_{\mathsf{PRD}} \left\langle 000\right|_{\mathsf{PRD}} U^\dagger_{0\to 2}.$$

更具体地说，

$$\mathop{\mathbb{E}}_{(a,b)\sim\mu_1} \left\| O'_1(a)O'_2(b) - (-1)^{a\cdot b} O'_2(b)O'_1(a) \right\|_\rho^2 = \Theta(\delta),$$

and

$$\mathop{\mathbb{E}}_{(a,b)\sim\mu_2} \left\| O'_1(a)O'_2(b) - (-1)^{a\cdot b} O'_2(b)O'_1(a) \right\|_\rho^2 = \Theta(\delta).$$

在证明主定理之前，我们先建立几个有助于证明的引理。我们首先考察定义 7.30 和定义7.28的一些基本性质。

引理 7.35 (证明者厄米特形式的性质)。 设 $O'_{q'}(a)$ 对于 $q' \in [2], a \in \mathbb{F}_2^k$ 如定义 *7.30*所述。

1. 对于 $q' \in [2]$, *2.* 对于 $a \in \mathbb{F}_2^k$, *3.* 对于 $q' \in [2]$、$a \in \mathbb{F}_2^k$, *4.* 对于 $q' \in [2]$、a、$b \in \mathbb{F}_2^k$、$q' \in [2]$、a、$b \in \mathbb{F}_2^k$,

$$O'_{q'}(a) = (O'_{q'}(a))^\dagger,$$

$$(O'_{q'}(a))^2 = I,$$

$$[O'_{q'}(a), O'_{q'}(b)] = 0,$$

$$O'_{q'}(a) \cdot O'_{q'}(b) = O'_{q'}(a \oplus b).$$

证明。 这个引理可通过直接计算得出。 □

引理 7.36 (验证者厄米特形式的性质)。 令 $O(a)$ 对于 $a \in \mathbb{F}_2^k$ 按照定义 *7.28*定义。

1. 对于 $a \in \mathbb{F}_2^k$, *2.* 对于 $a \in \mathbb{F}_2^k$, *3.* 对于 a、$b \in \mathbb{F}_2^k$, *4.* 对于 a、$b \in \mathbb{F}_2^k$,

$$O(a) = (O(a))^\dagger,$$

$$(O(a))^2 = I,$$

$$[O(a), O(b)] = 0,$$

$$O(a) \cdot O(b) = O(a \oplus b).$$

证明。 这个引理可通过直接计算得出。 □

接下来，我们考察总体成功概率与各配置下成功概率之间的关系。

引理 7.37。 设 V, P 如定理 *7.34*中所定义。设 D_c 是 M, F 在定义 *7.17*中的分布。设 D_v 是 u 在定义 *7.21*中的分布。

Then

$$\Pr[\ V \textit{ accepts } P\ ] \geq 1 - \Theta(\delta),$$

当且仅当

- 对于 D_v 的支撑集中的任意 $u \in [3]$、$F \in \{0,1\}^2$、$q' \in [2]$，

$$\Pr[\ \textit{validity check passes} \mid F, q', u, D\ ] \geq 1 - \Theta(\delta).$$

- 对于任意属于 D_c 的支撑集中的 M、$F \in \{0,1\}^2$，

$$\Pr[\ \textit{consistency check passes} \mid M, F, D\ ] \geq 1 - \Theta(\delta).$$

- 此外，

$$\Pr[\ \textit{anti-commuting test passes}\ \mid D] \geq 1 - \Theta(\delta).$$

*Pr*呃。 该引理可由并集界的直接应用得出 . □

下面的引理描述了局部测试的成功概率（参见定义 7.5）与底层量子态的系数之间的关系。

对于接下来的引理，回顾定理 7.1中的记号。

引理 7.38。设

$$|\psi\rangle = |\varphi\rangle_{\mathsf{PR}} \otimes |0\rangle_{\mathsf{L}} \otimes H^{\otimes l_{\mathtt{L}}} |0\rangle_{\mathsf{T_L}} \ ,$$

其中

$$|\varphi\rangle = \sum_{w\in\mathbb{F}_2^n} \alpha_w \, |\varphi_w\rangle_{\mathsf{P}} \, |w\rangle_{\mathsf{R}} \ ,$$

对于任意的（归一化）系数 α_w。那么

$$\|(|1\rangle\langle 1|_{\mathsf{L}} \otimes I_{\mathsf{PRT_L}}) \cdot L_{\mathsf{LRT_L}} \, |\psi\rangle \, \|^2 = \sum_{w\in\mathbb{F}_2^n} |\alpha_w|^2 \cdot \Pr[\mathtt{L}^w(1^k) = 1],$$

and

$$\|(|1\rangle\langle 1|_{\mathsf{L}} \otimes I_{\mathsf{PRT_L}}) \cdot L_{\mathsf{LRT_L}} \, |\psi\rangle \, \|^2 \leq 1 - \frac{\kappa\cdot\kappa'\cdot d}{2}\Big(1 - \sum_{dist(w,C_n)<\kappa'\cdot d/2} |\alpha_w|^2\Big).$$

证明。注意

$$L(|a\rangle \, |w\rangle \, |r\rangle) = \Big|a \oplus \mathtt{L}^w(1^k; r)\Big\rangle \, |w\rangle \, |r\rangle \, ,$$

thus

$$\Pr[\mathtt{L}^w(1^k) = 1] = \|(|1\rangle\langle 1|_{\mathsf{L}} \otimes I_{\mathsf{PRT_L}}) \cdot L_{\mathsf{LRT_L}}(|\varphi_w\rangle_{\mathsf{P}} \, |w\rangle_{\mathsf{R}} \, |0\rangle_{\mathsf{L}} \, H^{\otimes l_{\mathtt{L}}} \, |0\rangle_{\mathsf{T_L}})\|^2,$$

and

$$\sum_{w\in\mathbb{F}_2^n} |\alpha_w|^2 \cdot \Pr[\mathtt{L}^w(1^k) = 1] = \|(|1\rangle\langle 1|_{\mathsf{L}} \otimes I_{\mathsf{PRT_L}}) \cdot L_{\mathsf{LRT_L}}(|\psi\rangle)\|^2.$$

此外，根据定理 7.1 的保证，

$$\Pr[\mathtt{L}^w(1^k) = 1] \leq 1 - \kappa \cdot dist(w, C_n).$$

Thus

$$\begin{aligned}
&\sum_{w\in\mathbb{F}_2^n} |\alpha_w|^2 \cdot \Pr[\mathtt{L}^w(1^k) = 1] \\
\leq\ &\sum_{w\in\mathbb{F}_2^n} |\alpha_w|^2 \cdot (1 - \kappa \cdot dist(w, C_n)) \\
\leq\ &\sum_{dist(w,C_n)<\kappa'\cdot d/2} |\alpha_w|^2 + \sum_{dist(w,C_n)\geq\kappa'\cdot d/2} |\alpha_w|^2 \cdot (1 - \kappa\cdot\kappa'\cdot d/2) \\
=\ &1 - \frac{\kappa\cdot\kappa'\cdot d}{2}\Big(1 - \sum_{dist(w,C_n)<\kappa'\cdot d/2} |\alpha_w|^2\Big).
\end{aligned}$$

□

以下引理刻画了净化形式与干净形式之差，以及底层量子态的系数之间的关系。

引理 7.39。设

$$|\psi\rangle = |\varphi\rangle_{\mathsf{PR}} \otimes |0\rangle_{\mathsf{SD}} \otimes H^{\otimes l_{\mathsf{S}}} |0\rangle_{\mathsf{T_S}},$$

and

$$|\varphi\rangle = \sum_{w\in\mathbb{F}_2^n} \alpha_w |\varphi_w\rangle_{\mathsf{P}} |w\rangle_{\mathsf{R}}.$$

Then

$$\|\widetilde{O}_{p,\mathsf{SRT_S}} |\psi\rangle - O_{\mathsf{DR}}(g_p) |\psi\rangle\|^2 \le 4 - (4-4\varepsilon) \sum_{dist(w,C_n)<\kappa'\cdot d/2} |\alpha_w|^2.$$

证明。 注意到

$$O_{\mathsf{DR}}(a) = D_{\mathsf{DR}}^{\dagger} Z_{\mathsf{D}}(a) D_{\mathsf{DR}},$$

thus

$$O_{\mathsf{DR}}(g_p) |0\rangle |w\rangle = (-1)^{(\mathtt{E}\circ\mathtt{D}(w))_p} |0\rangle |w\rangle.$$

此外，注意到

$$\widetilde{O}_{p,\mathsf{SRT_S}} = S_p^{\dagger} \cdot Z \cdot S_p,$$

and

$$S_p(|a\rangle |w\rangle |r\rangle) = \left|a \oplus \mathtt{S}^w(1^k, p; r)\right\rangle |w\rangle |r\rangle,$$

thus

$$\widetilde{O}_p |0\rangle |w\rangle |r\rangle = (-1)^{\mathtt{S}^w(1^k,p;r)} |0\rangle |w\rangle |r\rangle.$$

于是，我们有

$$\begin{aligned} &\|\widetilde{O}_{p,\mathsf{SRT_S}} |\psi\rangle - O_{\mathsf{DR}}(g_p) |\psi\rangle\|^2 \\ &= 2 - 2\Re[(\widetilde{O}_{p,\mathsf{SRT_S}} |\psi\rangle)^{\dagger}(O_{\mathsf{DR}}(g_p) |\psi\rangle)], \end{aligned} \tag{4}$$

and

$$\begin{aligned} &(\widetilde{O}_{p,\mathsf{SRT_S}} |\psi\rangle)^{\dagger}(O_{\mathsf{DR}}(g_p) |\psi\rangle) \\ =& (\sum_w \mathop{\mathbb{E}}_r \alpha_w (-1)^{\mathtt{S}^w(1^k,p;r)} |0\rangle |\varphi_w\rangle |w\rangle |r\rangle)^{\dagger} (\sum_w \mathop{\mathbb{E}}_r \alpha_w (-1)^{(\mathtt{E}\circ\mathtt{D}(w))_p} |0\rangle |\varphi_w\rangle |w\rangle |r\rangle) \\ =& \sum_w \mathop{\mathbb{E}}_r |\alpha_w|^2 \cdot (-1)^{\mathtt{S}^w(1^k,p;r)+(\mathtt{E}\circ\mathtt{D}(w))_p}. \end{aligned} \tag{5}$$

注意，

$$dist(w, C_n) < \kappa' \cdot d/2 \implies \forall p \in [n], \Pr[\mathtt{S}^w(1^k, p) = (\mathtt{E}\circ\mathtt{D}(w))_p] \ge 1-\varepsilon,$$

thus

$$\begin{aligned}
&\sum_w \mathop{\mathbb{E}}_r |\alpha_w|^2 \cdot (-1)^{\mathtt{S}^w(1^k,p;r)+(\mathtt{E}\circ\mathtt{D}(w))_p} \\
\geq &\sum_{dist(w,C_n)<\kappa'\cdot d/2} |\alpha_w|^2 \mathop{\mathbb{E}}_r (-1)^{\mathtt{S}^w(1^k,p;r)+(\mathtt{E}\circ\mathtt{D}(w))_p} - \sum_{dist(w,C_n)\geq\kappa'\cdot d/2} |\alpha_w|^2 \\
\geq &(1-2\varepsilon) \sum_{dist(w,C_n)<\kappa'\cdot d/2} |\alpha_w|^2 - \sum_{dist(w,C_n)\geq\kappa'\cdot d/2} |\alpha_w|^2 \\
= &(2-2\varepsilon) \sum_{dist(w,C_n)<\kappa'\cdot d/2} |\alpha_w|^2 - 1.
\end{aligned}$$

代回（4）和（5），

$$\begin{aligned}
\|\widetilde{O}_{p,\mathsf{SRT_S}} |\psi\rangle - O_{\mathsf{DR}}(g_p) |\psi\rangle\|^2 &\leq 2 - 2((2-2\varepsilon) \sum_{dist(w,C_n)<\kappa'\cdot d/2} |\alpha_w|^2 - 1) \\
&= 4 - (4-4\varepsilon) \sum_{dist(w,C_n)<\kappa'\cdot d/2} |\alpha_w|^2.
\end{aligned}$$

□

引理 7.40（局部测试的蕴含）。设 $|\psi\rangle$ 属于引理 7.38。则

$$\|\widetilde{O}_{p,\mathsf{SRT_S}} |\psi\rangle - O_{\mathsf{DR}}(g_p) |\psi\rangle\|^2 \leq 4\varepsilon + \frac{8-8\varepsilon}{\kappa\cdot\kappa'\cdot d}\Big(1 - \|(|1\rangle\langle 1|_{\mathsf{L}} \otimes I_{\mathsf{PRT_L}}) \cdot L_{\mathsf{LRT_L}} |\psi\rangle\|^2\Big).$$

此外，对于 ε，κ，κ'，d 按定理 7.1中的定义，

$$\|\widetilde{O}_{p,\mathsf{SRT_S}} |\psi\rangle - O_{\mathsf{DR}}(g_p) |\psi\rangle\|^2 \leq \Theta(\varepsilon) + \Theta\Big(1 - \|(|1\rangle\langle 1|_{\mathsf{L}} \otimes I_{\mathsf{PRT_L}}) \cdot L_{\mathsf{LRT_L}} |\psi\rangle\|^2\Big).$$

证明。由引理 7.38 可得

$$1 - \frac{2}{\kappa\cdot\kappa'\cdot d}\Big(1 - \|(|1\rangle\langle 1|_{\mathsf{L}} \otimes I_{\mathsf{PRT_L}}) \cdot L_{\mathsf{LRT_L}} |\psi\rangle\|^2\Big) \leq \sum_{dist(w,C_n)<\kappa'\cdot d/2} |\alpha_w|^2.$$

因此，

$$\begin{aligned}
&4 - (4-4\varepsilon) \sum_{dist(w,C_n)<\kappa'\cdot d/2} |\alpha_w|^2 \\
\leq &4\varepsilon + \frac{8-8\varepsilon}{\kappa\cdot\kappa'\cdot d}\Big(1 - \|(|1\rangle\langle 1|_{\mathsf{L}} \otimes I_{\mathsf{PRT_L}}) \cdot L_{\mathsf{LRT_L}} |\psi\rangle\|^2\Big)
\end{aligned}$$

利用引理 7.39，

$$\|\widetilde{O}_{p,\mathsf{SRT_S}} |\psi\rangle - O_{\mathsf{DR}}(g_p) |\psi\rangle\|^2 \leq 4\varepsilon + \frac{8-8\varepsilon}{\kappa\cdot\kappa'\cdot d}\Big(1 - \|(|1\rangle\langle 1|_{\mathsf{L}} \otimes I_{\mathsf{PRT_L}}) \cdot L_{\mathsf{LRT_L}} |\psi\rangle\|^2\Big).$$

□

那么，我们开始考虑前两轮有效性检查的推论 s.

引理 7.41。设

$$|\varphi\rangle = |0\rangle_{\mathsf{PRDS}} \otimes H^{\otimes l_{\mathsf{S}}} |0\rangle_{\mathsf{T}_{\mathsf{S},1}} \otimes H^{\otimes l_{\mathsf{S}}} |0\rangle_{\mathsf{T}_{\mathsf{S},2}} \cdots \otimes H^{\otimes l_{\mathsf{S}}} |0\rangle_{\mathsf{T}_{\mathsf{S},u}},$$

那么对于 $u \in [2]$,

$$\begin{aligned}&\mathop{\mathbb{E}}_{(f_1,f_2)\sim D}[\||\widetilde{U}_{u,F,f}\,|\varphi\rangle - O(g_{f_u})^{F_u} U_u \widetilde{U}_{u-1,F,f}\,|\varphi\rangle\,\|^2]\\ \le\ &\Theta(\varepsilon) + \Theta\Big(1 - \Pr[\ \textit{validity check passes}\ \mid F, u, D\ ]\Big).\end{aligned}$$

证明。 令 $|\varphi'\rangle = U_u \widetilde{U}_{u-1,\ F,\ f}\,|\varphi\rangle$, $|\varphi''\rangle = |\varphi'\rangle \otimes |0\rangle_{\mathsf{L}} \otimes H^{\otimes l_{\mathsf{L}}} |0\rangle_{\mathsf{T}_{\mathsf{L}}}$。 那么

$$\begin{aligned}&\Pr[\ \text{validity check passes}\ \mid F, u\ ]\\ =\ &\mathop{\mathbb{E}}_{(f_1,f_2)\sim D} \|(|1\rangle\langle 1|_{\mathsf{L}} \otimes I) \cdot L_{\mathsf{LRT}_{\mathsf{L}}}(|\varphi''\rangle)\|^2.\end{aligned}$$

此外,

$$\begin{aligned}&\mathop{\mathbb{E}}_{(f_1,f_2)\sim D}[\||\widetilde{U}_{u,F,f}\,|\varphi\rangle - O(g_{f_u})^{F_u} U_u \widetilde{U}_{u-1,F,f}\,|\varphi\rangle\,\|^2]\\ =\ &\mathop{\mathbb{E}}_{(f_1,f_2)\sim D}[\||\widetilde{O}_{f_u}^{F_u}\,|\varphi'\rangle - O(g_{f_u})^{F_u}\,|\varphi'\rangle\,\|^2]\\ =\ &\mathop{\mathbb{E}}_{(f_1,f_2)\sim D}[\||\widetilde{O}_{f_u}^{F_u}\,|\varphi''\rangle - O(g_{f_u})^{F_u}\,|\varphi''\rangle\,\|^2]\\ \le\ &\mathop{\mathbb{E}}_{(f_1,f_2)\sim D}[\Theta(\varepsilon) + \Theta\Big(1 - \|(|1\rangle\langle 1|_{\mathsf{L}} \otimes I) \cdot L_{\mathsf{LRT}_{\mathsf{L}}}\,|\varphi''\rangle\,\|^2\Big)]\\ =\ &\Theta(\varepsilon) + \Theta\Big(1 - \Pr[\ \text{validity check passes}\ \mid F, u, D\ ]\Big),\end{aligned}$$

其中该不等式由引理7.40得出。 □

引理 7.42 （有效性检查 I 的推论）。 令

$$|\varphi\rangle = |0\rangle_{\mathsf{PRDS}} \otimes H^{\otimes l_{\mathsf{S}}} |0\rangle_{\mathsf{T}_{\mathsf{S},1}} \otimes H^{\otimes l_{\mathsf{S}}} |0\rangle_{\mathsf{T}_{\mathsf{S},2}} \cdots \otimes H^{\otimes l_{\mathsf{S}}} |0\rangle_{\mathsf{T}_{\mathsf{S},u}},$$

那么对于 $u \in [2]$,

$$\begin{aligned}&\mathop{\mathbb{E}}_{(f_1,f_2)\sim D}[\||\widetilde{U}_{u,F,f}\,|\varphi\rangle - U_{u,F,f}\,|\varphi\rangle\,\|^2]\\ \le\ &\Theta(\varepsilon) + \sum_{v\le u} \Theta\Big(1 - \Pr[\ \textit{validity check passes}\ \mid F, u = v, D\ ]\Big)\end{aligned}$$

证明。 该引理可由三角不等式和引理7.41得出。 □

接下来，我们开始考察最后一轮有效性检查的推论。**引理 7.43**。 设 $G_k = [g_1, g_2, \cdots, g_n]^T \in \mathbb{F}_2^n \otimes \mathbb{F}_2^k$ 如定义 7.3中所定义。设

$$|\varphi\rangle = |0\rangle_{\mathsf{PRDS}} \otimes H^{\otimes l_{\mathsf{S}}} |0\rangle_{\mathsf{T}_{\mathsf{S},1}} \otimes H^{\otimes l_{\mathsf{S}}} |0\rangle_{\mathsf{T}_{\mathsf{S},2}} \cdots \otimes H^{\otimes l_{\mathsf{S}}} |0\rangle_{\mathsf{T}_{\mathsf{S},u}}.$$

那么对于 $q' \in [2]$,

$$\begin{aligned}&\mathop{\mathbb{E}}_{(f_1,f_2)\sim D}[\||\widetilde{O}'_{q',f_{q'}} \widetilde{U}_{2,F,f}\,|\varphi\rangle - O'_{q'}(g_{f_{q'}}) \widetilde{U}_{2,F,f}\,|\varphi\rangle\,\|^2]\\ \le\ &\Theta(\varepsilon) + \Theta\Big(1 - \Pr[\ \textit{validity check passes}\ \mid F, q', u = 3, D\ ]\Big)\end{aligned}$$

证明。 令 $|\varphi'\rangle = U'_{q'}\widetilde{U}_{2,F,f}|\varphi\rangle$, $|\varphi''\rangle = |\varphi'\rangle \otimes |0\rangle_{\mathsf{L}} \otimes H^{\otimes l_{\mathsf{L}}}|0\rangle_{\mathsf{T_L}}$。那么根据定义,

$$\begin{aligned}&\Pr[\text{ validity check passes } \mid F, q', u=3, D\ ]\\ =\ &\mathop{\mathbb{E}}_{(f_1,f_2)\sim D}\|(|1\rangle\langle 1|_{\mathsf{L}}\otimes I)\cdot L_{\mathsf{LRT_L}}(|\varphi''\rangle)\|^2.\end{aligned}$$

此外,

$$\begin{aligned}&\mathop{\mathbb{E}}_{(f_1,f_2)\sim D}[\|\widetilde{O}'_{q',f_{q'}}\widetilde{U}_{2,F,f}|\varphi\rangle - O'_{q'}(g_{f_{q'}})\widetilde{U}_{2,F,f}|\varphi\rangle\|^2]\\ =\ &\mathop{\mathbb{E}}_{(f_1,f_2)\sim D}[\|\widetilde{O}_{f_{q'}}|\varphi'\rangle - O(g_{f_{q'}})|\varphi'\rangle\|^2]\\ =\ &\mathop{\mathbb{E}}_{(f_1,f_2)\sim D}[\|\widetilde{O}_{f_{q'}}|\varphi''\rangle - O(g_{f_{q'}})|\varphi''\rangle\|^2]\\ \le\ &\mathop{\mathbb{E}}_{(f_1,f_2)\sim D}[\Theta(\varepsilon)+\Theta\Big(1-\|(|1\rangle\langle 1|_{\mathsf{L}}\otimes I)\cdot L_{\mathsf{LRT_L}}(|\varphi''\rangle)\|^2\Big)]\\ =\ &\Theta(\varepsilon)+\Theta\Big(1-\Pr[\text{ validity check passes } \mid F, q', u=3, D\ ]\Big)\ ,\end{aligned}$$

其中不等式由引理7.40得出。 □

引理 7.44 （有效性检查 II 的推论）。设

$$|\varphi\rangle = |0\rangle_{\mathsf{PRDS}}\otimes H^{\otimes l_{\mathsf{S}}}|0\rangle_{\mathsf{T_{S,1}}}\otimes H^{\otimes l_{\mathsf{S}}}|0\rangle_{\mathsf{T_{S,2}}}\cdots\otimes H^{\otimes l_{\mathsf{S}}}|0\rangle_{\mathsf{T_{S,u}}},$$

则对于 $q'\in[2]$,

$$\begin{aligned}&\mathop{\mathbb{E}}_{(f_1,f_2)\sim D}[\|\widetilde{O}'_{q',f_{q'}}\widetilde{U}_{2,F,f}|\varphi\rangle - O'_{q'}(g_{f_{q'}})U_{2,F,f}|\varphi\rangle\|^2]\\ \le\ &\Theta(\varepsilon)+\sum_{u\in[3]}\Theta\Big(1-\Pr[\ \textit{validity check passes}\ \mid F, q', u, D\ ]\Big).\end{aligned}$$

证明。该引理由三角不等式、引理7.42和引理7.43得出。 □

引理 7.45 （一致性检查的推论）。 设 U_i 对于 $i\in[2]$ 按定义7.24中的方式定义。设 P、R 按定义 7.24中的方式定义。设 D 为 M在定义7.17中的抽样分布 F。对于任意 M, $F\in\{0,1\}^2$ 属于 D的支撑集。设 $M_u = 1$。
Then

$$\begin{aligned}&\mathop{\mathbb{E}}_{(f_1,f_2)\sim D}\|(U_{u\to 2,\mathsf{PR}}O_{\mathsf{DR}}(g_{f_u})U_{u,F,f,\mathsf{DPR}} - O'_{u,\mathsf{DPR}}(g_{f_u})U_{2,F,f,\mathsf{DPR}})|0\rangle_{\mathsf{DPR}}\|^2\\ \le\ &\Theta(1-\Pr[\ \textit{consistency check passes}\ \mid M,F,D])\\ &+\sum_{F,q',u}\Theta(1-\Pr[\ \textit{validity check passes}\ \mid F,q',u,D\ ])+\Theta(\varepsilon).\end{aligned}$$

证明。 通过直接计算,

$$\begin{aligned}&\Pr[\text{ consistency check passes } \mid M,F,D]\\ =\ &\mathop{\mathbb{E}}_{(f_1,f_2)\sim D}\sum_{a\in\{\pm 1\}}\|\frac{I+a\cdot\widetilde{O}'_{u,f_u}}{2}\cdot U_{u\to 2}\cdot\frac{I+a\cdot\widetilde{O}_{f_u}}{2}\cdot\widetilde{U}_{u,F,f}|0\rangle\|^2\end{aligned}$$

$$
\begin{aligned}
&= \mathop{\mathbb{E}}_{(f_1,f_2)\sim D} \langle 0| \frac{2I + \widetilde{U}^\dagger_{u,F,f}\widetilde{O}_{f_u}U^\dagger_{u\to 2}\widetilde{O}'_{u,f_u}\widetilde{U}_{2,F,f} + \widetilde{U}^\dagger_{2,F,f}\widetilde{O}'_{u,f_u}U_{u\to 2}\widetilde{O}_{f_u}\widetilde{U}_{u,F,f}}{4} |0\rangle \\
&= 1 - \mathop{\mathbb{E}}_{(f_1,f_2)\sim D} \frac{\| U_{u\to 2}\widetilde{O}_{f_u}\widetilde{U}_{u,F,f}|0\rangle - \widetilde{O}'_{u,f_u}\widetilde{U}_{2,F,f}|0\rangle \|^2}{4}.
\end{aligned}
$$

此外，

$$
\begin{aligned}
&\| U_{u\to 2}\widetilde{O}_{f_u}\widetilde{U}_{u,F,f}|0\rangle - \widetilde{O}'_{u,f_u}\widetilde{U}_{2,F,f}|0\rangle \|^2 \\
\geq\ &\| U_{u\to 2}O(g_{f_u})U_{u,F,f}|0\rangle - O'_u(g_{f_u})U_{2,F,f}|0\rangle \|^2 \\
&\quad - \| O'_u(g_{f_u})U_{2,F,f}|0\rangle - \widetilde{O}'_{u,f_u}\widetilde{U}_{2,F,f}|0\rangle \|^2 \\
&\quad - \| U_{u\to 2}\widetilde{O}_{f_u}\widetilde{U}_{u,F,f}|0\rangle - U_{u\to 2}O(g_{f_u})U_{u,F,f}|0\rangle \|^2 \\
\geq\ &\| U_{u\to 2}O(g_{f_u})U_{u,F,f}|0\rangle - O'_u(g_{f_u})U_{2,F,f}|0\rangle \|^2 \\
&\quad - \Theta(\varepsilon) - \sum_{F,q',u} \Theta\Big(1 - \Pr[\text{ validity check passes } \mid F,q',u,D\ ]\Big).
\end{aligned}
$$

因此，

$$
\begin{aligned}
&\mathop{\mathbb{E}}_{(f_1,f_2)\sim D} \| U_{u\to 2}O(g_{f_u})U_{u,F,f}|0\rangle - O'_u(g_{f_u})U_{2,F,f}|0\rangle \|^2 \\
\leq\ &4(1 - \Pr[\text{ consistency check passes } \mid M,F,D]) \\
&\quad + \Theta(\varepsilon) + \sum_{F,q',u} \Theta\Big(1 - \Pr[\text{ validity check passes } \mid F,q',u,D\ ]\Big).
\end{aligned}
$$

□

引理 7.46（反对易测试的推论）。设 U_i 对于 $i \in [2]$ 按定义 7.24定义。设 P，R 按定义 7.24定义。

那么，

$$
\begin{aligned}
&\mathop{\mathbb{E}}_{(m_1,m_2)\sim D} \| O'_1(m_1)O(m_2)U_{0\to 2}|0\rangle - (-1)^{g_{m_1}\cdot g_{m_2}}O(m_2)U_2O(m_1)U_1|0\rangle \|^2 \\
\leq\ &\Theta(1 - \Pr[\ \textit{anti-commuting test passes}\ \mid D]) \\
&\quad + \sum_{F,q',u} \Theta(1 - \Pr[\ \textit{validity check passes}\ \mid F,q',u,D\ ]) + \Theta(\varepsilon).
\end{aligned}
$$

证明。通过直接计算，

$$
\begin{aligned}
&\Pr[\text{反对易测试通过} \mid D] \\
=\ &\mathop{\mathbb{E}}_{(m_1,m_2)\sim D} \sum_{a\in\{\pm 1\}} \| \frac{I + (-1)^{g_{m_1}\cdot g_{m_2}}\cdot a\cdot \widetilde{O}'_{1,m_1}}{2}\cdot \widetilde{O}_{m_2}\cdot U_2\cdot \frac{I + a\cdot\widetilde{O}_{m_1}}{2}\cdot U_1|0\rangle \|^2 \\
=\ &\mathop{\mathbb{E}}_{(m_1,m_2)\sim D} \langle 0| \frac{2I + (-1)^{g_{m_1}\cdot g_{m_2}}\cdot\Big(U^\dagger_{0\to 2}\widetilde{O}_{m_2}\widetilde{O}'_{1,m_1}\widetilde{O}_{m_2}U_2\widetilde{O}_{m_1}U_1 + U^\dagger_1\widetilde{O}_{m_1}U^\dagger_2\widetilde{O}_{m_2}\widetilde{O}'_{1,m_1}\widetilde{O}_{m_2}U_{0\to 2}\Big)}{4} |0\rangle \\
=\ &1 - \mathop{\mathbb{E}}_{(m_1,m_2)\sim D} \frac{\| \widetilde{O}'_{1,m_1}\widetilde{O}_{m_2}U_{0\to 2}|0\rangle - (-1)^{g_{m_1}\cdot g_{m_2}}\widetilde{O}_{m_2}U_2\widetilde{O}_{m_1}U_1|0\rangle \|^2}{4}.
\end{aligned}
$$

此外，

$$\begin{aligned}
&\|\widetilde{O}'_{1,m_1}\widetilde{O}_{m_2}U_{0\to 2}\,|0\rangle-(-1)^{g_{m_1}\cdot g_{m_2}}\widetilde{O}_{m_2}U_2\widetilde{O}_{m_1}U_1\,|0\rangle\,\|^2\\
\geq\;&\|O'_1(m_1)O(m_2)U_{0\to 2}\,|0\rangle-(-1)^{g_{m_1}\cdot g_{m_2}}O(m_2)U_2O(m_1)U_1\,|0\rangle\,\|^2\\
&-\|\widetilde{O}'_{1,m_1}\widetilde{O}_{m_2}U_{0\to 2}\,|0\rangle-O'_1(m_1)O(m_2)U_{0\to 2}\,|0\rangle\,\|^2\\
&-\|\widetilde{O}_{m_2}U_2\widetilde{O}_{m_1}U_1\,|0\rangle-O(m_2)U_2O(m_1)U_1\,|0\rangle\,\|^2\\
\geq\;&\|O'_1(m_1)O(m_2)U_{0\to 2}\,|0\rangle-(-1)^{g_{m_1}\cdot g_{m_2}}O(m_2)U_2O(m_1)U_1\,|0\rangle\,\|^2\\
&-\Theta(\varepsilon)-\sum_{F,q',u}\Theta\Big(1-\Pr[\text{ validity check passes }\mid F,q',u,D\,]\Big).
\end{aligned}$$

因此，

$$\begin{aligned}
&\mathop{\mathbb{E}}_{(m_1,m_2)\sim D}\|O'_1(m_1)O(m_2)U_{0\to 2}\,|0\rangle-(-1)^{g_{m_1}\cdot g_{m_2}}O(m_2)U_2O(m_1)U_1\,|0\rangle\,\|^2\\
\leq\;&4(1-\Pr[\text{ anti-commuting test passes }\mid D])\\
&+\Theta(\varepsilon)+\sum_{F,q',u}\Theta\Big(1-\Pr[\text{ validity check passes }\mid F,q',u,D\,]\Big).
\end{aligned}$$

□

以下引理将在证明定理7.34的可靠性时发挥重要作用。

引理 7.47。设

$$\rho=U_{0\to 2}\,|00\rangle_{\mathsf{PRD}}\,\langle 00|_{\mathsf{PRD}}\,U_{0\to 2}^{\dagger}.$$

Then

$$\begin{aligned}
&\mathop{\mathbb{E}}_{(a,b)\sim D}\|O'_1(a)O'_2(b)-(-1)^{a\cdot b}O'_2(b)O'_1(a)\|_\rho^2\\
\leq\;&\sum_{M,F}\Theta(1-\Pr[\textit{ consistency check passes }\mid M,F,D])\\
&+\Theta(1-\Pr[\textit{ anti-commuting test passes }\mid D])\\
&+\sum_{F,q',u}\Theta(1-\Pr[\textit{ validity check passes }\mid F,q',u,D\,])+\Theta(\varepsilon).
\end{aligned}$$

证明。 我们有，

$$\begin{aligned}
&\mathop{\mathbb{E}}_{(a,b)\sim D}\|O'_1(a)O'_2(b)-(-1)^{a\cdot b}O'_2(b)O'_1(a)\|_\rho^2\\
=\;&\mathop{\mathbb{E}}_{(a,b)\sim D}\langle 00|_{\mathsf{PRD}}\,U_{0\to 2}^{\dagger}(h.c.)\cdot(O'_1(a)O'_2(b)-(-1)^{a\cdot b}O'_2(b)O'_1(a))U_{0\to 2}\,|00\rangle_{\mathsf{PRD}}\\
=\;&\mathop{\mathbb{E}}_{(a,b)\sim D}\|O'_1(a)O'_2(b)U_{0\to 2}\,|00\rangle_{\mathsf{PRD}}-(-1)^{a\cdot b}O'_2(b)O'_1(a)U_{0\to 2}\,|00\rangle_{\mathsf{PRD}}\,\|^2.
\end{aligned}$$

我们用 $|\alpha(a,\ b)\rangle\approx_{\delta,\ D}|\beta(a,\ b)\rangle$ 表示 $\mathbb{E}_{(a,b)\sim D}\|\,|\alpha(a,\ b)\rangle-|\beta(a,\ b)\rangle\,\|^2\leq\Theta(\delta)$。根据引理 7.37、7.45和 7.46，我们得到以下关系：

$$O'_1(a)O'_2(b)U_{0\to 2}\,|0\rangle$$

$$
\begin{aligned}
&\approx_{\delta,D} O_1'(a)O(b)U_2U_1\left|0\right\rangle \\
&\approx_{\delta,D} (-1)^{a\cdot b}O(b)U_2O(a)U_1\left|0\right\rangle \\
&\approx_{\delta,D} (-1)^{a\cdot b}O_2'(b)U_2O(a)U_1\left|0\right\rangle \\
&\approx_{\delta,D} (-1)^{a\cdot b}O_2'(b)O_1'(a)U_{0\to 2}\left|0\right\rangle .
\end{aligned}
$$

因此，

$$
\mathop{\mathbb{E}}_{(a,b)\sim D}\|O_1'(a)O_2'(b)U_{0\to 2}\left|00\right\rangle_{\mathsf{PRD}}-(-1)^{a\cdot b}O_2'(b)O_1'(a)U_{0\to 2}\left|00\right\rangle_{\mathsf{PRD}}\|^2\le\Theta(\delta).
$$

□

以下引理将有助于证明定理7.34的完备性。

引理 7.48（规范证明者形式下的诚实证明者）。令

$$
R_1=\prod_{p\in[n]}P((Z(g_p))_{\mathsf{P}},\mathsf{R}_p),R_2=\prod_{p\in[n]}P((X(g_p))_{\mathsf{P}},\mathsf{R}_p).
$$

定义 *7.12* 中的证明者是定义 *7.24* 中的证明者，并满足：

$$
\begin{aligned}
U_1&=R_1,\\
U_2&=R_2\cdot R_1^{-1},\\
U_1'&=R_1\cdot R_2^{-1},\\
U_2'&=I.
\end{aligned}
$$

证明。这个引理可通过直接计算得出。 □

引理 7.49（诚实证明者的性质）。对于 $i\in[2]$，令 U_i 如引理 *7.48*中所定义。对于 $q'\in[2]$，令 $U_{q'}'$ 如引理 *7.48* 中所定义。那么：

- 对于任意 $u\in[2]$,

$$
\widetilde{O}_{u,j}'U_{u\to 2}=U_{u\to 2}\widetilde{O}_j.
$$

- 此外，

$$
\widetilde{O}_{1,j_1}'\widetilde{O}_{j_2}U_2=(-1)^{g_{j_1}\cdot g_{j_2}}\widetilde{O}_{j_2}U_2\widetilde{O}_{j_1}
$$

证明。设 R_i 定义如引理7.48所示。

第一部分： 只需证明

$$
R_2^{-1}\widetilde{O}_{u,j}'R_2=R_u^{-1}\widetilde{O}_jR_u,
$$

这可以由.....推出

$$
\begin{aligned}
R_2^{-1}\widetilde{O}_{1,j}'R_2&=(Z(g_j))_{\mathsf{P}},\\
R_2^{-1}\widetilde{O}_{2,j}'R_2&=(X(g_j))_{\mathsf{P}},
\end{aligned}
$$

and

$$R_1^{-1}\widetilde{O}_j R_1 = (Z(g_j))_{\mathsf{P}},$$
$$R_2^{-1}\widetilde{O}_j R_2 = (X(g_j))_{\mathsf{P}}.$$

第二部分： 只需证明

$$R_1^{-1}\widetilde{O}_{j_1}R_1 R_2^{-1}\widetilde{O}_{j_2}R_2 = (-1)^{g_{j_1}\cdot g_{j_2}} R_2^{-1}\widetilde{O}_{j_2}R_2 R_1^{-1}\widetilde{O}_{j_1}R_1,$$

由此可得

$$(Z(g_{j_1}))_{\mathsf{P}}(X(g_{j_2}))_{\mathsf{P}} = (-1)^{g_{j_1}\cdot g_{j_2}}(X(g_{j_2}))_{\mathsf{P}}(Z(g_{j_1}))_{\mathsf{P}}.$$

□

定理 7.34 的证明。

完备性： 对于 $i \in [2]$，令 U_i 如引理 7.48中所定义。对于 $q' \in [2]$，令 $U'_{q'}$ 如引理 7.48中所定义。令 D 为 M 的抽样分布，F 如定义 7.17中所述。

根据定义 7.12 和定义 7.23，验证者的有效性检查以概率 **1** 通过。

按照引理 7.45 的证明，

$$\Pr[\text{ consistency check passes } \mid M, F] = 1 - \mathop{\mathbb{E}}_{(f_1,f_2)\sim D} \frac{\| U_{u\to 2}\widetilde{O}_{m_u}\widetilde{U}_{u,F,f}\,|0\rangle - \widetilde{O}'_{u,m_u}\widetilde{U}_{2,F,f}\,|0\rangle\,\|^2}{4}.$$

按照引理7.46 的证明，

$$\Pr[\text{ anti-commuting test passes }] = 1 - \mathop{\mathbb{E}}_{(m_1,m_2)\sim D} \frac{\| \widetilde{O}'_{1,m_1}\widetilde{O}_{m_2}U_{0\to 2}\,|0\rangle - (-1)^{g_{m_1}\cdot g_{m_2}}\widetilde{O}_{m_2}U_2\widetilde{O}_{m_1}U_1\,|0\rangle\,\|^2}{4}$$

因此，根据引理 7.37，我们只需证明对于任意 M，$F \in \{0,1\}^2$ 属于 D的支撑集，令 $M_u = 1$，

$$\widetilde{O}'_{u,m_u}U_{u\to 2} = U_{u\to 2}\widetilde{O}_{m_u},$$

and

$$\widetilde{O}'_{1,m_1}\widetilde{O}_{m_2}U_{0\to 2} = (-1)^{g_{m_1}\cdot g_{m_2}}\widetilde{O}_{m_2}U_2\widetilde{O}_{m_1}U_1.$$

这两部分均可直接由引理7.49得出。

可靠性： 可靠性可由引理 7.47得出。 □

8 强量子对数深度诚实证明者交互式预言机证明

本节将给出强量子交互式预言机证明的完整构造。除了第 7 节介绍的多量子比特测试外，我们还将介绍能量测试和能量一致性测试。此外，为了表述清晰，我们将泡利测量部分与能量一致性测试分开。

总体思路如下：验证者从放大的克利福德哈密顿量中随机抽取一个项，并指示证明者按照该项进行测量。然而，证明者可能不会遵循诚实策略，因此我们必须使证明者的测量策略与

一个已知与诚实策略接近的参照相关联；这通过多量子比特测试来实现。

请注意，5-局域Clifford投影本身并不是泡利测量。为了解决这个问题，我们将每个投影分解为 5-局域泡利测量。由于哈密顿量作用于N 份原始见证的副本，诚实证明者将获得 $5N$ 个测量结果。由于验证者无法读取所有 $5N$ 个比特，我们采用第6节中的方法，使用 PCPP 证明来验证这些测量结果是否会使验证者接受。

为了测试这 $5N$ 个结果是否正确，我们从相等性测试 [BK97]中汲取灵感。具体而言，我们计算这 $5N$比特串与一个随机掩码的内积。对于诚实证明者，该内积对应于一个泡利测量，其测量算符是按照随机掩码选取的 $5N$ 个局部泡利算符相乘所得。如果这 $5N$ 个单独结果中有任何一个偏离诚实测量结果，那么所得内积就不太可能与复合泡利可观测量的实际测量结果相符。可以通过多量子比特测试获得这一复合测量。

为了获得泡利测量，我们不使用多量子比特测试中由第三轮交互导出的可观测量，而是依赖证明者在前两轮中的消息：在 Z 基下的纯化测量结果，以及在 X 基下的纯化测量结果。测量一个可观测量等价于对处于 $|+\rangle$ 态的控制量子比特应用受控可观测量，并在哈达玛基下测量该控制量子比特。要测量形如 $X(a)Z(b)Y(c)$的可观测量，我们将第一轮中的受控-$Z(b+c)$、第二轮中的受控-$X(a+c)$结合起来，并由验证者直接施加相位因子 i^c 。我们注意到，我们测量 Y可观测量的方法明显比先前工作（例如 [CGJV19]）中使用的方法简单。

定理 8.1 (定理 8.17 的重述)。 $\mathsf{QMA} \subseteq \mathsf{SQIOP}(O(1)\ O(\exp\circ\mathrm{poly})\ O(1))$。

注 8.2。 对于诚实证明者而言，量子电路可以以对数深度实现。在多量子比特测试中，证明者在 Z 或 X 基下对其见证执行纯化测量。在这两种基之间切换只需要一层哈达玛门。利用无界扇出 *CNOT* 门，可以在计算基下将见证复制指数次。随后，对每个副本与相应的索引计算内积，从而得到见证的哈达玛码编码。这一计算中最深的部分是内积计算，仅需对数深度。

强量子 *IOP* 协议基于这一多量子比特测试。在能量一致性测试中，证明者进行泡利测量的行为与多量子比特测试中的行为一致。能量测试要求对见证进行测量，而该见证由原始见证的 N 个副本组成。每个副本都使用局部克利福德投影进行测量，该投影同样具有常数深度。

能量一致性测试的其他组成部分包括为与随机掩码的内积提供 *PCPP* 证明。同样，在能量测试中，证明者提供测量结果的纠错编码，并附上 *PCPP* 证明，使验证者信服并接受。这些步骤是经典的，因此不考虑其计算复杂度（多项式时间之外的部分）。

本节安排如下。在第 8.1 节中，我们介绍一种构造，使验证者能够执行泡利测量，同时证明者的行为与多量子比特测试中的完全相同。这构成了能量一致性测试的一个组成部分，该测试用于检验能量测试中使用的测量是否与多量子比特测试中的测量相匹配。第 8.2 节介绍验证者和诚实证明者在能量测试及能量一致性测试中的完整构造与行为。在第8.3节中，我们以不失一般性的形式描述恶意证明者的总体策略。最后，在第 8.4 节中，我们证明本节的主定理。

8.1 泡利基中的测量

我们定义验证者测量形如 $X(a)Z(b)Y(c)$ 的可观测量时所采用的策略。首先，我们描述验证者在协议前两轮中的一般操作，不指定参数。然后，我们详细说明验证者如何实例化这一模板，以实现对 $X(a)Z(b)Y(c)$ 的测量。

定义 8.3 (前两轮测量的验证者操作模板)。 设$\mathsf{R}=(\mathsf{R}j)^{j\in[n]}$ 为一个寄存器。设 S 为验证者持有的一个寄存器，并初始化为 $|0\rangle$。设 M 为验证者持有的一个寄存器。设 T_S 为验证者持有的一个寄存器，并初始化为 $H^{\otimes l_\mathsf{S}}|0\rangle$。 ~设 $m\in[n]$。设 $O_{m,}$ SRT_S 定义如定义 7.13。

- 证明者的第一步： 证明者向验证者发送寄存器 R。
- 验证者的第一步： 验证者从证明者处接收寄存器 R 。验证者~测量 T_S。然后，验证者应用 $C(O_{m,\mathsf{SRT}_\mathsf{S}},\mathsf{M})$。验证者向证明者发送寄存器 R。
- 证明者的第二步： 证明者从验证者处接收寄存器 R 。

定义 8.4 (测量 $X(a)Z(b)Y(c)$)。 设 $a,b,c\in\{0,1\}^k$，使得 $a\cap b=b\cap c=c\cap a=\emptyset$。令 $\mathsf{R}=(\mathsf{R}j)^{j\in[n]}$ 为一个寄存器。令 S 为验证者持有并初始化为 $|0\rangle$的寄存器。令M 为验证者持有并初始化为 $|+\rangle$的寄存器。令 $\mathsf{T}_{\mathsf{S},\mathsf{i}}$ 对于 $i\in[3]$ 为验证者持有并初始化为 $H^{\otimes l_\mathsf{S}}|0\rangle$的寄存器。验证者操作定义如下：

- 验证者设置 $m_1=b+c,m_2=a+c$。
- 验证者重复定义 7.15 中的验证者操作两次。在 i次中，验证者按照定义 7.15 执行，其中 $m=m_i$。
- 最后，验证者将相位门 $|c|$ 次应用于 $S^{|c|}$ M。然后，验证者应用H_M，在 Z_M下测量寄存器M ，并输出测量结果。

8.2 能量测试和能量一致性测试

本节将介绍验证者和证明者在能量测试与能量一致性测试中的操作。

在执行能量测试时，验证者首先向证明者发送索引 $l_i\in[m]$，用于 $i\in[N]$，这些索引对应于验证者希望测试的哈密顿量项。诚实证明者应返回所有可观测量 $O_{l_i,j}$ 对于 $i\in[N]$, $j\in[5]$ 的测量结果，并附上 PCPP 证明，以证明这些结果将使验证者接受。

然而，由于证明者可能并不诚实，因此引入能量一致性测试来确保完整性。在此测试中，验证者随机抽取一个二进制掩码，而证明者应计算测量结果与该掩码之间的内积。在经典情况下，即使只有一个报告的结果不正确，整个内积出错的概率也恰好为 $1/2$。

重要的是，验证者可以直接将这个内积测量为一个泡利可观测量，因为它对应于掩码下所有 $O_{l_i,j}$ 与 l_i,j 的乘积。这项测量可以在协议的前两轮中完成，使验证者能够将结果与证明者声称的值进行比较。

本节首先回顾相关的 PCPP 构造，然后介绍诚实证明者和验证者在两项测试中的策略。

定义 8.5（能量测试和能量一致性测试，诚实证明者在最后一轮的操作）。设 P 是一个包含 k 个量子比特的寄存器。设 p，q 如定理 *4.10*所述，s，N 如引理 *4.11*所述。使用定义 H、$O_{i,j}$ 以及 $a_{i,j}$、$b_{i,j}$、$c_{i,j}$ 中的 *7.22* 记号。设

$$C(x) = \bigoplus_{i\in[N]} (1 \oplus \bigvee_{j\in[5]} x_{i,j}),$$

其中 $x = (x_{i,j})_{i\in[N],\, j\in[5]}$。设 E 为定理 *6.5*中各码的编码电路，D 为定理 *6.5*中各码的解码电路，以及 T 为定理 *6.5*中各码的码测试器电路。

- 验证者向证明者发送 $l_i \in [m]$，用于 $i \in [N]$。
- 对于 $i \in [N]$，$j \in [5]$，诚实证明者在可观测量下测量P

$$\underbrace{I \otimes I \otimes \cdots \otimes I}_{i-1} \otimes O_{l_i,j} \otimes \underbrace{I \otimes I \otimes \cdots \otimes I}_{N-i},$$

，并将测量结果存储在 $r_{i,j}$ 中。设

$$r = (r_{i,j})_{i\in[N],j\in[5]}.$$

- 诚实证明者向验证者发送 $E(r)$、$C(r)$以及 w，其中 w 是一个见证，使得定理*4.14*中的验证者在显式输入电路 $C(D(\cdot))+C(r)+1$以及隐式输入电路的输入 $E(r)$ 时，接受 *PCPP* 见证 w。
- 验证者向证明者发送 $t \in_R \mathbb{F}_2^{5N}$。
- 设 $C'(r) = r \cdot t$。证明者向验证者发送 $C'(r)$ 和 w'，其中 w' 是一个见证，使得定理 ***4.14*** 中的验证者在显式输入 $V(C'(D(\cdot)) + C'(r) + 1)$ 和隐式输入 $E(r)$ 的情况下，接受见证 w'。

注记 8.6。如果 $C(D(e')) + r' + 1 = 1$，也就是说，若 $C(D(e')) = r'$，那么验证者使用显式输入、电路 $C(D(\cdot)) + r' + 1$，以及隐式输入（即电路的输入）e'和 *PCPP* 见证 w，以概率1 接受。

定义 8.7（能量测试和能量一致性测试，诚实证明者）。诚实证明者的操作定义如下：

- 诚实证明者在前两轮中按照定义 *7.12* 进行操作。
- 验证者向证明者发送符号“能量测试”或“量子比特测试”。
- 如果符号是“量子比特测试”，诚实证明者继续按照定义 *7.12*进行操作。如果符号是“能量测试”，诚实证明者按照定义 *8.5*进行操作。

定义 8.8（能量测试和能量一致性测试，最后一轮中的验证者操作）。设 c，$e \in \{0,1\}$。设 $t \in \mathbb{F}_2^{5N}$。设 $l_i \in [m]$ 对于 $i \in [N]$。设 E 为定理 *6.5* 中码的编码电路，D 为定理 *6.5* 中码的解码电路，T 为定理 *6.5* 中码的码测试器电路。

- 验证者向证明者发送 $l_i \in [m]$，用于 $i \in [N]$。
- 证明者向验证者发送 M, o, w：*PCPP* 的隐式输入、应为 $C(D(M))$ 的值（该值也用于构建 *PCPP* 的显式输入），以及 *PCPP* 的见证。
- 当且仅当 $a_1 = 1$ 时，验证者设置 $o = 0$，并且定理 *4.14*中的验证者在运行固定次数后，每次都接受以下参数：显式输入$x = C(D(\cdot)) + o + 1 \wedge T(\cdot)$、隐式输入 $y = M$、*PCPP* 证明 $\pi = w$。
- 验证者向证明者发送 t。
- 证明者向验证者发送 o'，w'。当且仅当 $a_2 = 1$ 时，验证者设置 $o' = e$，并且定理 *4.14*中的验证者在运行固定次数后，每次都接受以下参数：$x = C'(D(\cdot)) + o' + 1 \wedge T(\cdot)$、$y = M$、$\pi = w'$。
- 如果 $c = 0$，验证者接受当且仅当 $a_1 = 1$。如果 $c = 1$，验证者接受当且仅当 $a_2 = 1$。

定义 8.9（能量测试与能量一致性测试，验证者）。令 p，q 如定理*4.10*中所述，s，N 如引理*4.11*中所述。令 H，H_i和 $O_{i,\,j}$ 如定义 *8.5*中所述。验证者操作定义如下：

1. 验证者采样 $t \in_R \mathbb{F}_2^{5N}$并采样 $l_i \in_R [m]$，用于 $i \in [N]$。令

$$O = \prod_{i \in [N], j \in [5]} O_{l_{i,j}}^{t_{i,j}},$$

采用泡利表示

$$O = (-1)^d X(a) Z(b) Y(c).$$

2.（量子比特测试：）以概率 $1/3$，验证者按照定义 *7.23* 操作，并在前两轮结束后向证明者发送符号“量子比特测试”。

3.（能量测试：）以概率 $1/3$，验证者重复执行定义*7.15* 中的验证者操作 2 次。每次，验证者按照定义 *7.15* 进行操作，其中 $M = 0$，$F = 0$，$m = 0$，$f = 0$。最后，验证者向证明者发送符号“能量测试”，并按照定义 *8.8* 进行操作，其中 $c = 0$，$e = 0$。

4.（能量一致性测试：）以概率 $1/3$，验证者按照定义*8.4*进行操作，其中 $a = a$，$b = b$，$c = c$。令 e 为输出。最后，验证者向证明者发送符号“能量测试”，并按照定义*8.8*进行操作，其中 $c = 1$，$e = e + d$，$t = t$，$l_i = l_i$ 对于$i \in [N]$。

8.3 一般证明者的操作

为了陈述本节的主要定理，我们首先介绍恶意证明者的行为 .

定义 8.10（能量测试，规范证明者操作）。设 P 是一个寄存器。设 $h = |E(1^{5N})|$ 为定理 *6.5*中各码的编码电路的输出长度。令 g 表示

定理 4.14 中验证者使用的见证长度，其中电路的输入规模为 h。对于$l \in [m]^N$，令 $P_l = \{P_{l,M,o,w}\}_{M\in\mathbb{F}_2^h,\ o\in\mathbb{F}_2,\ w\in\mathbb{F}_2^g}$为作用于 P 上的投影测量。

典　　型证明者在能量测试最后一轮中的操作定义如下　　：

- 验证者的第一步：验证者向证明者发送 $l_i \in [m]$，用于 $i \in [N]$。
- 证明者的第一步：证明者根据 P_l, P进行测量。证明者将测量结果 M 和 o, w发送给验证者。
- 验证者的第二步：验证者向证明者发送 $t \in \mathbb{F}_2^{5N}$。
- 证明者的第二步：证明者向验证者发送 o'，w'。

8.4 主定理

引理 8.11（能量一致性测试的推论）。 设

$$P'_{l,t} = \sum_{M,o,w} 1_{D(M)\cdot t=0} P_{l,M,o,w} - \sum_{M,o,w} 1_{D(M)\cdot t=1} P_{l,M,o,w}.$$

对于任意 M, F, D, u, q',

$$\begin{aligned}\Pr[\ \textit{consistency check passes}\ \mid M, F, D] &\geq 1-\varepsilon'\\ \Pr[\ \textit{validity check passes}\ \mid F, q', u, D\ ] &\geq 1-\varepsilon'\\ \Pr[\ \textit{anti-commuting test passes}\ \mid D] &\geq 1-\varepsilon'.\end{aligned}$$

Then

$$\begin{aligned}&\mathop{\mathbb{E}}_{l\in[m]^N, t\in\mathbb{F}_2^{5N}} \|(P'_{l,t} - V^\dagger((-1)^d \cdot X(a)Z(b)Y(c)\otimes I)V)U_{0\to 2}\,|0\rangle\,\|^2\\ &\leq \Theta(\varepsilon+\delta+\varepsilon'),\end{aligned}$$

其中 a，b，c，d 的定义见定义 8.9，ε 是定理 7.1中的自校正参数，且 δ 是定理 4.14中的 *PCPP* 接近参数。

证明。 由引理 7.45,

$$\mathbb{E}\,\|O(a+c)U_2O(b+c)U_1\,|0\rangle - O'_2(a+c)U_2O(b+c)U_1\,|0\rangle\,\|^2 \leq \Theta(\varepsilon+\varepsilon'),$$

and

$$\mathbb{E}\,\|O'_2(a+c)U_2O(b+c)U_1\,|0\rangle - O'_2(a+c)O'_1(b+c)U_2U_1\,|0\rangle\,\|^2 \leq \Theta(\varepsilon+\varepsilon').$$

由引理 7.42,

$$\mathbb{E}\,\|O(a+c)U_2O(b+c)U_1\,|0\rangle - \widetilde{O}_{a+c}U_2\widetilde{O}_{b+c}U_1\,|0\rangle\,\|^2 \leq \Theta(\varepsilon+\varepsilon').$$

因此，通过结合上述三个不等式和三角不等式

$$\mathbb{E}\,\|O'_2(a+c)O'_1(b+c)U_2U_1\,|0\rangle - \widetilde{O}_{a+c}U_2\widetilde{O}_{b+c}U_1\,|0\rangle\,\|^2 \leq \Theta(\varepsilon+\varepsilon')\ . \tag{6}$$

为了分析能量一致性测试，请注意，根据定义8.4 和定义8.9，在能量一致性测试期间，验证者首先测量 $X(a)Z(b)Y(c)$，并利用前两个轮次。在证明的其余部分，我们不使用 e，而使用 s 来表示测量结果。

$$\begin{aligned}
&\frac{1}{\sqrt{2}}(U_2U_1\left|+\right\rangle_{\mathsf{M}}\left|0\right\rangle+\mathbf{i}^c\cdot\widetilde{O}_{a+c}U_2\widetilde{O}_{b+c}U_1\left|-\right\rangle_{\mathsf{M}}\left|0\right\rangle)\\
&\qquad=\frac{1}{2}(U_2U_1\left|0\right\rangle+\mathbf{i}^c\cdot\widetilde{O}_{a+c}U_2\widetilde{O}_{b+c}U_1\left|0\right\rangle)\left|0\right\rangle_{\mathsf{M}}\\
&\qquad\quad+\frac{1}{2}(U_2U_1\left|0\right\rangle-\mathbf{i}^c\cdot\widetilde{O}_{a+c}U_2\widetilde{O}_{b+c}U_1\left|0\right\rangle)\left|1\right\rangle_{\mathsf{M}}.
\end{aligned}$$

我们有

$\mathbf{Pr}$[能量一致性测试通过]

$$\begin{aligned}
&=\mathop{\mathbb{E}}_{\substack{l\in[m]^N\\t\in\mathbb{F}_2^{5N}}}\sum_{\substack{s\in\mathbb{F}_2\\M,o,w}}\Pr[\text{verifier accepts}|l,t,M,o',w']\cdot\left\|P_{l,M,o,w}\frac{U_2U_1\left|0\right\rangle+(-1)^s\mathbf{i}^c\cdot\widetilde{O}_{a+c}U_2\widetilde{O}_{b+c}U_1\left|0\right\rangle}{2}\right\|^2\\
&\le\mathop{\mathbb{E}}_{\substack{l\in[m]^N\\t\in\mathbb{F}_2^{5N}}}\sum_{\substack{s\in\mathbb{F}_2\\M,o,w}}\Pr[\text{verifier accepts}|l,t,M,o',w']\\
&\qquad\cdot\left\|P_{l,M,o,w}\frac{U_2U_1\left|0\right\rangle+(-1)^s\mathbf{i}^c\cdot O_2'(a+c)O_1'(b+c)U_2U_1\left|0\right\rangle}{2}\right\|^2+\Theta(\varepsilon+\delta)\,,
\end{aligned}\tag{7}$$

其中最后一步由（6）得出。

设 $S=\{x|C'(D(x))=s+d\wedge T(x)=1\}$。若 $dist(M,\ S)>\delta$,

$$\Pr[a_2=1|l,t,M,o',w']\le\Pr[\text{verifier accepts}|l,t,M,o'=s+d,w']\le\varepsilon.$$

如果 $dist(M,\ S)\le\delta$,

$$\Pr[a_2=1|l,t,M,o',w']\le1=1_{C'(D(M))=s+d}.$$

因此,

$$\Pr[\text{verifier accepts}|l,t,M,o',w']\le1_{D(M)\cdot t=s+d}+\varepsilon.$$

代回（7），

$\mathbf{Pr}$[能量一致性测试通过] $\le\Theta(\varepsilon+\delta)$

$$+E_{\substack{l\in[m]^N\\t\in\mathbb{F}_2^{5N}}}\sum_{\substack{s\in\mathbb{F}_2\\M,o,w}}\left\|(\sum_{M,o,w}1_{D(M)\cdot t=s}P_{l,M,o,w})\frac{I+(-1)^{d+s}\cdot\mathbf{i}^c\cdot O_2'(a+c)O_1'(b+c)}{2}U_{0\to2}\left|0\right\rangle\right\|^2.\tag{8}$$

Let

$$P'_{l,t}=\sum_{M,o,w}1_{D(M)\cdot t=0}P_{l,M,o,w}-\sum_{M,o,w}1_{D(M)\cdot t=1}P_{l,M,o,w}$$

对于任意矩阵 R,

$$\sum_{s\in\mathbb{F}_2}\left\|\frac{I+(-1)^sP'_{l,t}}{2}\cdot\frac{I+(-1)^sR}{2}U_{0\to2}\left|0\right\rangle\right\|^2=1-\frac{1}{4}\left\|P'_{l,t}U_{0\to2}\left|0\right\rangle-RU_{0\to2}\left|0\right\rangle\right\|^2,$$

因此，通过取

$$R = (-1)^d \cdot \mathbf{i}^c \cdot O_2'(a+c)O_1'(b+c),$$

以及公式（8），我们有

$$\begin{aligned}&\mathop{\mathbb{E}}_{l\in[m]^N, t\in\mathbb{F}_2^{5N}} \left\|(P'_{l,t} - (-1)^d \cdot \mathbf{i}^c \cdot O_2'(a+c)O_1'(b+c))U_{0\to 2}\left|0\right\rangle\right\|^2 \\ &\leq \Theta(1 - \Pr[\text{energy consistency test passes}]) + \Theta(\varepsilon+\delta). \end{aligned} \tag{9}$$

此外，根据引理 7.47 和定义 7.30，我们可以应用定理 4.23，

$$\mathbb{E}\left\|(-1)^d \cdot \mathbf{i}^c \cdot O_2'(a+c)O_1'(b+c)U_{0\to 2}\left|0\right\rangle - V^\dagger((-1)^d \cdot X(a)Z(b)Y(c)\otimes I)VU_{0\to 2}\left|0\right\rangle\right\|^2 \leq \Theta(\delta). \tag{10}$$

由公式（9）和公式（10）可得，

$$\begin{aligned}&\mathop{\mathbb{E}}_{l\in[m]^N, t\in\mathbb{F}_2^{5N}} \left\|(P'_{l,t} - V^\dagger((-1)^d \cdot X(a)Z(b)Y(c)\otimes I)V)U_{0\to 2}\left|0\right\rangle\right\|^2 \\ &\leq \Theta(\varepsilon+\delta+\varepsilon').\end{aligned}$$

□

下面的引理是通过随机掩码实现的经典内积相等性测试的量子类比。

引理 8.12（使用随机掩码的影响）。设 $d' > d$。设 $\{P_s\}_{s\in\mathbb{F}_2^n}$ 是 $\mathbb{C}^d$ 上的正交投影测量。设 O_i 是 $\mathbb{C}^{d'}$ 上关于 $i \in [n]$ 的可观测量。设 $V:\ \mathbb{C}^d \to \mathbb{C}^{d'}$ 是一个等距映射。对于 $t \in \mathbb{F}_2^n$，令

$$O^{(t)} = \prod O_i^{t_i}.$$

此外，令

$$P^{(t)} = \sum_s (-1)^{st} \cdot P_s.$$

Then

$$\sum_s \left\|P_s - V^\dagger \prod_{i\in[n]} \frac{I + (-1)^{s_i} O_i}{2} V\right\|_\rho^2 \leq \mathop{\mathbb{E}}_t \|P^{(t)} - V^\dagger O^{(t)} V\|_\rho^2 + 1 - \mathop{\mathbb{E}}_t \|V^\dagger O^{(t)} V\|_\rho^2.$$

证明。注意

$$\begin{aligned}\mathop{\mathbb{E}}_t \|P^{(t)} - V^\dagger O^{(t)} V\|_\rho^2 &= 1 + \mathop{\mathbb{E}}_t \operatorname{tr}(V^\dagger O^{(t)} V V^\dagger O^{(t)} V \rho) - 2\mathop{\mathbb{E}}_t \Re(\operatorname{tr}((P^{(t)})^\dagger V^\dagger O^{(t)} V\rho)) \\ &= 1 + \mathop{\mathbb{E}}_t \|V^\dagger O^{(t)} V\|_\rho^2 - 2\mathop{\mathbb{E}}_t \sum_s \Re(\operatorname{tr}(((-1)^{st} \cdot P_s)^\dagger V^\dagger O^{(t)} V\rho)) \,. \end{aligned} \tag{11}$$

此外，

$$\sum_s \left\|P_s - V^\dagger \prod_{i\in[n]} \frac{I + (-1)^{s_i} O_i}{2} V\right\|_\rho^2$$

$$
\begin{aligned}
&= \sum_s \mathrm{tr}(P_s\rho) + \sum_s \mathrm{tr}(V^\dagger \prod_{i\in[n]} \frac{I+(-1)^{s_i}O_i}{2} VV^\dagger \prod_{i\in[n]} \frac{I+(-1)^{s_i}O_i}{2} V\rho) \\
&\quad - 2\sum_s \Re(\mathrm{tr}(P_s^\dagger V^\dagger \prod_{i\in[n]} \frac{I+(-1)^{s_i}O_i}{2} V\rho)) \\
&\le 2 - 2\sum_s \Re(\mathrm{tr}(P_s^\dagger V^\dagger \prod_{i\in[n]} \frac{I+(-1)^{s_i}O_i}{2} V\rho)) \,, \qquad (12)
\end{aligned}
$$

其中，中间项的界是利用 V 是等距映射这一事实得到的。此外，

$$
\prod_{i\in[n]} \frac{I+(-1)^{s_i}O_i}{2} = \frac{1}{2^n}\sum_{t\in\mathbb{F}_2^n}\prod_i O_i^{t_i}(-1)^{s_i t_i} = \mathop{\mathbb{E}}_t (-1)^{st} O^{(t)}.
$$

因此，代回式（12），

$$
\begin{aligned}
&\sum_s \|P_s - V^\dagger \prod_{i\in[n]} \frac{I+(-1)^{s_i}O_i}{2} V\|_\rho^2 \\
&\le 2 - 2\mathop{\mathbb{E}}_t \sum_s \Re(\mathrm{tr}(P_s^\dagger (-1)^{st} V^\dagger O^{(t)} V\rho)) \\
&\le \mathop{\mathbb{E}}_t \|P^{(t)} - V^\dagger O^{(t)} V\|_\rho^2 + 1 - \mathop{\mathbb{E}}_t \|V^\dagger O^{(t)} V\|_\rho^2 \,,
\end{aligned}
$$

其中第二个不等式由式（11）得到。 □

引理 8.13（能量一致性测试的进一步推论）。

$$
\mathop{\mathbb{E}}_l \sum_s \Big\| \sum_{M,o,w} 1_{D(M)=s} P_{l,M,o,w} - V^\dagger \prod_{i\in[n]} \frac{I+(-1)^{s_i}O_{i,j}}{2} V \Big\|_\rho^2 \le \Theta(\sqrt{\varepsilon+\varepsilon'+\delta}) \,.
$$

证明。令

$$
P'_{l,t} = \sum_{M,o,w} 1_{D(M)\cdot t=0} P_{l,M,o,w} - \sum_{M,o,w} 1_{D(M)\cdot t=1} P_{l,M,o,w}.
$$

根据引理 8.12，取

$$
\begin{aligned}
n &= 5N, \\
P_s &= \sum_{M,o,w} 1_{D(M)=s} P_{l,M,o,w}, \\
O_{i,j} &= (-1)^{d_{l_i,j}} X(a_{l_i,j}) Z(b_{l_i,j}) Y(c_{l_i,j}),
\end{aligned}
$$

我们有

$$
\begin{aligned}
&\sum_s \Big\| \sum_{M,o,w} 1_{D(M)=s} P_{l,M,o,w} - V^\dagger \prod_{i\in[N],j\in[5]} \frac{I+(-1)^{s_{i,j}}O_{l_i,j}}{2} V \Big\|_\rho^2 \\
&\qquad \le \mathop{\mathbb{E}}_t \|P'_{l,t} - V^\dagger O(t,l) V\|_\rho^2 + 1 - \mathop{\mathbb{E}}_t \|V^\dagger O(t,l) V\|_\rho^2 \,. \qquad (13)
\end{aligned}
$$

根据引理 8.11，

$$
\mathop{\mathbb{E}}_l \mathop{\mathbb{E}}_t \|P'_{l,t} - V^\dagger O(t,l) V\|_\rho^2 \le \Theta(\varepsilon+\delta+\varepsilon').
$$

注意，根据引理 4.17，

$$\begin{aligned}
&\mathop{\mathbb{E}}_{l}\mathop{\mathbb{E}}_{t}\|V^\dagger O(t,l)V\|_\rho \\
\geq\ &\mathop{\mathbb{E}}_{l}\mathop{\mathbb{E}}_{t}\|P'_{l,t}\|_\rho - \mathop{\mathbb{E}}_{l}\mathop{\mathbb{E}}_{t}\|P'_{l,t} - V^\dagger O(t,l)V\|_\rho \\
=\ &1 - \mathop{\mathbb{E}}_{l}\mathop{\mathbb{E}}_{t}\|P'_{l,t} - V^\dagger O(t,l)V\|_\rho \\
\geq\ &1 - \sqrt{\mathop{\mathbb{E}}_{l}\mathop{\mathbb{E}}_{t}\|P'_{l,t} - V^\dagger O(t,l)V\|_\rho^2} \\
\geq\ &1 - \Theta(\sqrt{\varepsilon+\varepsilon'+\delta}).
\end{aligned}$$

因此，

$$\begin{aligned}
&\mathop{\mathbb{E}}_{l}\mathop{\mathbb{E}}_{t}\|V^\dagger O(t,l)V\|_\rho^2 \\
\geq\ &(\mathop{\mathbb{E}}_{l}\mathop{\mathbb{E}}_{t}\|V^\dagger O(t,l)V\|_\rho)^2 \\
\geq\ &(1 - \Theta(\sqrt{\varepsilon+\varepsilon'+\delta}))^2 \\
\geq\ &1 - \Theta(\sqrt{\varepsilon+\varepsilon'+\delta}).
\end{aligned}$$

代回（13）中，

$$\mathop{\mathbb{E}}_{l}\sum_{s}\Big\|\sum_{M,o,w}1_{D(M)=s}P_{l,M,o,w} - V^\dagger\prod_{i\in[N],j\in[5]}\frac{I+(-1)^{s_{i,j}}O_{l_i,j}}{2}V\Big\|_\rho^2 \leq \Theta(\sqrt{\varepsilon+\varepsilon'+\delta})\ .$$

□

引理 8.14（能量测试的推论）。

$$\Pr[\textit{energy test passes}] \leq \varepsilon + \mathop{\mathbb{E}}_{l\in_R[m]^N}\Big\|\sum_{M,o,w}1_{C(D(M))=0}\cdot P_{l,M,o,w}U_{0\to 2}\left|0\right\rangle\Big\|^2.$$

证明。设 $S=\{t|C(D(t))=0\wedge T(t)=1\}$。如果 $dist(M,\ S)>\delta$，

$$\Pr[a_1=1|l,M,o,w] \leq \Pr[\text{verifier accepts}|l,M,o=0,w] \leq \varepsilon.$$

如果 $dist(M,\ S)\leq\delta$，

$$\Pr[a_1=1|l,M,o,w] \leq 1 = 1_{C(D(M))=0}.$$

于是，

$$\begin{aligned}
\Pr[\text{energy test passes}] &= \mathop{\mathbb{E}}_{l\in_R[m]^N}\sum_{M,o,w}\Pr[a_1=1|l,M,o,w]\cdot\|P_{l,M,o,w}U_{0\to 2}\left|0\right\rangle\|^2 \\
&\leq \varepsilon + \mathop{\mathbb{E}}_{l\in_R[m]^N}\sum_{M,o,w}1_{C(D(M))=0}\cdot\|P_{l,M,o,w}U_{0\to 2}\left|0\right\rangle\|^2 \\
&= \varepsilon + \mathop{\mathbb{E}}_{l\in_R[m]^N}\Big\|\sum_{M,o,w}1_{C(D(M))=0}\cdot P_{l,M,o,w}U_{0\to 2}\left|0\right\rangle\Big\|^2.
\end{aligned}$$

□

引理 8.15（能量一致性测试在能量测试中的作用）。

$$\begin{aligned}
&\mathop{\mathbb{E}}_{l\in_R[m]^N}\Big\|\sum_{M,o,w}1_{C(D(M))=0}\cdot P_{l,M,o,w}U_{0\to 2}\left|0\right\rangle\Big\|^2\\
&\leq \Theta(\sqrt{\varepsilon+\varepsilon'+\delta})+1.01\cdot\mathop{\mathbb{E}}_{l\in_R[m]^N}\sum_s 1_{C(s)=0}\Big\|V^\dagger\prod_{i\in[N],j\in[5]}\frac{I+(-1)^{s_{i,j}}O_{l_i,j}}{2}VU_{0\to 2}\left|0\right\rangle\Big\|^2.
\end{aligned}$$

证明。对于任意 $n>0$,

$$\|a+b\|^2\leq\frac{1+n^2}{n^2}\|a\|^2+(1+n^2)\|b\|^2,$$

因为

$$0\leq\frac{1}{n^2}\|a\|^2+n^2\|b\|^2-a^\dagger b-b^\dagger a=\Big\|\frac{1}{n}a-nb\Big\|^2.$$

因此

$$\begin{aligned}
&\mathop{\mathbb{E}}_{l\in_R[m]^N}\Big\|\sum_{M,o,w}1_{C(D(M))=0}\cdot P_{l,M,o,w}U_{0\to 2}\left|0\right\rangle\Big\|^2\\
=&\mathop{\mathbb{E}}_{l\in_R[m]^N}\sum_s 1_{C(s)=0}\Big\|\sum_{M,o,w}1_{D(M)=s}\cdot P_{l,M,o,w}U_{0\to 2}\left|0\right\rangle\Big\|^2\\
\leq& 101\mathop{\mathbb{E}}_{l\in_R[m]^N}\sum_s 1_{C(s)=0}\Big\|(\sum_{M,o,w}1_{D(M)=s}\cdot P_{l,M,o,w}-V^\dagger\prod_{i\in[N],j\in[5]}\frac{I+(-1)^{s_{i,j}}O_{l_i,j}}{2}V)U_{0\to 2}\left|0\right\rangle\Big\|^2\\
&+\frac{101}{100}\mathop{\mathbb{E}}_{l\in_R[m]^N}\sum_s 1_{C(s)=0}\Big\|V^\dagger\prod_{i\in[N],j\in[5]}\frac{I+(-1)^{s_{i,j}}O_{l_i,j}}{2}VU_{0\to 2}\left|0\right\rangle\Big\|^2\\
\leq&\Theta(\sqrt{\varepsilon+\varepsilon'+\delta})+1.01\cdot\mathop{\mathbb{E}}_{l\in_R[m]^N}\sum_s 1_{C(s)=0}\Big\|V^\dagger\prod_{i\in[N],j\in[5]}\frac{I+(-1)^{s_{i,j}}O_{l_i,j}}{2}VU_{0\to 2}\left|0\right\rangle\Big\|^2,
\end{aligned}$$

最后一个不等式由引理 8.13 得出。 □

引理 8.16（通过泡利测量估计 Clifford 哈密顿量的能量）。设 H、H_i、$O_{i,j}$ 和 C 如定义 8.5中所述。那么，

$$\begin{aligned}
&\mathop{\mathbb{E}}_{l\in_R[m]^N}\sum_s 1_{C(s)=0}\Big\|\prod_{i\in[N],j\in[5]}\underbrace{I\otimes I\cdots\otimes I}_{i-1}\otimes\frac{I+(-1)^{s_{i,j}}O_{l_i,j}}{2}\otimes\underbrace{I\otimes I\cdots\otimes I}_{N-i}\left|\varphi\right\rangle\Big\|^2\\
=&\left\langle\varphi\right|\frac{1+(1-2H)^{\otimes N}}{2}\left|\varphi\right\rangle.
\end{aligned}$$

证明。注意

$$H_i=\prod_{j\in[5]}\frac{I+(-1)^0O_{i,j}}{2}=\sum_{1\oplus\vee_{j\in[5]}x_j=1}\prod_{j\in[5]}\frac{I+(-1)^{x_j}O_{i,j}}{2}.$$

and

$$I-H_i=I-\prod_{j\in[5]}\frac{I+O_{i,j}}{2}=\sum_{1\oplus\vee_{j\in[5]}x_j=0}\prod_{j\in[5]}\frac{I+(-1)^{x_j}O_{i,j}}{2}.$$

因此，

$$\begin{aligned}\frac{1}{2}+\frac{1}{2}(1-2H)^{\otimes N} &= \frac{1}{2}+\frac{1}{2}\cdot\frac{1}{m^N}\sum_{l\in[m]^N}\bigotimes_{i\in[N]}(1-2H_{l_i})\\ &= \frac{1}{m^N}\sum_{l\in[m]^N}(\frac{1}{2}+\frac{1}{2}\bigotimes_{i\in[N]}(1-2H_{l_i}))\\ &= \mathop{\mathbb{E}}_{l\in_R[m]^N}\sum_{\oplus_{k\in[N]}r_k=0}\prod_{i=1}^{N}(\frac{1}{2}+(-1)^{r_i}(\frac{1}{2}-H_{l_i}))\\ &= \mathop{\mathbb{E}}_{l\in_R[m]^N}\sum_{\oplus_{k\in[N]}r_k=0}\prod_{i=1}^{N}\sum_{1\oplus\vee_{j\in[5]}s_{i,j}=r_i}\prod_{j\in[5]}\frac{I+(-1)^{s_{i,j}}O_{l_i,j}}{2}\\ &= \mathop{\mathbb{E}}_{l\in_R[m]^N}\sum_{s}1_{C(s)=0}\prod_{i\in[N],j\in[5]}\frac{I+(-1)^{s_{i,j}}O_{l_i,j}}{2}\,.\end{aligned}$$

□

定理 8.17。 QMA $\subseteq$ SQIOP($O(1)$ $O(\exp\circ\text{poly})$ $O(1)$) 。

证明。令 $\mathtt{V}$ 为定义 8.9中的验证者。我们将证明$\mathtt{V}$ 是 O关于 $\mathcal{LCH}(5,\ 2^{-p(n)},\ 1/q(n))$ 的 (1) 消息非自适应强量子交互式预言机证明系统，因此

$$\mathcal{LCH}(5,2^{-p(n)},1/q(n))\in\mathsf{SQIOP}(O(1),O(\exp\circ\text{poly}),O(1)).$$

根据定理 4.10，$\mathcal{LCH}(5,\ 2^{-p(n)},\ 1/q(n))$ 是 QMA-完全的。因此，

$$\mathsf{QMA}\subseteq\mathsf{SQIOP}(O(1),O(\exp\circ\text{poly}),O(1)).$$

根据定义 8.7、定义 8.9和定义 5.12，$\mathtt{V}$ 具有一致性、多项式时间复杂度和高效性，证明长度为 $O(\exp\circ\text{poly})$，查询复杂度为 $O(1)$。此外，完备性和可靠性结果如下。令

$$p=\Pr[\text{The verifier opts to execute the ``EnergyTests'' subroutine}].$$

完备性： 根据定理 7.34，“量子比特测试”以概率 1 通过。根据定义 8.7和定义 8.9，能量一致性测试以概率 1 通过，而能量测试通过的概率为

$$\langle\varphi|\frac{1+(1-2H)^{\otimes N}}{2}|\varphi\rangle\,.$$

因此，

$$\begin{aligned}\Pr[\mathtt{V}\text{ accepts}] &= 1-p+p\cdot\langle\varphi|\frac{1+(1-2H)^{\otimes N}}{2}|\varphi\rangle\\ &\geq 1-p\cdot\Theta(2^{-s(n)}).\end{aligned}$$

可靠性： 假设

$$\Pr[\text{energy consistency test passes}])\geq 1-\Theta(\varepsilon')$$

$$\begin{aligned}\Pr[\text{ consistency check passes }]) &\geq 1-\Theta(\varepsilon')\\ \Pr[\text{ validity check passes }] &\geq 1-\Theta(\varepsilon')\\ \Pr[\text{ anti-commuting test passes }] &\geq 1-\Theta(\varepsilon')\,.\end{aligned}$$

那么，通过结合引理 8.14、引理 8.15和引理 8.16,

$$\Pr[\text{energy test passes}] \leq \Theta(\sqrt{\varepsilon+\varepsilon'+\delta}) + 1.01\cdot\langle\varphi|\,\frac{1+(1-2H)^{\otimes N}}{2}\,|\varphi\rangle\,.$$

此外，根据定义 8.9，验证者的接受概率由两部分组成：能量测试的接受概率和其他测试的接受概率。根据上述不等式,

$$\begin{aligned}\Pr[\mathtt{V}\text{ accepts}] &\leq 1-p+p\cdot(\Theta(\sqrt{\varepsilon+\varepsilon'+\delta}) + 1.01\cdot\langle\varphi|\,\frac{1+(1-2H)^{\otimes N}}{2}\,|\varphi\rangle)\\ &\leq 1-p+p\cdot(\Theta(\sqrt{\varepsilon+\varepsilon'+\delta}) + 0.505 + \Theta(2^{-s(n)}))\\ &\leq 1-0.4p,\end{aligned}\tag{14}$$

其中，最后一步是通过令 ε，ε'，δ 足够小得到的。

如果以下条件中有一项不成立

$$\begin{aligned}\Pr[\text{energy consistency test passes}]) &\geq 1-\Theta(\varepsilon')\\ \Pr[\text{ consistency check passes }]) &\geq 1-\Theta(\varepsilon')\\ \Pr[\text{ validity check passes }] &\geq 1-\Theta(\varepsilon')\\ \Pr[\text{ anti-commuting test passes }] &\geq 1-\Theta(\varepsilon')\,,\end{aligned}$$

then

$$\begin{aligned}\Pr[\mathtt{V}\text{ accepts}] &\leq p+(1-p)\cdot(1-\Theta(\varepsilon'))\\ &= 1-(1-p)\cdot\Theta(\varepsilon')\,.\end{aligned}\tag{15}$$

注意，ε 是定理 7.1 中的自校正参数，而 δ 是定理 4.14中的 PCPP 接近参数。因此，我们可以取 $p=1/3$，并将 $\varepsilon=\delta=\varepsilon'$ 选得足够小。我们可以将 ε 设为任意固定的小常数，代价是将自校正过程的查询复杂度增加一个较大的常数因子。通过将 PCPP 验证器重复运行常数次，我们可以得到接近参数和可靠性误差都任意小的常数 PCPP。根据等式（14）和等式（15），可得

$$\Pr[\mathtt{V}\text{ accepts}] \leq \max\{1-(1-p)\cdot\Theta(\varepsilon'), 1-0.4p\} \leq 1-c\,,$$

其中 c 是一个较小的常数。 □

单量子比特测试

我们的单量子比特测试从对应于 X 测量和 Z 测量的两轮开始。游戏过程如下：每一轮中，诚实证明者在第一轮发送 X 的纯化测量，在第二轮发送 Z 的纯化测量。验证者要么在 Z 基下进行测量，要么对某些量子比特应用 Z门，然后验证者将证明者消息中的所有寄存器发回，诚实证明者撤销纯化测量。

最后还有额外一轮。验证者发送符号“X”或“Z”。诚实证明者返回测量结果。

验证者执行反对易测试和一致性检查。更具体地说，验证者检查第一次 Z 测量与最后一轮中间应用 X 后进行的 Z 测量之间的一致性。此外，验证者检查前两轮与最后几轮是否一致。我们将证明，反对易关系会在最后一轮出现。

A.1 诚实证明者的策略

现在我们定义诚实证明者在前两轮中每轮采取的确切操作。诚实证明者在不同轮次使用不同的 O。稍后，我们将介绍该模板实现的细节。

定义 A.1 (诚实证明者前两轮操作的模板)**.** 设 P 是一个包含1 个量子比特的寄存器，R 是一个包含1 个量子比特的寄存器。P和R 最初由证明者持有。设 O_1、O_2 是寄存器 P 上的可观测量。

- 证明者的第一步：证明者应用以下酉算子

$$P(O_{\mathsf{P}}, \mathsf{R}).$$

  证明者向验证者发送寄存器R。

- 验证者的第一步：验证者从证明者处收到寄存器R 。验证者向证明者发送寄存器R。

- 证明者的第二步：证明者从验证者处收到寄存器R 。证明者应用以下酉算子

$$(P(O_{\mathsf{P}}, \mathsf{R}))^{-1}.$$

接下来，我们描述诚实证明者在最后一轮的操作：

定义 A.2 (诚实证明者在最后一轮的操作)。 设P 是一个包含1 个量子比特的寄存器。P最初由证明者持有。

- 验证者的第一步：验证者向证明者发送 $q' \in [2]$。
- 证明者的第一步：证明者使用可观测量 Z （若 $q' = 1$），使用可观测量 X （若 $q' = 2$ ）测量P ，并返回测量结果。

现在我们总结诚实证明者的操作：

定义 A.3 (单量子比特测试，诚实证明者)。设P 是一个包含1 个量子比特的寄存器，R 是一个包含1 个量子比特的寄存器。P、R 最初由证明者持有，并初始化为 $|0\rangle$。

诚实证明者的操作定义如下：

- 诚实证明者按照定义 *A.1* 进行操作，其中 $O = Z$。
- 诚实证明者按照定义 *A.1* 进行操作，其中 $O = X$。
- 最后，诚实证明者按照定义 *A.2*进行操作。

A.2 验证者策略

接下来我们介绍验证者的操作。为便于阐述，我们先对在证明者的消息中对单个量子比特施加特定酉操作的过程进行抽象。

在前两轮中，验证者可以用多种方式回应证明者的消息。稍后，我们将说明验证者在单量子比特测试的整个协议中如何选择回应方式。在以下定义中， M， F 可视为模板的输入。 M 表示是否进行测量。 F 表示是否进行翻转。

定义 A.4 （。验证者在前两轮的行动模板）设 R 为一个寄存器。设M， $F \in \{0, 1\}$。

- 证明者的第一步：证明者向验证者发送寄存器 R。
- 验证者的第一步：验证者从证明者处接收寄存器 R 。如果 $F = 1$，验证者对 Z_R进行操作。如果 $M = 1$，验证者测量 Z_R 并输出测量结果。验证者将寄存器 R发送给证明者。
- 证明者的第二步：证明者从验证者处接收寄存器 R 。

接着，我们描述验证者在最后一轮中的行动，其中 $q' = 1$对应符号“X”， $q' = 2$ 对应符号“Z”：

定义 A.5 （最后一轮中验证者的操作）。 设 $q' \in [2]$。

- 验证者的第一步： 验证者将 q' 发送给证明者。
- 证明者的第一步： 证明者返回一个比特 r'。

现在，我们介绍验证者在单量子比特测试中的操作。验证者有两类检查：一致性检查和反对易检查。我们首先介绍一致性检查。在此检查中，验证者检查前两轮与最后一轮之间的一致性。更具体地说，验证者检查最后一轮中的答案是否与前一轮的答案相匹配。

定义 A.6 （单量子比特测试，一致性检查）。 设 R 为一个寄存器。验证者的操作定义如下：

- 验证者采样 $u \in_R [2]$，设置 $M_u = 1$，并为 $i \neq u, i \in [2]$设置 $M_i = 0$ 。
- 如果 $M_1 = 1$，验证者将 $F_i = 0$ 设为 $i \in [2]$。如果 $M_2 = 1$，验证者将 $F_1 \in_R \mathbb{F}_2$ 设为 $F_2 = 0$。
- 验证者重复执行定义*A.4*中的2次操作。在第 i次中，

验证者按照定义 $A.4$ 的方式行动，给定 $M = M_i$，$F = F_i$，如果 $M_i = 1$，则令 r_i 为输出。

- 最后，验证者按照定义 $A.5$ 执行，其中 $q' = u$。令 r' 表示验证者从证明者处收到的比特。
- 当且仅当 $r_u = r'$ 时，验证者接受。

然后，我们引入反对易测试，在该测试中，验证者检查与第一次 Z 测量相对应的一致性，并检查最后一轮的 Z 测量的一致性，其中间应用 X。

定义 A.7（单量子比特测试，反对易测试）。令 R 为一个寄存器。验证者的操作定义如下：

- 验证者设置 $M_1 = 1, F_1 = 0, M_2 = 0, F_2 = 1$。
- 验证者重复定义$A.4$中的验证者操作2次。在第 i次时，验证者按照定义 $A.4$ 执行，其中 $M = M_i$，$F = F_i$，如果 $M_i = 1$，则设置 r_i 为输出。
- 最后，验证者按照定义 $A.5$ 的方式行事，其中使用 $q' = 1$（对应符号“Z”）。令 r' 表示验证者从证明者那里收到的比特。
- 当且仅当 $r_1 = r' \oplus 1$ 时，验证者接受。

现在我们把所有内容整合起来，并定义验证者在单量子比特测试中的操作。

定义 A.8（单量子比特测试，验证者）。设 R 为一个寄存器。验证者的操作定义如下：

1. 以概率 $1/2$，验证者按照定义$A.6$行事，
2. 以概率 $1/2$，验证者按照定义$A.7$行事。

A.3 主定理

在本节陈述主定理之前，我们先介绍一般证明者操作。

定义 A.9（规范证明者操作）。设 P 是一个寄存器，R 是一个含有 1 个量子比特的寄存器。P、R 最初由证明者持有，并初始化为 $|0\rangle$。对于 $q' \in [2]$，设 $O'_{q'}$ 是一个可观测量，使得 $(O'_{q'})^2 = I$。对于 $i \in [2]$，设 U_i 是一个酉算子。

规范证明者在前两轮中的操作定义如下：在第 i 轮，

- 证明者的第一步： 证明者施加酉算子$U_{i,\mathsf{PR}}$。证明者向验证者发送寄存器R。
- 验证者的第一步： 验证者接收证明者发送的寄存器 R 。验证者向证明者发送寄存器R。
- 证明者的第二步：证明者从验证者处接收寄存器R 。

最后一轮的规范证明者操作定义如下：

- 验证者的第一步：验证者向证明者发送 $q' \in [2]$ 。
- 证明者的第一步：证明者测量可观测量 $O'_{q',\,\mathsf{PR}}$ 并返回测量结果。

注 A.10. 请注意，任何证明者操作都可以纯化为上述描述的规范证明者操作。

为便于表述，我们引入转移作用。

定义 A.11 （转移作用）。 设 U_i 对于 $i \in [2]$ 如定义 *A.9*中所定义。对于 $i < j$， i, $j \in \{0,1,2\}$，定义从 i 到 j 的转移作用如下：

$$U_{i\to j} = U_j \cdots U_{i+2} U_{i+1}.$$

现在，我们陈述本节的主定理。

定理 A .12 (单量子比特测试)。 设 V 为定义 *A.8* 中定义的验证者。则 ，

1. 完备性： V 以概率 *1* 接受定义 A.3 中的证明者。

2. 可靠性： 设 P 为定义 *A.9* 中定义的证明者。设 O'_1， O'_2 如定义 *A.9* 中所定义。若 V接受 P 的概率大于 $1-\delta$，则 O'_1， O'_2 在该量子态下满足近似反对易关系

$$\rho = U_{0\to 2} \left|00\right\rangle_{\mathsf{PR}} \left\langle 00\right|_{\mathsf{PR}} U_{0\to 2}^{\dagger}.$$

更具体地说，

$$\mathrm{tr}((O'_1 O'_2 + O'_2 O'_1)^2 \rho) < \Theta(\delta).$$

在证明主定理之前，我们先引入必要的记号。随后，我们将建立若干引理，以助于证明主定理。

定义 A.13 (带翻转的转移动作)。 设 U_i 针对 $i \in [2]$ 如定义 *A.9* 中所定义。对于 $u \in [2]$， $F \in \{0,1\}^2$，定义带翻转的转移作用如下：

$$U_{1,F} = Z_{\mathsf{R}}^{F_1} U_1,$$
$$U_{2,F} = Z_{\mathsf{R}}^{F_2} U_2 Z_{\mathsf{R}}^{F_1} U_1.$$

接下来，我们考察总体成功概率与每种配置下成功概率之间的关系。

引理 A.14。 令 V， P 如定理 *A.12* 中所定义。令 D 为 M在F 定义*A.6*中的分布。则

$$\Pr[\ V \textit{ accepts } P\ ] \geq 1 - \Theta(\delta)\ ,$$

当且仅当：

- 对于 D 的支撑集中的任意 M、 $F \in \{0,1\}^2$ ，

$$\Pr[\ \textit{consistency check passes}\ \mid M, F] \geq 1 - \Theta(\delta)\ ;$$

- 与

$$\Pr[\ \textit{anti-commuting test passes}\ ] \geq 1 - \Theta(\delta)\ .$$

证明。这个引理可通过直接计算得出。 □

引理 A.15。 设 O_1、$O_2 \in \mathbb{C}^{n\times n}$ 是可观测量， $O_1^2 = O_2^2 = I$、$O_1^\dagger = O_1$、$O_2^\dagger = O_2$。设 $|\varphi\rangle \in \mathbb{C}^n$ 是一个量子态。则

$$\sum_{a\in\{\pm 1\}} \left\| \frac{I + a\cdot O_1}{2} \cdot U \cdot \frac{I + a\cdot O_2}{2} |\varphi\rangle \right\|^2 = \langle\varphi| \frac{2I + U^\dagger O_1 U O_2 + O_2^\dagger U^\dagger O_1 U}{4} |\varphi\rangle .$$

证明。 我们有

$$\begin{aligned}
&\sum_{a\in\{\pm 1\}} \left\| \frac{I + a\cdot O_1}{2} \cdot U \cdot \frac{I + a\cdot O_2}{2} |\varphi\rangle \right\|^2 \\
=& \sum_{a\in\{\pm 1\}} \langle\varphi| \frac{I + a\cdot O_2^\dagger}{2} \cdot U^\dagger \cdot \frac{I + a\cdot O_1}{2} \cdot U \cdot \frac{I + a\cdot O_2}{2} |\varphi\rangle \\
=& \sum_{a\in\{\pm 1\}} \langle\varphi| \frac{2I + U^\dagger O_1 U O_2 + O_2^\dagger U^\dagger O_1 U + a(O_2 + U^\dagger O_1 U + O_2^\dagger + O_2^\dagger U^\dagger O_1 U O_2)}{8} |\varphi\rangle \\
=& \langle\varphi| \frac{2I + U^\dagger O_1 U O_2 + O_2^\dagger U^\dagger O_1 U}{4} |\varphi\rangle .
\end{aligned}$$

□

引理 A.16 (一致性检查的推论)。 设 U_i 对于 $i \in [2]$ 按定义*A.9*定义。设 P、R 按定义 *A.9*定义。设 D 为定义 M中 F的分布， *A.6*。对于任意 M、$F \in \{0,1\}^2$ 属于 D的支撑集，令 $u \in \{0,1\}$ 满足 $M_u = 1$。则

$$\|(O'_u U_{2,F} - U_{u\to 2} Z_{\mathsf{R}} U_{u,F}) |00\rangle_{\mathsf{PR}} \|^2 = 4\cdot(1 - \Pr[\ \textit{consistency check passes}\ \mid M, F]) .$$

证明。 通过直接计算可得，

$$\begin{aligned}
&\Pr[\text{ consistency check passes } \mid M, F] \\
=& \sum_{a\in\{\pm 1\}} \| \frac{I + a\cdot O'_u}{2} \cdot U_{u\to 2} \cdot \frac{I + a\cdot Z}{2} \cdot U_{u,F} |0\rangle \|^2 \\
=& \langle 0| \frac{2I + U_{u,F}^\dagger Z U_{u\to 2}^\dagger O'_u U_{2,F} + U_{2,F}^\dagger O'_u U_{u\to 2} Z U_{u,F}}{4} |0\rangle .
\end{aligned}$$

此外，我们有

$$\begin{aligned}
&\|O'_u U_{2,F} |0\rangle - U_{u\to 2} Z_{\mathsf{R}} U_{u,F} |0\rangle \|^2 \\
=& 2 - \langle 0| U_{u,F}^\dagger Z U_{u\to 2}^\dagger O'_u U_{2,F} + U_{2,F}^\dagger O'_u U_{u\to 2} Z U_{u,F} |0\rangle .
\end{aligned}$$

□

引理 A.17 (反对易测试的推论)。 设 U_i 对于 $i \in [2]$ 按定义 *A.9*定义。设 P、R 按定义 *A.9*定义。

那么，

$$\|(O'_1 Z U_{0\to 2} + Z U_2 Z U_1) |00\rangle_{\mathsf{PR}} \|^2 = 4\cdot(1 - \Pr[\ \textit{anti-commuting test passes}\ ]).$$

证明。 通过直接计算，

$$\begin{aligned}
&\Pr[\text{ anti-commuting test passes }] \\
=& \sum_{a\in\{\pm 1\}} \| \frac{I - a\cdot O_1'}{2} \cdot Z \cdot U_2 \cdot \frac{I + a\cdot Z}{2} \cdot U_1 |0\rangle \|^2 \\
=& \langle 0| \frac{2I - U_{0\to 2}^\dagger Z O_1' Z U_2 Z U_1 - U_1^\dagger Z U_2^\dagger Z O_1' Z U_{0\to 2}}{4} |0\rangle .
\end{aligned}$$

此外，我们还有

$$\begin{aligned}
&\| O_1' Z U_{0\to 2} |0\rangle + Z U_2 Z U_1 |0\rangle \|^2 \\
=& 2 + \langle 0| U_{0\to 2}^\dagger Z O_1' Z U_2 Z U_1 + U_1^\dagger Z U_2^\dagger Z O_1' Z U_{0\to 2} |0\rangle .
\end{aligned}$$

□

以下引理将有助于证明定理A.12的完备性。

引理 A.18 （规范证明者形式下的诚实证明者）。 设

$$R_1 = P(Z_{\mathsf{P}}, \mathsf{R}), R_2 = P(X_{\mathsf{P}}, \mathsf{R}).$$

定义 *A.3* 中的证明者是定义*A.9* 中的证明者，并满足：

$$\begin{aligned}
U_1 &= R_1, \\
U_2 &= R_2 \cdot R_1^{-1},
\end{aligned}$$

and

$$\begin{aligned}
O_1' &= R_2 \cdot Z_{\mathsf{P}} \cdot R_2^{-1}, \\
O_2' &= R_2 \cdot X_{\mathsf{P}} \cdot R_2^{-1}.
\end{aligned}$$

证明。 该引理可由直接计算得到。 □

引理 A.19 （诚实证明者的性质）。 对于 $i \in [2]$，令 U_i 按照引理 *A.18* 定义。对于 $q' \in [2]$，令 $O_{q'}'$ 按照引理 *A.18* 定义。则：

- 对于任意 $u \in [2]$，

$$O_u' U_{u\to 2} = U_{u\to 2} Z_{\mathsf{R}}.$$

- 此外，

$$O_1' Z_{\mathsf{R}} U_2 = -Z_{\mathsf{R}} U_2 Z_{\mathsf{R}}$$

证明。

设 R_i 如引理A.18中所定义。

第一部分： 只需证明

$$R_2^{-1} O_u' R_2 = R_u^{-1} Z_{\mathsf{R}} R_u,$$

这由.....即可得出

$$R_2^{-1}O_1'R_2 = Z_{\mathsf{P}},$$
$$R_2^{-1}O_2'R_2 = X_{\mathsf{P}},$$

and

$$R_1^{-1}Z_{\mathsf{R}}R_1 = Z_{\mathsf{P}},$$
$$R_2^{-1}Z_{\mathsf{R}}R_2 = X_{\mathsf{P}}.$$

第二部分： 只需证明

$$Z_{\mathsf{P}}R_2^{-1}Z_{\mathsf{R}}R_2 = -R_2^{-1}Z_{\mathsf{R}}R_2R_1^{-1}Z_{\mathsf{R}}R_1,$$

这可由下式推出

$$Z_{\mathsf{P}}X_{\mathsf{P}} = -X_{\mathsf{P}}Z_{\mathsf{P}}.$$

□

定理 *A.12* 的证明

完备性： 对于 $i \in [2]$，令 U_i 按引理 A.18中的定义取值。对于 $q' \in [2]$，令 $O_{q'}'$ 按引理 A.18中的定义取值。令 D 为 M在定义 A.6中的抽样分布，其中 F

根据引理 A.14、引理 A.16和引理 A.17，我们只需证明：对于任意 M，$F \in \{0,1\}^2$ 属于 D的支撑集，令 u 满足 $M_u = 1$,

$$O_u'U_{u\to 2} = U_{u\to 2}Z_{\mathsf{R}},$$

and

$$O_1'Z_{\mathsf{R}}U_{0\to 2} = -Z_{\mathsf{R}}U_2Z_{\mathsf{R}}U_1.$$

这两部分可直接由引理A.19得出。

可靠性：

我们用 $|\alpha\rangle \approx_\delta |\beta\rangle$ 表示 $\| |\alpha\rangle - |\beta\rangle \|^2 \le \Theta(\delta)$。我们有

$$\begin{aligned}
&\mathrm{tr}((O_1'O_2' + O_2'O_1')^2U_{0\to 2}|00\rangle_{\mathsf{PR}}\langle 00|_{\mathsf{PR}}U_{0\to 2}^\dagger) \\
=\ &\langle 00|_{\mathsf{PR}}U_{0\to 2}^\dagger(O_1'O_2' + O_2'O_1')^2U_{0\to 2}|00\rangle_{\mathsf{PR}} \\
=\ &\|O_1'O_2'U_{0\to 2}|00\rangle_{\mathsf{PR}} + O_2'O_1'U_{0\to 2}|00\rangle_{\mathsf{PR}}\|^2.
\end{aligned}$$

根据引理 A.14、引理 A.16和引理 A.17，我们得出以下关系：

$$\begin{aligned}
&O_1'O_2'U_{0\to 2}|0\rangle \\
\approx_\delta\ &O_1'ZU_2U_1|0\rangle \\
\approx_\delta\ &-ZU_2ZU_1|0\rangle \\
\approx_\delta\ &-O_2'U_2ZU_1|0\rangle \\
\approx_\delta\ &-O_2'O_1'U_{0\to 2}|0\rangle.
\end{aligned}$$

因此,

$$\|O_1'O_2'U_{0\to 2}|00\rangle_{\mathsf{PR}} + O_2'O_1'U_{0\to 2}|00\rangle_{\mathsf{PR}}\|^2 \le \Theta(\delta).$$

□

参考文献

[AALV09] Dorit Aharonov、Itai Arad、Zeph Landau 和 Umesh Vazirani。可检测性引理与量子间隙放大。载于《计算理论研讨会》第41届ACM年会论文集，第417–426页，2009年。[AAV13] Dorit Aharonov、Itai Arad 和 Thomas Vidick。量子 PCP 猜想。CoRR，abs/1309.7495，2013年。[ABCY22] Gal Arnon、Amey Bhangale、Alessandro Chiesa 和 Eylon Yogev。交互式预言机证明中障碍的工具箱。载于 Eike Kiltz 和 Vinod Vaikuntanathan（编），《密码学理论——第20届国际会议，TCC 2022，美国伊利诺伊州芝加哥，2022年11月7日至10日，论文集》，第一部分，《计算机科学讲义》第13747卷，第447–466页。施普林格，2022年。[ABN23] Anurag Anshu、Nikolas P. Breuckmann 和 Chinmay Nirkhe。由优质量子码构造的 NLTS 哈密顿量。载于 Barna Saha 和 Rocco A. Servedio（编），《第55届ACM计算理论年会论文集，STOC 2023，美国佛罗里达州奥兰多，2023年6月20日至23日》，第1090–1096页。ACM，2023年。[ABOEM17] Dorit Aharonov、Michael Ben-Or、Elad Eban 和 Urmila Mahadev。量子计算的交互式证明。arXiv 预印本 arXiv:1704.04487，2017年。[ALM+98] Sanjeev Arora、Carsten Lund、Rajeev Motwani、Madhu Sudan 和 Mario Szegedy。证明验证与近似问题的困难性。《ACM 学报》，45(3)：501–555，1998年。[AN02] Dorit Aharonov 和 Tomer Naveh。量子 NP——综述。arXiv 预印本 quant-ph/0210077，2002年。[AS98] Sanjeev Arora 和 Shmuel Safra。概率性证明检验：NP 的一种新刻画。《ACM 学报》，45(1)：70–122，1998年。[BCS16] Eli Ben-Sasson、Alessandro Chiesa 和 Nicholas Spooner。交互式预言机证明。载于 Martin Hirt 和 Adam D. Smith（编），《密码学理论——第14届国际会议，TCC 2016-B，中国北京，2016年10月31日至11月3日，论文集》，第二部分，《计算机科学讲义》第9986卷，第31–60页，2016年。[BFL90] L´aszl´o Babai、Lance Fortnow 和 Carsten Lund。非确定性指数时间具有双证明者交互协议。载于《第31届计算机科学基础年会》，美国密苏里州圣路易斯，1990年10月22日至24日，第一卷，第16–25页。IEEE 计算机学会，1990年。[BGH+04] Eli Ben-Sasson、Oded Goldreich、Prahladh Harsha、Madhu Sudan 和 Salil P. Vad han。鲁棒近邻 PCP、更短的 PCP 及其在编码中的应用。载于 L´aszl´o Babai（编），《第36届ACM计算理论年会论文集》，美国伊利诺伊州芝加哥，2004年6月13日至16日，第1–10页。ACM，2004年。[BH13] Fernando G. S. L. Brand˜ao 和 Aram W. Harrow。量子基态的乘积态近似。载于 Dan Boneh、Tim Roughgarden 和 Joan Feigenbaum（编），《计算理论研讨会会议》，STOC'13，美国加利福尼亚州帕洛阿尔托，2013年6月1日至4日，第871–880页。ACM，2013年。

[BHW24]Harry Buhrman、Jonas Helsen 和 Jordi Weggemans。量子 PCP：关于自适应性、多证明者以及归约到局部哈密顿量。*arXiv*预印本 *arXiv:2403.04841*，2024年。[BJSW16] Anne Broadbent、Zhengfeng Ji、Fang Song 和 John Watrous。面向 QMA 的零知识证明系统。载于 Irit Dinur 编，*IEEE* 第*57*届计算机科学基础年会（*FOCS 2016*），*2016*年*10*月*9*日至*11*日，美国新泽西州新不伦瑞克凯悦酒店，第31–40页。IEEE 计算机学会，2016年。[BK97] L´aszl´o Babai 和 Peter G. Kimmel。随机化同时消息：解决 Yao 在通信复杂度中的一个问题。载于第*12*届*IEEE*计算复杂性年会论文集，德国乌尔姆，*1997*年*6*月*24*日至*27*日，第239–246页。IEEE 计算机学会，1997年。[BKL+22] James Bartusek、Yael Tauman Kalai、Alex Lombardi、Fermi Ma、Giulio Malavolta、Vinod Vaikuntanathan、Thomas Vidick 和 Lisa Yang。量子计算的简洁经典验证。载于 Yevgeniy Dodis 和 Thomas Shrimpton 编，密码学进展——*CRYPTO 2022*——第*42*届国际密码学年会，*CRYPTO 2022*，美国加利福尼亚州圣巴巴拉，*2022*年*8*月*15*日至*18*日，论文集，第二部分，第13508卷计算机科学讲义，第195–211页。施普林格，2022年。[CGJV19]Andrea Coladangelo、Alex Bredariol Grilo、Stacey Jeffery 和 Thomas Vidick。受约束验证者：可验证委托量子计算的新方案，所需资源为准线性。载于 Yuval Ishai 和 Vincent Rijmen 编，密码学进展——*EUROCRYPT 2019*——第*38*届国际密码学理论与应用会议，德国达姆施塔特，*2019*年*5*月*19*日至*23*日，论文集，第三部分，第11478卷计算机科学讲义，第247–277页。施普林格，2019年。[CRSV17] Rui Chao、Ben W. Reichardt、Chris Sutherland 和 Thomas Vidick。重叠量子比特。载于 Christos H. Papadimitriou 编，第*8*届理论计算机科学创新会议（*ITCS 2017*），*2017*年*1*月*9*日至*11*日，美国加利福尼亚州伯克利，第67卷*LIPIcs*，第48:1–48:21页。Schloss Dagstuhl - Leibniz-Zentrum f¨ur Informatik，2017年。[Din06] Irit Dinur。通过间隙放大证明 PCP 定理。载于 Jon M. Kleinberg 编，第*38*届*ACM*计算理论年会论文集，美国华盛顿州西雅图，*2006*年*5*月*21*日至*23*日，第241–250页。ACM，2006年。[dlS22] Mikael de la Salle。群与非局域博弈的谱隙和稳定性（2022）。*arXiv*预印本 *arXiv:2204.07084*，2022年。[FGL+91] Uriel Feige、Shafi Goldwasser、L´aszl´o Lov´asz、Shmuel Safra 和 Mario Szegedy。团的近似求解几乎是 NP 完全的（初步版本）。载于第*32*届计算机科学基础年会，波多黎各圣胡安，*1991*年*10*月*1*日至*4*日，第2–12页。IEEE 计算机学会，1991年。[FH14]Michael H Freedman 和 Matthew B Hastings。非 k-超有限复形上的量子系统：扩张图上经典统计力学的推广。《量子信息与计算》，14(1-2):144–180，2014年。

[FHM18] Joseph F Fitzsimons、Michal Hajdu˘sek 和 Tomoyuki Morimae。量子计算的事后验证。《物理评论快报》，120(4):040501，2018年。[FK17] Joseph F Fitzsimons 和 Elham Kashefi。无条件可验证盲量子计算。《物理评论A辑》，96(1):012303，2017年。[GH17] WT Gowers 和 O Hatami。有限群近似表示的逆定理与稳定性定理。《数学文集》，208(12):1787–1817，2017年。[GJMZ23] Sam Gunn、Nathan Ju、Fermi Ma 和 Mark Zhandry。量子态承诺。载于 Barna Saha 和 Rocco A. Servedio 编，第55届ACM计算理论年会论文集（STOC 2023），美国佛罗里达州奥兰多，2023年6月20日至23日，第1579–1588页。ACM，2023年。[GKK19] Alexandru Gheorghiu、Theodoros Kapourniotis 和 Elham Kashefi。量子计算验证：现有方法综述。《计算系统理论》，63:715–808，2019年。[Gri19] Alex B. Grilo。单轮可验证委托量子计算的简单协议。载于 Christel Baier、Ioannis Chatzigiannakis、Paola Flocchini 和 Stefano Leonardi 编，第46届国际自动机、语言与编程研讨会（ICALP 2019），2019年7月9日至12日，希腊帕特雷，第132卷 LIPIcs，第28:1–28:13页。Schloss Dagstuhl - Leibniz-Zentrum f¨ur Informatik，2019年。[KLVY23] Yael Kalai、Alex Lombardi、Vinod Vaikuntanathan 和 Lisa Yang。任意非局域博弈带来的量子优势。载于 Barna Saha 和 Rocco A. Servedio 编，第55届ACM计算理论年会论文集（STOC 2023），美国佛罗里达州奥兰多，2023年6月20日至23日，第1617–1628页。ACM，2023年。[LMS22] Alex Lombardi、Fermi Ma 和 Nicholas Spooner。后量子零知识，重访：如何做到无法察觉的量子回绕。载于第63届IEEE计算机科学基础年会（FOCS 2022），美国科罗拉多州丹佛，2022年10月31日至11月3日，第851–859页。IEEE，2022年。[MNZ24] Tony Metger、Anand Natarajan 和 Tina Zhang。基于标准假设、通过编译后的非局域博弈为 QMA 构造简洁论证。CoRR，abs/2404.19754，2024年。[NN24] Anand Natarajan 和 Chinmay Nirkhe。量子 PCP 猜想的现状（博弈版本）。CoRR，abs/2403.13084，2024年。[NV16]Anand Natarajan 和 Thomas Vidick。多量子比特态的鲁棒自检验。CoRR，abs/1610.03574，2016年。[NW19] Anand Natarajan 和 John Wright。NEEXP 包含于 MIP*。载于2019年第60届IEEE计算机科学基础年会（FOCS），第510–518页。IEEE，2019年。[NZ23] Anand Natarajan 和 Tina Zhang。编译后的非局域博弈量子值界定：从 CHSH 到 BQP验证。载于第64届IEEE计算机科学基础年会（FOCS 2023），美国加利福尼亚州圣克鲁兹，2023年11月6日至9日，第1342–1348页。IEEE，2023年。

[RRR16] Omer Reingold、Guy N. Rothblum 和 Ron D. Rothblum。《用于委托计算的常数轮交互式证明》。载于 Daniel Wichs 和 Yishay Mansour 编，第*48*届年度 *ACM SIGACT* 计算理论研讨会论文集，*STOC 2016*，美国马萨诸塞州剑桥，*2016*年*6*月*18*日至*21*日，第49–62页。ACM，2016年。[SS96] M. Sipser 和 D.A. Spielman。《扩展码》。*IEEE* 信息论汇刊，42(6)：1710–1722，1996年。[Vid11] Thomas Vidick。《纠缠博弈的复杂性》。博士论文，加州大学伯克利分校，2011年。[Vid20] Thomas Vidick。2020年秋季 FSMP课程：与量子设备的交互，2020年。[Weh06] Stephanie Wehner。交互式证明系统中具有二元答案的纠缠。载于 Bruno Durand 和 Wolfgang Thomas 编，*STACS 2006*：第*23*届年度计算机科学理论方面研讨会，法国马赛，*2006*年*2*月*23*日至*25*日，论文集，第3884卷计算机科学讲义，第162–171页。施普林格，2006年。