薛定谔：量子程序员——通过量子导引估算纠缠

Aby Philip[1], Soorya Rethinasamy[1], Vincent Russo[2], 和 Mark M. Wilde[3,1]

[1]康奈尔大学应用与工程物理学院，美国纽约州伊萨卡 14850[2]Unitary Fund[3]康奈尔大学电气与计算机工程学院，美国纽约州伊萨卡 14850

arXiv:2303.07911v4 [quant-ph] 1 Jun 2024

纠缠量化是一项重要任务，可用于衡量量子态所蕴含的资源价值。本文利用最初由薛定谔发现的量子导引效应，开发了一种量子算法，用于检验一般双体态的可分性并对其进行量化。我们的可分性检验涉及两个参与方之间的分布式量子计算：一方是计算能力有限的客户端，负责制备目标态的纯化；另一方是计算能力不受限的服务器，试图将约化系统导引至由纯乘积态构成的概率系综。为设计实用算法，我们以参数化酉电路和经典优化技术的组合取代服务器，以执行所需的计算。由此得到变分量子导引算法（VQSA），这是一种改进的可分性检验，可在当今已有的量子计算机上实现。随后，我们在含噪量子模拟器上模拟 VQSA，发现其在所测试示例中具有良好的收敛特性。我们还开发了可在经典计算机上运行的半正定规划，用以对 VQSA 的结果进行基准评估。因此，我们的研究结果揭示了量子导引、纠缠、量子算法与量子计算复杂性理论之间的有意义联系，同时也展示了参数化电路中测量在 VQSA 中的价值。

目录

1 引言 **2**

2 结果 **3**

2.1 可分性保真度的量子交互式证明 3

2.2 可分性保真度的变分量子导引算法 5

. .2.3 半定规划基准测试与示例 .2.4 推广至多体可分性保真度 .2.5 量子计算复杂性考量 . 6

4 7 3 结论与讨论 7 4 方法 8 致谢 10 参考文献 10 A 定理 1 的证明 14 B 公式 (19) 的另一种证明 15 C 公式 (20) 的证明 17 D 定理2 的证明 17 E 首个基准测试半定规划 $\widetilde{F}_s^1$ 及公式 (21) 的证明 18 F 第二个基准测试半定规划 F_s^2 及公式 (23) 的证明 20 G 更多模拟与详情 22 H 软件 23 I 多部情形 23 J 复杂度类 $\mathrm{QIP}_{\mathrm{EB}}$(2) 26 K $\mathrm{QIP}_{\mathrm{EB}}$(2) 的定位 31 K.1 QAM $\subseteq \mathrm{QIP}_{\mathrm{EB}}$(2).31 K.2 QSZK $\subseteq \mathrm{QIP}_{\mathrm{EB}}$(2).32 L 局部奖励函数 32

已于 2024-05-29 接收，点击标题进行验证。根据 CC-BY 4.0 协议发布。

1 引言

纠缠是量子力学的一项独特特征，最初由爱因斯坦、波多尔斯基和罗森 [1]揭示。多年后，现代纠缠定义得以提出 [2], ，现回顾如下。两个空间分离系统 σ_{AB} 的双部量子态 A 和 B 若可写成乘积态的概率混合 [2]，则称其为可分（无纠缠）：

$$\sigma_{AB} = \sum_{x\in\mathcal{X}} p(x)\,\psi_A^x \otimes \phi_B^x, \tag{1}$$

其中 $\{p(x)\}_{x\in\mathcal{X}}$ 是一个概率分布，而 ψ_A^x和 ϕ_B^x 是纯态。这里的思想是， A 和 B 之间的相关性完全可以归因于一个具有概率分布 $\{p(x)\}_{x\in\mathcal{X}}$的经典、不可访问的随机变量。

上述定义写出来很直观，但要制定一个算法来判断一般量子态是否可分，则是另一回事；事实上，已有证明表明，在多种框架下，这在计算上都是困难的 [3, 4, 5, 6, 7]。直观而言，要得出答案，就需要搜索该量子态所有可能的概率分解，而可能性多到无法一一考察。尽管如此，判断一般量子态 ρ_{AB} 是可分还是纠缠态，即所谓的可分性问题，仍是一个重要的基础问题，与物理学的多个领域相关，包括凝聚态物质 [8, 9, 10], 量子引力 [11, 12, 13, 14, 15], 量子光学 [16], 和量子密钥分发 [17, 18]。在量子信息科学中，纠缠是若干基本量子信息处理任务的核心资源 [17, 19, 20]„ 因此可分性问题在这一领域也至关重要。

使用纠缠态来执行各种任务面临的一项挑战是，在任何物理平台上，都很难忠实地制备并维持这些量子态。纠缠态与完美纠缠态或最大纠缠态相差越远，其效用就会急剧下降。因此，评估所制备纠缠态的质量成为一项重要任务，这也促使人们在判定是否存在纠缠之外，还要对纠缠进行量化 [21, 22, 23, 24], 。

要通过实验检验量子态是否存在纠缠，并量化其纠缠含量，一种基础方法是利用量子态层析术重构密度矩阵，再检验该矩阵是否表示一个纠缠态 [25, 26]。然而，这种方法的计算复杂度会随量子比特数量呈指数增长，因此无法用于研究较大的量子态。随着规模不断扩大的量子计算机迅速发展，要通过层析术估算描述这些计算机量子态的密度矩阵已不切实际。利用各种知名的单侧纠缠检验来解决可分性问题，更是难上加难 [27, 28, 29, 30]。因此，我们需要寻找解决可分性问题的替代方法，其中一个具有前瞻性的方向是借助量子计算机来解决这一问题 [5, 6, 7, 31]。

我们在此采用的一种解决可分性问题的方法涉及量子导引效应，该效应最初由薛定谔发现 [32, 33]。量子导引的思想是：如果两个相距遥远的系统处于纠缠态，那么在一个系统上进行不同的测量，就能在另一个系统上制备出不同的概率系综。为了更精确地描述这一现象，我们可以借助量子力学中的一些基本概念。设 ψ_{CD} 是两个相距遥远的量子系统 C 和 D的一个纯态，并设 $\rho_C = \mathrm{Tr}_D[\psi_{CD}]$ 是系统 C的约化态。那么，通过对系统 D进行测量，可以在系统 C 上实现一个满足$\rho_C = \sum_z p(z)\psi_C^z$的纯态概率系综$\{(p(z)\ \psi_C^z)\}_z$ 。此外，对于 ρ_C的每一种可能的概率分解，都可以通过对 D 进行测量来实现。近年来，量子导引一直备受关注，其应用包括量子密钥分发 [34, 35], 、量子光学 [36, 37], 以及量子力学的基础研究 [38, 39]。

如上所述，我们可以在可分性问题与量子导引之间建立一种非平凡的联系，从而为解决前者提供一种量子力学方法。为此，请回想可分态 σ_{AB} 在 (1) 的一个纯化是满足 φ_{RAB} 的纯态 $\mathrm{Tr}_R[\varphi_{RAB}] = \sigma_{AB}$，并注意到，在这种情况下，状态向量 $|\varphi\rangle_{RAB}$ 的一种选择如下：

$$|\varphi\rangle_{RAB} = \sum_{x\in\mathcal{X}} \sqrt{p(x)}\,|x\rangle_R \otimes |\psi^x\rangle_A \otimes |\phi^x\rangle_B, \tag{2}$$

其中 $\{|x_R\}_{x\in\mathcal{X}}$ 是正交归一基。纯化并不唯一，但 σ_{AB} 的所有其他纯化都可由对参考系统 R [40]施加酉算子，将式（2）中的纯化变换得到。观察式（2）可知，通过对系统 φ_{RAB}的参考系统 R 进行投影测量 $\{|xx|_R\}_{x\in\mathcal{X}}$，可以将系统 A 和 B 引导到由乘积态组成的概率系综 $\{(p(x)\ \psi_A^x \otimes \phi_B^x)\}_{x\in\mathcal{X}}$。由此可得出一种在一般情况下检验可分性的思路。如果可以获得一般量子态 ρ_{AB} 的纯化，且量子态 ρ_{AB} 确实可分，那么可以：a）尝试找到实现式（2）中纯化的酉算子；b）对参考系统 R进行测量 $\{|xx|_R\}_{x\in\mathcal{X}}$。得到结果 x后，最后可以检验约化态是否为乘积态

。

正如我们将在后文详细阐述的那样，上述基本思路正是我们检验一个量子态是否可分的方法的核心。此外，这种方法还引出了量子算法和复杂性理论方面的结论，可用于量化量子态中的纠缠程度。因此，我们建立了量子导引、纠缠、量子算法与量子计算复杂性理论之间有意义的联系，而此前尚未有人发现这种联系。

本文将进一步阐述上述思路，利用量子导引效应开发多种可分性检验。我们针对混合态提出的可分性检验由两个参与方进行分布式量子计算：一个计算能力不受限制的服务器，称为证明者，原则上能够执行任何可以设想的量子计算；另一个计算能力有限的客户端，称为验证者，能够执行时间高效的量子计算（见图 1）。我们证明了定理 1 和 2，表明在理想情况下，我们的算法的接受概率与一个真正的纠缠度量——可分性保真度——直接相关。我们还运用量子计算复杂性理论中的概念 [41, 42]来了解执行该检验的难度。我们的第二项贡献源于对可分性检验的改进。为了设计一种实用的算法，我们用参数化酉电路与经典优化技术相结合的方式取代证明者，以执行所需的计算。由此得到变分量子导引算法（VQSA），它可以近似实现上述可分性检验（见图 2）。量子导引的概念同样是 VQSA 的核心，正如其所近似的可分性检验一样。有趣的是，我们证明了这两种检验的接受概率都与一种称为可分性保真度的纠缠度量相关 [22, 23]。我们还采用适当的多体可分性定义，将可分性检验和 VQSA 推广到多体情形。

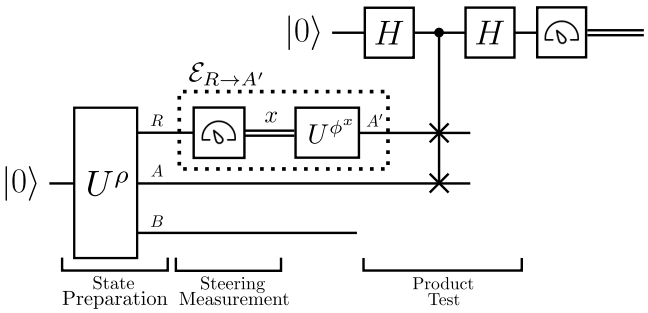


图1：混合态的可分性测试。验证者使用酉电路 U^ρ 制备量子态 ψ_{RAB}，该态是 ρ_{AB}的纯化。证明者（由虚线框标出）通过测量秩一正算子值测度 $\mathcal{E}_{R\to A'}$，对 R施加纠缠破坏信道；测度为$\{\mu_R^x\}_x$，随后根据测量结果 x，从集合 $\{\phi_{A'}^x\}_x$中制备一个纯态。最终态被发送给验证者，由验证者执行交换测试。定理 1 指出，该交互式证明的最大接受概率等于 $\frac{1}{2}(1+F_s(\rho_{AB}))$，即可分性保真度的一个简单函数。

接下来，我们报告了在量子模拟器上对 VQSA 进行模拟的结果，发现其表现出良好的收敛特性。考虑到近期量子计算机规模有限且误差容限有限，我们开发了半定规划（SDP），利用正偏转置（PPT）条件 [27, 28] 和 k-可扩展性 [29, 30] 来近似可分性保真度，从而为 VQSA 得到的结果提供基准。由于变分量子算法（VQA）通常容易遭遇贫瘠高原 [43]，，我们也探讨了如何运用 [44]中提出的思路来缓解这一问题。

我们的方法与近期利用量子算法估计纠缠的研究不同——子算法估计纠缠。例如，变分量子算法已被用于通过估计希尔伯特–施密特距离来解决这一问题 [45]，方法是利用参数化幺正电路构建零和博弈 [46]，，采用对称可扩展性测试 [31]，，估计对数负性 [47],以及使用正映射判据 [47]。变分量子算法还被用于估计多量子比特纯态的纠缠几何度量 [48]。 [49]的研究与我们最为相关，但该研究使用的测试要求每次运行算法时都提供两个目标量子态的副本，并执行受控交换操作，而我们的 VQSA 两者都不需要。与此不同，我们为变分量子算法引入了一种采用参数化电路中途测量的范式；这正是我们估计纠缠方法的核心。我们认为，这种方法将有助于未来各类变分量子算法的研究。此外，正如定理1和2所示，在理想情况下，我们算法的接受概率与一种真正的纠缠度量——可分性的保真度——直接相关。

2 个结果

2.1 关于可分性保真度的量子交互式证明

我们首先介绍用于检验混合态可分性的方法。回顾一下，如果双体态可以写成 (1) 中给出的形式，其中 $|\mathcal{X}|\le$ 秩$(\sigma_{AB})^2$ [2, 50]，则称其为可分态或非纠缠态。

我们针对混合态的可分性检验由以下内容组成：

一项涉及证明者和验证者的分布式量子计算。该计算（如图1所示）首先由验证者制备 ψ_{RAB}的纯化 ρ_{AB}。验证者将系统 R 发送给量子证明者；在我们的模型中，我们限定证明者只能执行纠缠破坏信道。因此，证明者对参考系统 R 执行纠缠破坏信道，并向验证者发送系统 A' 。纠缠破坏信道 $\mathcal{E}_{R\to A'}$ 总可以写成如下的测量-制备信道 [51], :

$$\mathcal{E}_{R\to A'}(\cdot)=\sum_{x\in\mathcal{X}}\mathrm{Tr}[\mu_R^x(\cdot)]\,\phi_{A'}^x, \tag{3}$$

其中，$\{\mu_R^x\}_{x\in\mathcal{X}}$ 是一个秩一正算子值测度（POVM），而$\{\phi_{A'}^x\}_{x\in\mathcal{X}}$ 是一组纯态。（由于纠缠破坏信道具有上述测量并制备分解，我们也可以将证明者视为由两位证明者组成：第一位可以执行一般的量子操作，随后将经典数据传递给第二位；第二位则可以执行一般操作，然后再向验证者传递量子数据。不过，以下内容仍采用单个证明者的说法。）通过执行纠缠破坏信道中的测量部分，证明者实质上将验证者的系统 A 和 B 导引至某个纯态的概率系综。导引验证者的系统后，证明者通过纠缠破坏信道中的制备部分，将系统 A' 发送给验证者。最后，验证者对系统 A 和 A'进行交换测试，当且仅当交换测试的测量结果为零时才接受。量子计算复杂性理论中的标准模型 [41, 42]认为，证明者总是试图让验证者接受计算：在此情形下，证明者会将验证者的系统 A 和 B 导引至一个与乘积态系综重叠最大的系综，然后发送适当的态，以尽可能高的概率通过交换测试。

上述分布式量子计算的最大接受概率等于

$$\max_{\mathcal{E}\in\mathrm{EB}_{R\to A'}}\mathrm{Tr}\left[\left(\Pi_{A'A}^{\mathrm{sym}}\otimes I_{RB}\right)\mathcal{E}_{R\to A'}\left(\psi_{RAB}\right)\right], \tag{4}$$

其中 $\Pi_{A'A}^{\mathrm{sym}}$ 是投影到 A' 以及 A 系统的对称子空间上的投影算子，而$\mathrm{EB}_{R\to A'}$ 表示所有输入系统为 R 且输出系统为 A'的纠缠破坏信道的集合。我们在下文的定理1中指出，式(4)中的最大接受概率可以表示为 ρ_{AB} 的可分性保真度的简单函数；后者定义为 [22, 23]

$$F_s(\rho_{AB}):=\max_{\sigma_{AB}\in\mathrm{SEP}(A:B)}F(\rho_{AB},\sigma_{AB}), \tag{5}$$

其中，SEP($A:B$) 表示 Alice 与 Bob 共享的可分态集合，而 $F(\rho,\ \sigma):=\left\|\sqrt{\rho}\sqrt{\sigma}\right\|_1^2$是态 ρ 与 σ [52]的保真度。可分性保真度也称为最大可分保真度 [5, 6, 7]。根据此定义，我们给出本文的首个关键理论结果：

定理 1 对于纯态 ψ_{RAB}，有如下等式：

$$\max_{\mathcal{E}\in\mathrm{EB}_{R\to A'}}\mathrm{Tr}[(\Pi_{A'A}^{\mathrm{sym}}\otimes I_{RB})\,\mathcal{E}_{R\to A'}\left(\psi_{RAB}\right)] = \frac{1+F_s(\rho_{AB})}{2}, \tag{6}$$

其中 $F_s(\rho_{AB})$ 是量子态ρ_{AB} =迹$_R[\psi_{RAB}]$的可分性保真度。

证明的简要概述请见第 4 节的第一部分，详细证明请见附录 A 。附录 B 和 C 回顾了支持附录 A中证明的一些辅助结果。借助此定理，我们建立了针对混合态的可分性检验。

2.2 用于可分性保真度的变分量子导引算法

我们想指出第 2.1 节中可分性检验的两个重要方面。首先请注意，计算末尾的交换测试实质上测量了验证者系统的量子态与证明者提供的量子态之间的重叠。另一个重要方面是，在现实世界中，并不存在能够提供测试所需理想量子态的计算能力不受限制的量子证明者。

综合考虑这两点，我们对图1中的计算场景进行修改，以便：a）直接测量所需的重叠；b）运用量子变分技术 [53] （参数化酉电路和参数的经典优化），近似计算能力不受限制的证明者的操作。该过程还通过估算可分性保真度，检验并量化给定量子态的可分性。这是一种不同的量子变分技术，称为变分量子导引算法（VQSA）。如图2所示，量子导引通过使用参数化的电路中测量，构成 VQSA 的核心。

我们的 VQSA 结构如下。设 ρ_{AB} 表示我们想要估算其可分性保真度的量子态，并设 ψ_{RAB} 是它的一个纯化，该纯化由酉算符 U^ρ 作用于全零纯态 $|0\rangle\langle 0|$得到。得到 ψ_{RAB}后，我们可以通过对系统 R施加酉操作，尝试访问 ρ_{AB} 的所有可能纯态分解 $\{(p(x)\ \psi_{AB}^x)\}_{x\in\mathcal{X}}$

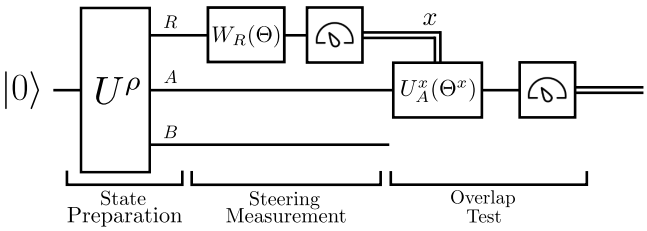


图2：用于估计可分性保真度 $F_s(\rho_{AB})$ 的 VQSA 量子部分。酉电路 U^ρ 制备量子态 ψ_{RAB}，它是 ρ_{AB} 的一种纯化。参数化电路 $W_R(\Theta)$ 作用于 R，将 ψ_{RAB} 演化为 ρ_{AB} 的另一种纯化。随后进行标记为“量子导引测量”的测量；若测量结果 x 出现，该测量便会导引系统 AB 处于纯态 ψ_{AB}^x。在结果 x 的条件下，最终的参数化电路 $U_A^x(\Theta^x)$及后续测量以最大概率 $F_s(\rho_{AB})$接受。

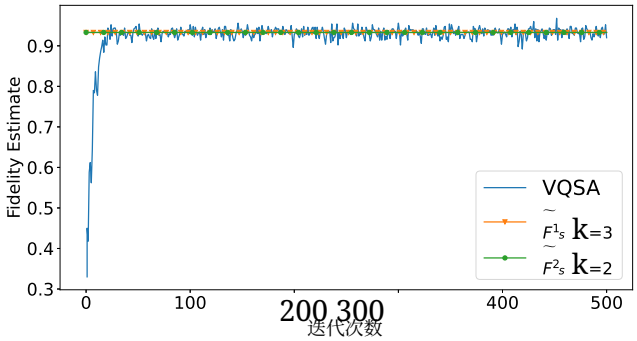


图3：使用我们的 VQSA（蓝线）计算的 $|\Phi^+\rangle$ 与 $|\Phi^-\rangle$ 的 (3/4,1/4) 经典混合态的可分性保真度。算法收敛至 0.93，与使用基准方法 $\widetilde{F}_s^1$和 $\widetilde{F}_s^2$得到的值一致。

施加酉操作。我们使用第一个参数化酉算符 $W_R(\Theta)$。为确保测量结果的数量足够（以涵盖 $|\mathcal{X}| = \text{rank}(\rho_{AB})^2$的可能情况），我们可以在系统 R'中制备一些处于全零态的辅助量子比特，并对 R 和 R'施加 W。不过，不失一般性地，这些额外量子比特可以归入整体参考系统的一部分，并将其重新标记为 R。

经过 $W_R(\Theta)$ 的作用后，在标准基下测量参考系统，并根据结果 x，系统 AB 的测量后状态为纯态 ψ_{AB}^x。接下来，我们估计约化态 ψ_A^x的最大特征值：具体做法是根据结果 x，对约化态 ψ_A^x施加参数化酉算子 $U_A^x(\Theta^x)$，在计算基下测量 A 的所有量子比特，并在出现全零结果时接受。

通过量子-经典混合优化循环，我们可以最大化接受概率，以估计可分性保真度的值。这个 VQSA 的量子部分总结于图2。

定理2 如果图2所总结的 *VQSA* 量子部分中涉及的参数化酉电路，能够表示各自系统的所有可能酉算子，那么该量子电路的最大接受概率等于 $F_s(\rho_{AB})$。

详细证明请参见附录D 。

2.3 半定规划基准测试与示例

由于我们的算法将在规模和误差容限有限的近期量子计算机上运行，

我们开发了半定规划（SDP），以基准评估 VQSA 的结果，因为对于量子比特数量较少的情况，理想结果可以通过经典计算估算。我们的基准方法 $\widetilde{F}_s^1(\rho_{AB},\ k)$ 和 $\widetilde{F}_s^2(\rho_{AB},\ k)$基于正偏转置（PPT）和$k$可扩展性层级。详情见附录 E和 F。

现在，我们展示一个 VQSA 的模拟示例，以证明它能够估计可分性保真度。在第一个示例中，我们将所关注的量子态 ρ_{AB} 设为两个最大纠缠态 $|\Phi^+\rangle = \sqrt{1/2}(|00\rangle + |11\rangle)$ 和 $|\Phi^-\rangle = \sqrt{1/2}(|00\rangle - |11\rangle)$ 的 (3/4,1/4) 概率混合态，因此

$$\rho_{AB} = \frac{3}{4}|\Phi^+\rangle\langle\Phi^+| + \frac{1}{4}|\Phi^-\rangle\langle\Phi^-|. \tag{7}$$

系统 R、 A和 B 的纯化 ρ_{AB} 各包含一个量子比特。结果见图3 。我们使用基准方法和 VQSA 来估计可分性保真度，得到 ≈ 0.93。我们针对 k-可扩展性层级的不同级别评估这些基准方法。更多示例见附录G，有关我们开发的代码的详细信息见附录H 。

作为第二个示例，我们考虑一个由四个量子比特组成的量子态。考虑如下定义的四量子比特量子态 $|\psi\rangle$:

$$\frac{1}{\sqrt{2}}\left(|0\rangle_{A_1}|0\rangle_{A_2}|0\rangle_{B_1}|0\rangle_{B_2} + |1\rangle_{A_1}|1\rangle_{A_2}|1\rangle_{B_1}|1\rangle_{B_2}\right), \tag{8}$$

其中， A 由两个量子比特 A_1 和 A_2 组成，而 B 由两个量子比特 B_1 和 B_2组成。随后，我们将 A_1 和A_2 通过一个定义如下的量子比特退极化信道$\mathcal{D}_p(\rho) \coloneqq (1-p)\rho + p\mathbb{I}/2$，其中 $p = 0.7$。因此，所考虑的最终量子态可写为

$$\tilde{\rho}_{AB} \coloneqq \left(\mathcal{D}_{p,A_1} \otimes \mathcal{D}_{p,A_2} \otimes \mathbb{I}_{B_1} \otimes \mathbb{I}_{B_2}\right)(|\psi\rangle\langle\psi|). \tag{9}$$

然后，我们可以使用 VQSA 来估计.....的保真度

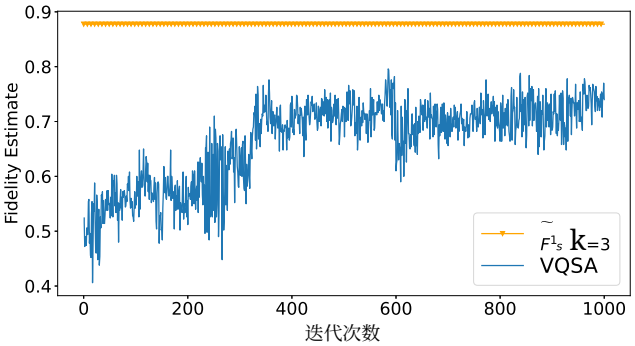


图 4：按 $\tilde{\rho}_{AB}$ 中所规定的(9)，使用我们的 VQSA（蓝线）和 $\widetilde{F}_s^1$ （橙线）计算得到的量子态的可分性保真度。

.....的可分性 $\tilde{\rho}_{AB}$ 并将结果与先前的半定规划基准进行比较。结果见图 4 。

2.4 推广至多体可分性保真度

我们还将 VQSA 推广如下，以测量多体态的可分性保真度。

若多体态 $\rho_{A_1\cdots A_M} \in \mathcal{D}(\mathcal{H}_{A_1\cdots A_M}) \equiv \mathcal{D}(\mathcal{H}_{A_1}\otimes\cdots\otimes\mathcal{H}_{A_M})$ 可以写成如下形式，则称其为可分态

$$\rho_{A_1\cdots A_M} = \sum_{x\in\mathcal{X}} p(x)\psi_{A_1}^{x,1}\otimes\cdots\otimes\psi_{A_M}^{x,M} \tag{10}$$

其中 $\psi^{x,i}_{A_i}$ 对每个 $x\in\mathcal{X}$ 和 $i\in\{1,\ldots,M\}$都是纯态。令 M-SEP 表示所有满足 $\rho_{A_1\cdots A_M}$ 可分的 $\rho_{A_1\cdots A_M}\in\mathcal{D}(\mathcal{H}_{A_1\cdots A_M})$ 的集合。

对于分布式量子计算的多体情形，验证者制备 $\rho_{A_1\cdots A_M}$的一个纯化$\psi^{\rho}_{RA_1\cdots A_M}$ 。证明者对 R施加一个多体纠缠破坏信道，该信道可写为：

$$\mathcal{E}_{R\to A_1'\cdots A_{M-1}'}(\cdot) = \sum_{x\in\mathcal{X}} \mathrm{Tr}[\mu_R^x(\cdot)]\left(\phi_{A_1'}^{x,1}\otimes\cdots\otimes\phi_{A_{M-1}'}^{x,M-1}\right), \tag{11}$$

其中 $\{\mu_R^x\}_x$ 是一个秩一正算子值测度，而 $\{\phi^{x,i}_{A_i'}\}_{x,i}$ 是一组纯态。证明者将系统 $(A^{M-1})'\equiv A_1'\cdots A_{M-1}'$ 发送给验证者。（这里同样可以认为，证明者实际上分成了 M 个证明者：其中一位执行测量 $\{\mu_R^x\}_x$ ，并将结果 x 传达给其他证明者；第 i 位证明者制备量子态 $\phi^{x,i}_{A_i'}$ ，并将其发送给验证者，对所有 $i\in\{1,\ldots,M-1\}$均如此。）最后，验证者对这些系统执行集体交换测试，并且

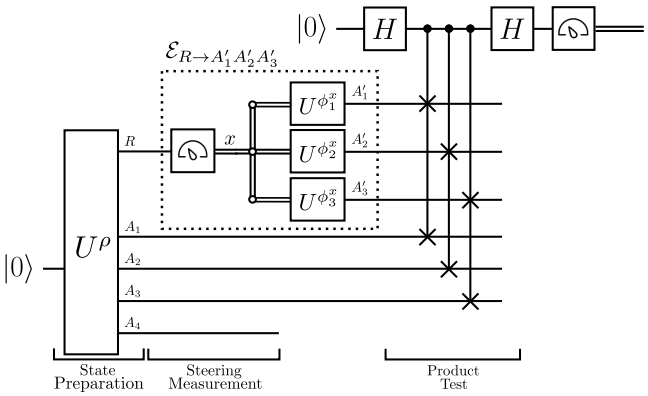


图 5：用于检验多体混合态可分性的测试。验证者使用酉电路 U^ρ 制备量子态 $\psi_{RA_1A_2A_3A_4}$，这是 $\rho_{A_1A_2A_3A_4}$ 的一个纯化。证明者（由虚线框标出）通过测量秩一正算子值测度$\{\mu_R^x\}_{x\in\mathcal{X}}$，在 R 上施加纠缠破坏信道 $\mathcal{E}^{R\to A_1'A_{r2}A_{r3}}$ ，然后根据测量结果 x，从集合 $\{\phi^{x,A_1'}_{1}\otimes\phi^{x,A_2'}_{2}\otimes\phi^{x,A_3'}_{r3}\}_{x\in\mathcal{X}}$中制备一个量子态。最终量子态被发送给验证者，后者执行集体交换测试。定理 3 指出，该交互式证明的最大接受概率等于 $\frac{1}{2}(1+F_s(\rho_{A_1A_2A_3A_4}))$，即可分性保真度的一个简单函数。

系统 $A_1\cdots A_M$，如图 5 所示。这种分布式量子计算的接受概率为

$$\max_{\mathcal{E}\in\mathrm{EB}_{M-1}} \mathrm{Tr}[\Pi^{\mathrm{sym}}_{(A^{M-1})'A^{M-1}}\mathcal{E}_{R\to(A^{M-1})'}(\psi_{RA^{M-1}})], \tag{12}$$

其中 $\Pi^{\mathrm{sym}}{}_{(A^{M-1})'A^{M-1}}$ 是系统$(A^{M-1})'$ 的对称子空间上的投影，且 A^{M-1} 以及EB_{M-1}表示式（11）中定义的多体纠缠破坏信道集合。由此可得以下定理，它将定理1推广到多体情形：

定理 3 对于纯态 $\psi_{RA^M}\equiv\psi_{RA_1\cdots A_M}$，以下等式成立：

$$\max_{\mathcal{E}\in\mathrm{EB}_{M-1}} \mathrm{Tr}[\Pi^{\mathrm{sym}}_{(A^{M-1})'(A^{M-1})}\mathcal{E}_{R\to A_1'\cdots A_{M-1}'}(\psi_{RA^M})] = \frac{1}{2}\left(1+F_s(\rho_{A_1\cdots A_M})\right), \tag{13}$$

其中，多体可分性保真度定义为

$$F_s(\rho_{A_1\cdots A_M}) := \max_{\sigma_{A_1\cdots A_M}\in M-\mathrm{SEP}} F(\rho_{A_1\cdots A_M},\sigma_{A_1\cdots A_M}). \tag{14}$$

参见附录I中的证明。接下来，我们可以使用广义混合态可分性检验，为多体情形开发一种 VQSA。参见图6。该方法

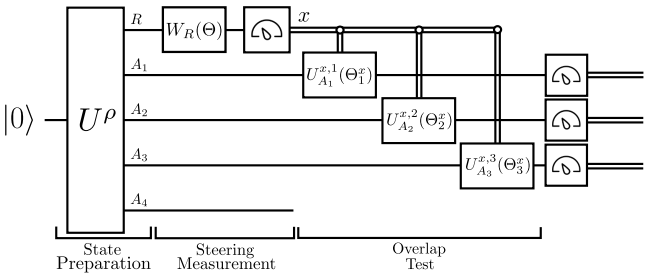


图 6：用于估计多体可分性的保真度 VQSA $F_s(\rho_{A_1A_2A_3A_4})$。酉电路 U^ρ 制备量子态 $\psi_{RA_1A_2A_3A_4}$，它是 $\rho_{A_1A_2A_3A_4}$ 的纯化。参数化电路 $W_R(\Theta)$ 作用于 R，使量子态演化为 $\rho_{A_1A_2A_3A_4}$ 的另一种纯化。随后进行标记为“导引测量”的测量；若测量结果为 x，则剩余系统会被导引至量子态 $\psi^x_{A_1A_2A_3A_4}$。在测量结果为 x 的条件下，应用最终的参数化电路 $U^{x,1}_{A_1}(\Theta^x_1)$、$U^{x,2}_{A_2}(\Theta^x_2)$ 和 $U^{x,3}_{A_3}(\Theta^x_3)$，随后进行的测量以最大概率 $F_s(\rho_{A_1A_2A_3A_4})$接受。

涉及将图5中的集体交换测试替换为重叠测量，类似于我们从图2 得到图1的做法。

2.5 量子计算复杂性考量

我们的最终结果涉及估算可分性保真度 $F_s(\rho_{AB})$的计算复杂性。复杂性理论方法使我们能够根据可分性问题的计算困难程度对其进行分类。这类分析可以在量子计算复杂性理论 [41, 42]的框架内有效开展。

在复杂性理论 [54], 的范式中，复杂度类是一组需要类似资源来求解的计算问题。如果一个复杂度类 A 包含于另一个复杂度类 B中，那么 B中的某些问题可能比 A中的问题需要更多计算资源。为了有效表征一类问题的难度，我们会选取一个能代表该类或对该类而言是完全的问题。若问题 h属于复杂度类 A，并且 h 包含于该类中，且能够高效地将求解问题 h的能力扩展到求解 A中的每一个其他问题，那么问题 h就被认为是该复杂度类的完全问题。

为了解决关于估计可分性保真度的计算复杂性这一问题，我们将 $\mathrm{QIP}_{\mathrm{EB}}(2)$ 定义为这样一个复杂度类：其中的问题可以通过一位证明者来解决，但该证明者仅限于应用纠缠破坏信道；该信道处理从验证者接收到的量子消息，并向验证者发回一条量子消息。

因此，估计给定量子态的可分性保真度属于 $\mathrm{QIP}_{\mathrm{EB}}(2)$，如图1所示。为了完整刻画这一新颖的复杂度类，我们为其给出了一个完全问题。我们证明，给定用于生成信道 $\mathcal{N}_{A\to B}$ 和量子态 ρ_B，估计以下量是 $\mathrm{QIP}_{\mathrm{EB}}(2)$-完全的：

$$\max_{\substack{\{(p(x),\psi^x)\}_x,\{\varphi^x\}_x,\\ \rho_B=\sum_x p(x)\psi^x_B}} \sum_x p(x)F(\psi^x_B,\mathcal{N}_{A\to B}(\varphi^x_A)), \quad (15)$$

其中 $\{(p(x)\ \psi^x)\}_x$ 是一个纯态系综，而 $\{\varphi^x\}_x$是一组纯态。有关这一量的详细信息和解释，请参见附录 J。

通过将可分性保真度估计问题归入 $\mathrm{QIP}_{\mathrm{EB}}(2)$类，我们建立了量子导引和可分性问题与量子计算复杂性理论之间的联系。此外，我们证明复杂度类 $\mathrm{QIP}_{\mathrm{EB}}(2)$包含 QAM [55] 和 QSZK [56]。由此还可直接推广 [5, 6], 中的困难性结果，得出可分性保真度估计问题对 QSZK 和 NP 均为困难问题。上述所有复杂性类在最坏情况下都被认为超出了高效量子计算机的能力范围。证明见附录K，详细示意图见图 7。不过，沿用 [57], 的方法，我们可以尝试使用参数化电路和变分量子算法求解这些类中的一些问题实例。

3 结论与讨论

本文详细介绍了一种分布式量子计算，用于检验量子态的可分性，其核心是运用量子导引。该检验揭示了量子导引与可分性问题之间的联系。这种分布式量子计算的接受概率与一种称为可分性保真度的纠缠度量直接相关。借助该检验的结构，我们还展示了计算复杂性理论方面的结果，并确立了量子导引、量子算法与量子计算复杂性之间的联系。通过用参数化电路替换证明者，我们对这种分布式量子计算进行了改造，开发出变分量子导引算法（VQSA）。这是一种新型变分量子算法，利用量子导引解决可分性保真度估计问题。该算法可以直接估计可分性保真度，无需进行量子态层析，也无需随后对可分性进行近似检验。我们的算法

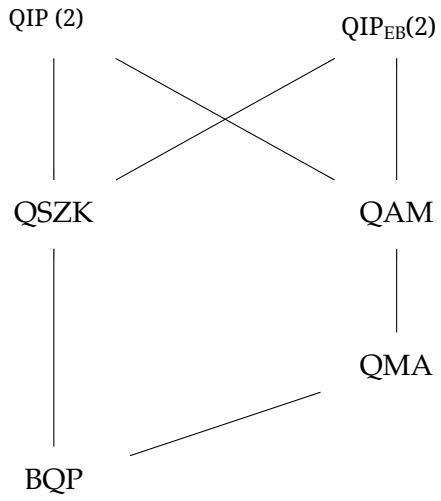


图 7：QIP$_{EB}$(2) 相对于其他已知复杂度类的位置。复杂度类的排列方式如下：如果某个类与其上方的一个类相连，则较低位置的复杂度类是上方类的子集。例如，QIP$_{EB}$(2) 同时是 QSZK 和 QAM 的超集。

由于对系统进行电路中途测量 R 并在系统上执行相应的条件操作，因此它不是酉算子 A。这与大多数变分量子算法有重要区别，因为它们不使用参数化电路中测量。我们还讨论了可分性检验和 VQSA 的多体推广。最后，我们使用含噪 Qiskit Aer 模拟器模拟了 VQSA [58], ，结果显示出良好的收敛趋势，并将其与两个经典半定规划基准进行了比较。

我们的 VQSA 除了可用于在单台量子计算机上进行纠缠量化外，还有其他应用。我们也可以将 VQSA 视为一种分布式变分量子算法，用于测量双体态的纠缠。关于分布式变分量子算法的先前实例，请参见 [59, 60, 61]。事实上，我们的算法可以在量子网络上执行，其中每个节点都配备能够运行变分量子算法的量子计算机和经典计算机。算法的初始部分将 R 分发给 Rob，将 A 分发给 Alice，并将 B 分发给 Bob；他们都身处相距遥远的地点。随后，Rob 执行参数化测量，并通过经典信道将结果发送给 Alice，由 Alice 再进行一次参数化测量。他们可以重复这一过程，以评估 Alice 与 Bob 之间纠缠的质量。对于多体情形下的量子网络，这种解释更有意思：经典数据会从 Rob 广播给除最后一个节点之外的所有其他节点。

VQSA 还可以解决涉及量子导引的其他问题，例如最大化量子态的纯态分解。这种技术也可能有助于估计其他需要在可分态集合上进行优化的纠缠度量。结合 [62, 附录 A] 中的见解和我们在此提出的方法，显然，VQSA 还有助于估计与其他资源理论相关的最大保真度，例如相干性资源理论 [63]。更广泛地说，鉴于近期实验实现方面的进展 [64, 65, 66, 67]，我们认为，参数化电路中测量和分布式变分量子算法这一范式将有助于解决量子信息科学和物理学领域中其他值得关注的计算问题。

从这里开始，我们将为量子计算复杂性理论中的一个重要开放问题：为 QIP$_{EB}$(2)类确定一个非平凡的上界。如备注 7所示，采用 [68, 定理 II.7']中的已知量子 de Finetti 定理的方法，似乎无助于解决这一问题。

4 方法

本节简要概述用于证明定理 1（我们的主要结果之一）的技术，简要介绍我们的半定规划基准方法，并说明有关模拟的必要细节。

为了直观理解混合态的可分性检验，我们先来构造一个用于检验纯态可分性的简单方法。从 (1)可以看出，纯双部态 φ_{AB} 若能写成乘积形式，即

$$\varphi_{AB} = \psi_A \otimes \phi_B, \tag{16}$$

其中 ψ_A 和 ϕ_B 是纯态。我们在下文提出的检验方法十分重要，因为它将与量子导引一同，作为一般情况下可分性检验的一部分再次出现。此外，我们的方法与纯态纠缠检验的标准方法略有不同；标准方法使用该量子态的两个副本进行交换测试 [69, 70, 7]。而我们的方法只需该量子态的一个副本。

我们的纯态可分性测试由证明者和验证者参与的分布式量子计算组成（见图 8）。计算开始时，验证者制备纯态 ψ_{AB}。证明者向验证者发送寄存器 A'中的纯态 $\phi_{A'}$。（需要指出的是，证明者可以发送混合态；不过，该测试的最大接受概率可由纯态实现。因此，不失一般性，证明者应发送纯态。）随后，验证者对 A 和 A'执行标准交换测试 [71, 72]，并在测量结果为零时接受。在量子计算复杂性

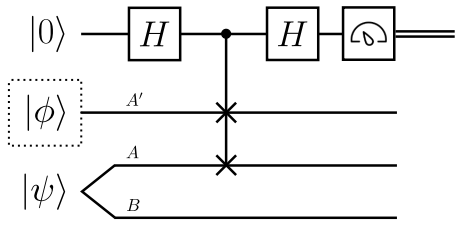


图 8：纯态可分性测试：验证者持有感兴趣的纯态 ψ_{AB}。证明者（虚线框所示）向验证者发送一个纯态 $\phi_{A'}$，随后验证者对系统 A' 和 A执行标准交换测试。如 (18) 中所述，接受概率等于 $\frac{1}{2}(1+\|\psi_A\|_\infty)$。

[41, 42], 中，证明者试图让验证者以尽可能高的概率通过交换测试。因此，在这种情形下，证明者选择 $\phi_{A'}$，以最大化约化态$\psi_A := \mathrm{Tr}_B[\psi_{AB}]$与 $\phi_{A'}$之间的重叠。最大接受概率等于

$$\begin{aligned}
&\max_{\phi} \mathrm{Tr}[(\Pi^{\mathrm{sym}}_{A'A} \otimes I_B)(\phi_{A'} \otimes \psi_{AB})] \\
&= \frac{1}{2}\left(1 + \max_{\phi} \mathrm{Tr}[F_{A'A}(\phi_{A'} \otimes \psi_A)]\right) \qquad (17)\\
&= \frac{1}{2}\left(1 + \max_{\phi} \mathrm{Tr}[\phi_A \psi_A]\right) = \frac{1}{2}\left(1 + \|\psi_A\|_\infty\right), \qquad (18)
\end{aligned}$$

其中， $F_{A'A}$ 是作用于系统 A' 和 A上的酉交换算子，投影算子 $\Pi^{\mathrm{sym}}_{A'A} := \frac{1}{2}(I_{A'A} + F_{A'A})$投影到 A' 和 A的对称子空间，而$\|\psi_A\|_\infty$ 是约化态 ψ_A的谱范数（等于其最大特征值）。由于 $\|\psi_A\|_\infty = 1$ 当且仅当 ψ_A 是纯态，而这又当且仅当 ψ_{AB} 是乘积态，因此，最大接受概率等于 1，当且仅当 ψ_{AB} 是乘积态。

现在我们概述定理1的证明，该证明依赖于两个重要事实。首先，可分性保真度可以用凸屋顶表示如下 [62,定理 1]:

$$F_s(\rho_{AB}) = \max_{\substack{\{(p(x),\psi^x_{AB})\}_x,\\ \rho_{AB}=\sum_x p(x)\psi^x_{AB}}} \sum_x p(x) F_s(\psi^x_{AB}), \qquad (19)$$

其中 $\{p(x)\}_x$ 是一个概率分布，且每个ψ^x_{AB} 都是一个纯态。另请参见 [73, 引理 1]。第二个事实是，对于一个纯双体态， $F_s(\psi_{AB})$可以改写为 [62, 第 6 节。2]

$$F_s(\psi_{AB}) = \|\psi_A\|_\infty . \qquad (20)$$

此外，我们还注意到，对 (4) 中所有纠缠破坏信道的优化等价于

对 ρ_{AB} 的所有纯态分解进行优化，证明的其余部分也随之得出。为完整起见，我们在附录 B 和附录 C 中分别给出 (19) 和 (20) 的证明。由 (1) 和 (20) 可知，对于可分态， $\sum_x p(x)\|\psi^x_A\|_\infty = 1$，这是 $F_s(\rho_{AB})$ 可能达到的最大值。因此，图1中的分布式量子计算通过估计其可分性保真度来检验并量化一个量子态的可分性。最后请注意，如果净化系统 R 是平凡的，那么图1中的计算可以化简为图8中的计算；这意味着在这种情况下，验证者只需在系统 A 和 B 上制备一个纯态。

通过半定规划进行基准测试—下面简要说明半定规划基准 $\widetilde{F}^1_s(\rho_{AB},\ k)$ 和 $\widetilde{F}^2_s(\rho_{AB},\ k)$ 的推导。

首先，回顾一下，两个量子态之间的保真度可以用半定规划表示 [74]。由于没有能够直接对应于在可分态集合上进行优化的半正定约束 [75], ，我们可以通过最大化某个量子态与正偏转置（PPT）态的保真度，来近似该量子态的可分性保真度 [27, 28] 以及 k-可扩展态 [29, 30]。进一步注意到，PPT 和 k-可扩展性约束都是半正定约束，由此得到第一个基准 $\widetilde{F}^1_s(\rho_{AB},\ k)$，其定义见附录 E，并在其中证明其满足以下界：

$$\begin{aligned}
&F_s(\rho_{AB}) \le \widetilde{F}^1_s(\rho_{AB}, k)\\
&\le 1 - \left[\sqrt{1 - F_s(\rho_{AB})} - 2\sqrt{\frac{|B|^2}{k}\left(1 - \frac{|B|^2}{k}\right)}\right]^2, \qquad (21)
\end{aligned}$$

其中， $|B|$ 是系统 B的维数。观察上述不等式可知，

$$\lim_{k\to\infty} \widetilde{F}^1_s(\rho_{AB}, k) = F_s(\rho_{AB}). \qquad (22)$$

第二种基准可通过 (4) 得到。与第一种基准中使用正偏转置和 k-可延拓态来近似可分态类似，我们使用正部分转置信道 [76, 77] 和 k-可延拓信道 [78, 79, 80, 81] 来近似纠缠破坏信道，从而得到第二种基准 $\widetilde{F}^2_s(\rho_{AB},\ k)$。我们证明 $\widetilde{F}^2_s(\rho_{AB},\ k)$ 是一个半定规划，并以下述方式逼近可分性保真度：

$$F_s(\rho_{AB}) \le \widetilde{F}^2_s(\rho_{AB}, k) \le F_s(\rho_{AB}) + \frac{4|A|^3|B|}{k}. \qquad (23)$$

其中 $|A|$ 和 $|B|$ 分别是系统 A和B的维度。证明见附录 F 。同样，

注意到

$$\lim_{k\to\infty} \widetilde{F}_s^2(\rho_{AB}, k) = F_s(\rho_{AB}). \tag{24}$$

模拟与奖励函数——在模拟中，我们使用 Qiskit Aer 模拟器和 Qiskit 的同时扰动随机近似（SPSA）优化器来执行经典优化。VQSA 的迭代过程中，保真度值的波动可归因于使用 Qiskit Aer 模拟器估算接受概率时产生的投影噪声，以及我们用于执行经典优化的 SPSA 优化器本身是一种随机算法。更多示例见附录 G。

变分量子技术（如变分量子算法）的一项关键问题是，随着量子比特数量增加，可能出现贫瘠高原或梯度消失 [43]。然而，近期研究结果表明，将全局奖励函数改为局部奖励函数可以缓解这一问题 [44]。在我们的情形中，全局奖励函数是指测量构成系统的所有量子比特 A，如定理 2 中讨论的方法所做的那样。局部奖励函数的一个例子是，从系统中 A 随机选取一个量子比特，在计算基下进行测量并记录结果，若结果为零则接受。按照[82, 附录 C] 中的方法，并在附录 L 中为完整性起见进行讨论，我们提出的局部奖励函数可用于求得初始全局奖励函数的上界和下界。近期研究也使用局部函数，在利用纯态估计纠缠几何度量时避免变分量子算法中的贫瘠高原 [83]。我们在附录G中给出了局部奖励函数的模拟，表明该函数也可用于估计给定量子态的可分性保真度。

致谢

我们特别感谢 Gus Gutoski，他于 2013 年 9 月提出了图 1 中详述的量子交互式证明的主要思路。我们还感谢 Paul Alsing、Eric Chitambar、Zoë Holmes 和 Wilfred Salmon 富有启发性的讨论，也感谢 Ludovico Lami、Bartosz Regula 和 Alexander Streltsov 与我们进行了同样富有启发性的讨论，并向我们指出了 [73]。AP、SR 和 MMW 感谢美国国家科学基金会第 1907615 号拨款以及美国空军研究实验室根据协议编号 FA8750-23-2-0031 提供的资助。

本材料基于美国空军研究实验室通过协议编号 FA8750-23-2-0031 资助的研究。美国政府获准为政府用途复制和分发重印本，无论其上是否注明版权。本文所述观点和结论均为作者所有，不应被视为必然代表美国空军研究实验室或美国政府的官方政策或明示或暗示的认可。

参考文献

[1]阿尔伯特·爱因斯坦、鲍里斯·波多尔斯基和内森·罗森。“量子力学对物理实在的描述能否被认为是完备的？”《物理评论》**47**，777–780（1935 年）。[2] Reinhard F. Werner。“具有爱因斯坦-波多尔斯基-罗森关联且可由隐变量模型描述的量子态。”《物理评论A辑》**40**，4277–4281（1989 年）。[3] 列奥尼德·古尔维茨。“埃德蒙兹问题的经典确定性复杂度与量子纠缠。”载于第三十五届 ACM 计算理论年会论文集。第 10–19 页。美国加利福尼亚州圣迭戈（2003 年）。[4] 塞瓦格·加里比安。“量子可分性问题的强 NP 困难性。”《量子信息与计算》**10**，343–360（2010 年）。

[5]帕特里克·海登、凯文·米尔纳和 Mark M. Wilde。“双消息量子交互式证明与量子可分性问题”。载于第十八届 IEEE 计算复杂性年会论文集。第 156–167 页。美国加利福尼亚州帕洛阿尔托（2013年）。

[6]帕特里克·海登、凯文·米尔纳和 Mark M. Wilde。“双消息量子交互式证明与量子可分性问题”。《量子信息与计算》**14**，384–416 (2014年)。

[7] Gus Gutoski、帕特里克·海登、凯文·米尔纳和 Mark M. Wilde。“量子交互式证明与可分性测试的复杂性”。《计算理论》**11**，59–103(2015)。

[8]路易吉·阿米科、罗萨里奥·法齐奥、安德烈亚斯·奥斯特洛和 Vlatko Vedral。“多体系统中的纠缠”。《现代物理评论》**80**，517–576 (2008)。

[9]Marcus Cramer、Martin B. Plenio 和哈拉尔德·温德利希。“测量凝聚态系统中的纠缠”。《物理评论》快报**106**，020401(2011)。

[10]尼古拉·拉弗洛朗西。《凝聚态物质系统中的量子纠缠》。《物理报告》**646**，1–59（2016）。

[11] Tadashi Takayanagi。《全息观点下的纠缠熵》。《经典与量子引力》29，153001（2012）。

[12] Sougato Bose、Anupam Mazumdar、Gavin W. Mor- ley、Hendrik Ulbricht、Marko Toroš、Mauro Pater- nostro、Andrew A. Geraci、Peter F. Barker、M. S. Kim 和 Gerard Milburn。《量子引力的自旋纠缠见证》。《物理评论快报》119，240401（2017年）。[13]Chiara Marletto 和 Vlatko Vedral。《引力诱导的两个大质量粒子间纠缠，足以作为引力中存在量子效应的证据》。《物理评论快报》119，240402（2017年）。[14] Xiao-Liang Qi。《引力是否源于量子信息？》。《自然·物理》14，984–987（2018年）。[15]Brian Swingle。《由纠缠产生的时空》。《凝聚态物理年度评论》9，345–358（2018年）。[16] Claude Fabre 和 Nicolas Treps。《量子光学中的模式与态》。《现代物理评论》92，035005（2020年）。[17] Artur K. Ekert。《基于贝尔定理的量子密码学》。《物理评论快报》67，661–663（1991年）。[18] Umesh Vazirani 和 Thomas Vidick。《完全设备无关的量子密钥分发》。《物理评论快报》113，140501（2014年）。[19] Charles H. Bennett 和 Stephen J. Wiesner。《通过爱因斯坦-波多尔斯基-罗森态上的单粒子和双粒子算符进行通信》。《物理评论快报》69，2881（1992年）。[20] Charles H. Bennett、Gilles Brassard、Claude Cré- peau、Richard Jozsa、Asher Peres 和 William K. Wootters。《通过经典信道与爱因斯坦-波多尔斯基-罗森信道传送未知量子态》。《物理评论快报》70，1895（1993年）。[21] Charles H. Bennett、David P. DiVincenzo、John A. Smolin 和 William K. Wootters。《混合态纠缠与量子纠错》。《物理评论 A》54，3824–3851（1996年）。[22] Vlatko Vedral、Martin B. Plenio、M. A. Rippin 和 Peter L. Knight。《纠缠量化》。《物理评论快报》78，2275–2279（1997年）。[23] Vlatko Vedral 和 Martin B. Plenio。《纠缠度量与纯化过程》。《物理评论 A》57，1619–1633（1998年）。

[24]Ryszard Horodecki、Pawel Horodecki、Michal Horodecki 和 Karol Horodecki。“量子纠缠”。《现代物理评论》81，865–942（2009）。[25] J. P. Home、M. J. McDonnell、D. M. Lucas、G. Imreh、B. C. Keitch、D. J. Szwer、N. R. Thomas、S. C. Webster、D. N. Stacey 和 A. M. Steane。“离子-自旋量子比特的确定性纠缠与层析术”。《新物理学杂志》8，188–188（2006）。[26] Matthias Steffen、M. Ansmann、Radoslaw C. Bialczak、N. Katz、Erik Lucero、R. McDermott、Matthew Neeley、E. M. Weig、A. N. Cleland 和 John M. Martinis。“通过量子态层析术测量两个超导量子比特的纠缠”。《科学》313，1423–1425（2006）。[27]Asher Peres。“密度矩阵的可分性判据”。《物理评论快报》77，1413–1415（1996）。[28] Michal Horodecki、Pawel Horodecki 和 Ryszard Horodecki。“混合态的可分性：充要条件”。《物理快报A辑》223，1–8（1996）。[29]Reinhard F. Werner。“贝尔不等式在量子态扩展问题中的应用”。《数学物理快报》17，359–363（1989）。[30] Andrew C. Doherty、Pablo A. Parrilo 和 Federico M. Spedalieri。“完备的可分性判据族”。《物理评论A辑》69，022308（2004）。[31] Margarite L. LaBorde、Soorya Rethinasamy 和 Mark M. Wilde。“在量子计算机上检验对称性”。Quantum 7，1120（2023）。[32] 埃尔温·薛定谔。“量子力学的现状”。《自然科学》23，844–849（1935）。[33] 埃尔温·薛定谔。“关于分离系统间概率关系的讨论”。《剑桥哲学学会数学学报》31，555–563（1935）。[34] Daniel Cavalcanti 和 Paul Skrzypczyk。“量子导引：侧重半定规划的综述”。《物理学进展报告》80，024001（2016）。[35] Roope Uola、Ana C. S. Costa、H. Chau Nguyen 和 Otfried Gühne。“量子导引”。《现代物理评论》92，015001（2020）。[36]Shuheng Liu、Dongmei Han、Na Wang、Yu Xiang、Fengxiao Sun、Meihong Wang、Zhongzhong Qin、Qihuang Gong、Xiaolong Su 和 Qiongyi He。“实验演示远程制备

维格纳负性通过量子导引”。《物理评论快报》**128**，200401（2022年）。

[37]Marie Ioannou、Bradley Longstaff、Mikkel V. Larsen、Jonas S. Neergaard-Nielsen、Ulrik L. Andersen、Daniel Cavalcanti、Nicolas Brunner 和 Jonatan Bohr Brask。《基于量子导引的随机性认证：压缩态与零差测量》。《物理评论A辑》106，042414（2022年）。[38] Bernhard Wittmann、Sven Ramelow、Fabian Steinlechner、Nathan K. Langford、Nicolas Brunner、Howard M. Wiseman、Rupert Ursin 和 Anton Zeilinger。《通过量子导引实现无漏洞的爱因斯坦–波多尔斯基–罗森实验》。《新物理学杂志》14，053030（2012）。[39] Meng Wang、Yu Xiang、Qiongyi He 和 Qihuang Gong。《多体连续变量类格林伯格–霍恩–塞林格态中的量子导引检测》。《物理评论A辑》91，012112（2015）。[40] Michael A. Nielsen 和 Isaac L. Chuang。《量子计算与量子信息》。剑桥大学出版社。（2000）。[41] John Watrous。《量子计算复杂性》。《复杂性与系统科学百科全书》（2009）。[42] Thomas Vidick 和 John Watrous。《量子证明》。《理论计算机科学基础与趋势》11，1–215（2016）。[43]Jarrod R. McClean、Sergio Boixo、Vadim N. Smelyanskiy、Ryan Babbush 和 Hartmut Neven。《量子神经网络训练景观中的贫瘠高原》。《自然·通讯》9，4812（2018年）。[44] Marco Cerezo、Akira Sone、Tyler Volkoff、Lukasz Cincio 和 Patrick J. Coles。《浅层参数化量子电路中依赖于代价函数的贫瘠高原》。《自然·通讯》12，1791（2021年）。[45] Mirko Consiglio、Tony John George Apollaro 和 Marcin Wieśniak。《量子可分性问题的变分方法》。《物理评论A辑》106，062413（2022年）。[46] Xu-Fei Yin、Yuxuan Du、Yue-Yang Fei、Rui Zhang、Li-Zheng Liu、Yingqiu Mao、Tongliang Liu、Min-Hsiu Hsieh、Li Li、Nai-Le Liu、Dacheng Tao、Yu-Ao Chen 和 Jian-Wei Pan。《利用量子对抗求解器实现高效双体纠缠检测方案》。《物理评论快报》128，110501（2022年）。

[47] Kun Wang、Zhixin Song、Xuanqiang Zhao、Zihe Wang 和 Xin Wang。《在近期量子设备上检测并量化纠缠》。npjQuantum Information **8**，52 (2022年)。[48]A. D. Muñoz Moller、L. Pereira、L. Zambrano、J. Cortés-Vega 和 A. Delgado。《在含噪中等规模量子计算机中变分确定多量子比特几何纠缠》。《物理评论应用》**18**，024048(2022年)。

[49] George Androulakis 和 Ryan McGaha。《用于近似凸屋顶的变分量子算法》。《量子信息与计算》**22**，1081–1109（2022年）。

[50] John Watrous。《量子信息理论》。剑桥大学出版社。（2018年）。

[51] Michal Horodecki、Peter W. Shor 和 Mary Beth Ruskai。《纠缠破坏信道》。《数学物理评论》15，629–641（2003）。[52] A. Uhlmann。《态空间中的“跃迁概率”》。Reports on Mathematical Physics 9，273–279（1976）。[53] Marco Cerezo、Andrew Arrasmith、Ryan Babbush、Simon C. Benjamin、Suguru Endo、Keisuke Fujii、Jarrod R. McClean、Kosuke Mitarai、Xiao Yuan、Lukasz Cincio 和 Patrick J. Coles。《变分量子算法》。Nature Reviews Physics 3，625–644（2021）。[54] Sanjeev Arora 和 Boaz Barak。《计算复杂性：现代方法》。剑桥大学出版社（2009）。[55]Chris Marriott 和 John Watrous。《量子 Arthur–Merlin 博弈》。载于第19届 IEEE 计算复杂性年会论文集，275–285页。IEEE（2004）。[56] John Watrous。《抵御量子攻击的零知识》。载于第38届 ACM 计算理论研讨会年会论文集，296–305页（2006）。[57]Soorya Rethinasamy、Rochisha Agarwal、Kunal Sharma 和 Mark M. Wilde。《在量子计算机上估计可区分性度量》。《物理评论A辑》108，012409（2023）。[58]Matthew Treinish 等。《Qiskit：一个用于量子计算的开源框架》（2023）。https://doi.org/10.5281/zenodo.2573505.[59] Xuanqiang Zhao、Benchi Zhao、Zihe Wang、Zhixin Song 和 Xin Wang。《借助 LOCCNet 实现实用的分布式量子信息处理》。npj Quantum Information 7，159（2021）。

[60] Brian Doolittle、R. Thomas Bromley、Nathan Killoran 和 Eric Chitambar。《在含噪量子网络中对非定域性进行变分量子优化》。IEEE Transactions on Quantum Engineering 4，1–27（2023）。[61]Yun-Fei Niu、Shuo Zhang、Chen Ding、Wan-Su Bao 和 He-Liang Huang。《参数并行分布式变分量子算法》。SciPost Phys. 14，132（2023）。[62] Alexander Streltsov、Hermann Kampermann 和 Dagmar Bruß。《将纠缠距离度量与其凸屋顶联系起来》。《新物理学杂志》12，123004（2010）。[63] Tillmann Baumgratz、Marcus Cramer 和 Martin B. Plenio。《量化相干性》。《物理评论快报》113，140401（2014）。[64] J. Cramer、N. Kalb、M. A. Rol、B. Hensen、M. S. Blok、M. Markham、D. J. Twitchen、R. Hanson 和 T. H. Taminiau。《通过实时反馈，在连续编码的量子比特上重复进行量子纠错》。《自然·通讯》7，11526（2016）。[65] Laird Egan、Dripto M. Debroy、Crystal Noel、Andrew Risinger、Daiwei Zhu、Debopriyo Biswas、Michael Newman、Muyuan Li、Kenneth R. Brown、Marko Cetina 和 Christopher Monroe。《对纠错量子比特的容错控制》。《自然》598，281–286（2021）。[66] Rajeev Acharya 等。《通过扩展表面码逻辑量子比特来抑制量子错误》。《自然》614，676–681（2023）。[67]T. M. Graham、L. Phuttitarn、R. Chinnarasu、Y. Song、C. Poole、K. Jooya、J. Scott、A. Scott、P. Eichler 和 M. Saffman。《在单种中性碱金属原子量子处理器上进行电路中测量》。《物理评论X》13，041051（2023）。[68]Matthias Christandl、Robert König、Graeme Mitchison 和 Renato Renner。《一个半量子 de Finetti 定理》。《数学物理通讯》273，473–498（2007）。[69] Gavin K. Brennen。《多量子比特系统纯态的可观测纠缠度量》。《量子信息与计算》3，619–626（2003）。[70] Aram Harrow 和 Ashley Montanaro。《一种高效的乘积态检验方法及其在量子 Merlin–Arthur 博弈中的应用》。载于第51届IEEE计算机科学基础年会（FOCS）论文集，633–642页。美国内华达州拉斯维加斯（2010）。

[71]Adriano Barenco、André Berthiaume、David Deutsch、Artur Ekert、Richard Jozsa 和 Chiara Macchiavello。“通过对称化稳定量子计算”。《SIAM计算杂志》26，1541–1557（1997年）。[72] Harry Buhrman、Richard Cleve、John Watrous 和 Ronald de Wolf。“量子指纹”。《物理评论快报》87，167902（2001年）。[73]Bartosz Regula、Ludovico Lami 和 Alexander Streltsov。“量子相干的非渐近辅助蒸馏”。《物理评论A辑》98，052329（2018年）。[74] John Watrous。“完全有界范数的更简单半正定规划”。《芝加哥理论计算机科学杂志》（2013年）。[75]Hamza Fawzi。“除维数为 3×2外，可分态集合不存在有限半正定表示”。《数学物理通讯》386，1319–1335（2021年）。[76]Eric M. Rains。“可蒸馏纠缠的界限”。《物理评论A辑》60，179–184（1999年）。[77] Eric M. Rains。“可蒸馏纠缠的半正定规划”。IEEE信息论汇刊47，2921–2933（2001年）。[78]Lukasz Pankowski、Fernando G. S. L. Brandao、Michal Horodecki 和 Graeme Smith。“通过可扩展映射蒸馏纠缠”。《量子信息与计算》13，751–770（2013年）。[79] Eneet Kaur、Siddhartha Das、Mark M. Wilde 和 Andreas Winter。“可扩展性限制量子处理器的性能”。《物理评论快报》123，070502（2019年）。[80] Eneet Kaur、Siddhartha Das、Mark M. Wilde 和 Andreas Winter。“不可扩展性的资源理论与非渐近量子容量”。《物理评论A辑》104，022401（2021年）。[81] Mario Berta、Francesco Borderi、Omar Fawzi 和 Volkher Scholz。“约束双线性优化的半定规划层级”。《数学规划》194，781–829（2022年）。[82] Sumeet Khatri、Ryan LaRose、Alexander Poremba、Lukasz Cincio、Andrew T. Sornborger 和 Patrick J. Coles。“量子辅助量子编译”。Quantum 3，140（2019年）。[83]L. Zambrano、A. D. Muñoz-Moller、M. Muñoz、L. Pereira 和 A. Delgado。“避免变分确定几何纠缠中的贫瘠高原”。《量子科学与技术》9，025016（2024年）。

[84] Alexey E. Rastegin。“量子态的正弦距离”（2006年）。arXiv:quant-ph/0602112。[85] Christopher A. Fuchs 和 Jeroen van de Graaf。“量子力学态的密码学可区分性度量”。IEEE信息论汇刊 **45**，1216（1999年）。[86] Joel J. Wallman 和 Steven T. Flammia。“带置信度的随机基准测试”。《新物理学杂志》**16**，103032（2014年）。[87] Abhinav Kandala、Antonio Mezzacapo、Kristan Temme、Maika Takita、Markus Brink、Jerry M. Chow 和 Jay M. Gambetta。“适用于小分子和量子磁体的硬件高效变分量子本征求解器”。《自然》**549**，242–246（2017年）。[88] Guillaume Sagnol 和 Maximilian Stahlberg。“PICOS：锥优化求解器的 Python 接口 ”。《开放源代码软件期刊》**7**，3915（2022年）。[89]Lieven Vandenberghe。“CVX-OPT线性与二次锥规划求解器”。网址：http://www.seas.ucla.edu/van-denbe/publications/coneprog.pdf。[90] Vincent Russo。“TOQITO——量子信息理论工具包：用于研究量子信息的 Python 软件包”。《开放源代码软件期刊》**6**，3082（2021年）。

[91] Benjamin Schumacher。《量子编码》。《物理评论 A》**51**，2738–2747 (1995年)。[92] Nilanjana Datta、Min-Hsiu Hsieh 和 Mark M. Wilde。《量子率失真、反向香农定理与信源-信道分离》。IEEE信息论汇刊 **59**，615–630 (2013年)。[93] Koenraad M. R. Audenaert、Christopher A. Fuchs、Christopher King 和 Andreas Winter。《量子态集合的可访问保真度与量子性的可乘性》。《量子信息与计算》**4**，1–11(2004年)。[94] Valerio Scarani、Sofyan Iblisdir、Nicolas Gisin 和 Antonio Acín。《量子克隆》。《现代物理评论》**77**，1225–1256(2005年)。[95] John Watrous。《量子统计零知识的能力界限》。载于《第43届IEEE计算机科学基础年度研讨会论文集》。第459–468页。(2002年)。[96] Carl W. Helstrom。《检测理论与量子力学》。《信息与控制》**10**，254–291 (1967年)。[97] Carl W. Helstrom。《量子检测与估计理论》。《统计物理学杂志》**1**，231–252 (1969年)。

定理1的证明

在本附录中，我们证明定理1，说明混合态的第一个可分性检验的接受概率等于$\frac{1}{2}(1+F_s(\rho_{AB}))$。

定理1的证明。 回顾一下，纠缠破坏信道可以重写为 [51]

$$\mathcal{E}_{R\to A'}(\cdot)=\sum_x \mathrm{Tr}[\mu_R^x(\cdot)]\phi_{A'}^x, \tag{25}$$

其中$\{\mu_R^x\}_x$是一个秩一正算子值测度，而$\{\phi_{A'}^x\}_x$是一组纯态。于是，对于固定的$\mathcal{E}_{R\to A'}$，我们得到

$$\begin{aligned}\mathrm{Tr}[\Pi_{A'A}^{\mathrm{sym}}\mathcal{E}_{R\to A'}(\psi_{RAB})] &= \frac{1}{2}\mathrm{Tr}[(I_{A'A}+F_{A'A})\mathcal{E}_{R\to A'}(\psi_{RAB})] &(26)\\ &= \frac{1}{2}\left(1+\mathrm{Tr}[F_{A'A}\mathcal{E}_{R\to A'}(\psi_{RAB})]\right). &(27)\end{aligned}$$

那么，让我们来处理这个表达式$\mathrm{Tr}[F_{A'A}\mathcal{E}_{R\to A'}(\psi_{RAB})]$。考虑

$$\mathrm{Tr}[F_{A'A}\mathcal{E}_{R\to A'}(\psi_{RAB})]=\mathrm{Tr}\left[F_{A'A}\sum_x \mathrm{Tr}_R[\mu_R^x\psi_{RAB}]\otimes\phi_{A'}^x\right] \tag{28}$$

$$= \mathrm{Tr}\left[F_{A'A}\sum_x p(x)\psi^x_{AB}\otimes\phi^x_{A'}\right] \tag{29}$$

$$= \mathrm{Tr}\left[F_{A'A}\sum_x p(x)\psi^x_{A}\otimes\phi^x_{A'}\right] \tag{30}$$

$$= \sum_x p(x)\langle\phi^x|_A\psi^x_A|\phi^x\rangle_A, \tag{31}$$

其中

$$p(x) := \mathrm{Tr}[\mu^x_R\psi_{RAB}], \tag{32}$$

$$\psi^x_{AB} := \frac{1}{p(x)}\mathrm{Tr}_R[\mu^x_R\psi_{RAB}]. \tag{33}$$

因此，接　受概率对于固定的纠缠破坏信道可表示为

$$\mathrm{Tr}[\Pi^{\mathrm{sym}}_{A'A}\mathcal{E}_{R\to A'}(\psi_{RAB})] = \frac{1}{2}\left(1+\sum_x p(x)\langle\phi^x|_A\psi^x_A|\phi^x\rangle_A\right). \tag{34}$$

对$\mathrm{EB}_{R\to A'}$中的每个元素进行优化后，其中 R 表示所有输入系统为 A'、输出系统为 的纠缠破坏信道所构成的集合；并注意到，对 $\mathcal{E}_{R\to A'}$ 中的测量进行优化会得到 ρ_{AB} 的纯态分解，而对 $\mathcal{E}_{R\to A'}$ 中的制备信道进行优化则给出 ψ^x_A的谱范数，将其与附录 B 和 C中的推导结合起来，即可得到所述的接受概率公式:

$$\max_{\mathcal{E}\in\mathrm{EB}_{R\to A'}}\mathrm{Tr}[(\Pi^{\mathrm{sym}}_{A'A}\otimes I_{RB})\mathcal{E}_{R\to A'}(\psi_{RAB})] = \frac{1+F_s(\rho_{AB})}{2}. \tag{35}$$

证明至此完成。 ■

方程 (19) 的另一种证明

本附录给出 [62] 中定理 1 的另一种证明。该证明依赖于乌尔曼定理 [52], 三角不等式和柯西–施瓦茨不等式。另请参见 [73, 引理 1]。

定理 4（[62]） 对于量子态 ρ_{AB}，以下公式成立

$$F_s(\rho_{AB}) = \max_{\{(p(x),\psi^x_{AB})\}_x}\left\{\sum_x p(x)F_s(\psi^x_{AB}) : \rho_{AB} = \sum_x p(x)\psi^x_{AB}\right\}, \tag{36}$$

其中纯态系综 $\{(p(x)\ \psi^x_{AB})\}_x$ 满足 $\sum_x p(x)\ \psi^x_{AB} = \rho_{AB}$，所有 ψ^x_{AB} 均为纯态，并且

$$F_s(\psi_{AB}) = \max_{|\phi\rangle_A,|\varphi\rangle_B}|\langle\psi|_{AB}|\phi\rangle_A\otimes|\varphi\rangle_B|^2. \tag{37}$$

证明。 由于 (5) 中的定义要求对所有可分态进行优化，因此我们取 $|\mathcal{X}| = (|A|\,|B|)^2$。 (1) 中的可分量子态由以下方式纯化

$$|\psi^\sigma\rangle_{RAB} = \sum_{x\in\mathcal{X}}\sqrt{p(x)}|x\rangle_R|\psi^x\rangle_A|\phi^x\rangle_B. \tag{38}$$

现在考虑一个一般的纯化 $|\psi^{\rho}\rangle_{R'AB}$，其对应的量子态为 ρ_{AB}。回想一下，净化系统 R' 的维度满足 $\text{rank}(\rho_{AB}) \leq |R'|$，因此我们可以直接设定 $|R'| = |A||B|$。令 R'' 为一个维度为 $|A||B|$的系统，则有

$$|\psi^{\rho}\rangle_{R'AB}|0\rangle_{R''} \tag{39}$$

进行净化 ρ_{AB}。应用乌尔曼定理 [52], 可将最大可分根保真度写为

$$\max_{\sigma_{AB}\in \text{SEP}(A:B)} \sqrt{F}(\rho_{AB},\sigma_{AB}) = \max_{\substack{U,\\ \{(p(x),\psi^x{}_A,\phi^x_B)\}_x}} \left| \left(\sum_{x'} \sqrt{p(x')} \langle x'|_R \langle \psi^{x'}|_A \langle \phi^{x'}|_B \right) \left(U_{R'R''\to R}\otimes I_{AB}\right) |\psi^{\rho}\rangle_{R'AB}|0\rangle_{R''} \right|, \tag{40}$$

其中，最大化遍历所有酉算子 $U_{R'R''\to R}$。将 $U_{R'R''\to R}|\psi^{\rho}\rangle_{R'AB}|0\rangle_{R''}$ 按标准基 $|x\rangle$ 展开为

$$U_{R'R''\to R}|\psi^{\rho}\rangle_{R'AB}|0\rangle_{R''} = \sum_{x\in\mathcal{X}} \sqrt{q(x)}|x\rangle_R|\varphi^x\rangle_{AB}, \tag{41}$$

注意到，U 随后在标准基下进行测量，会将 ρ_{AB} 凸分解为由系综 $\{(q(x)\ \varphi^x_{AB})\}_x$表示的形式。根保真度可写为

$$\begin{aligned}
\max_{\sigma_{AB}\in \text{SEP}(A:B)} \sqrt{F}(\rho_{AB},\sigma_{AB}) &= \max_{\substack{\{(p(x),\psi^x{}_A,\phi^x_B)\}_x,\\ \{(q(x),\varphi^x_{AB})\}_x}} \left| \sum_{x,x'} \sqrt{q(x)p(x')} \langle x|x'\rangle_R \langle \varphi^x|_{AB}|\psi^{x'}\rangle_A |\phi^{x'}\rangle_B \right| \\
&= \max_{\substack{\{(p(x),\psi^x{}_A,\phi^x_B)\}_x,\\ \{(q(x),\varphi^x_{AB})\}_x}} \left| \sum_{x} \sqrt{q(x)p(x)} \langle \varphi^x|_{AB}|\psi^x\rangle_A |\phi^x\rangle_B \right| \qquad (42)\\
&= \max_{\substack{\{(p(x),\psi^x{}_A,\phi^x_B)\}_x,\\ \{(q(x),\varphi^x_{AB})\}_x}} \left| \sum_{x} \sqrt{q(x)p(x)} \langle \varphi^x|_{AB}|\psi^x\rangle_A |\phi^x\rangle_B \right|. \qquad (43)
\end{aligned}$$

接下来，对于固定的 $\{(p(x)\ \psi^x{}_A,\phi^x_B)\}_x$ 和 $\{(q(x)\ \varphi^x_{AB})\}_x$，我们对上述优化问题中的目标函数作如下界定:

$$\begin{aligned}
\left| \sum_{x} \sqrt{q(x)p(x)} \langle \varphi^x|_{AB}|\psi^x\rangle_A |\phi^x\rangle_B \right| &\leq \sum_x \sqrt{p(x)q(x)}\, |\langle \varphi^x|_{AB}|\psi^x\rangle_A |\phi^x\rangle_B| \qquad (44)\\
&\leq \sqrt{\sum_x p(x)} \sqrt{\sum_x q(x)\, |\langle \varphi^x|_{AB}|\psi^x\rangle_A |\phi^x\rangle_B|^2} \qquad (45)\\
&= \sqrt{\sum_x q(x)\, |\langle \varphi^x|_{AB}|\psi^x\rangle_A |\phi^x\rangle_B|^2}. \qquad (46)
\end{aligned}$$

第一个不等式由三角不等式得出，第二个则是应用柯西–施瓦茨不等式的结果。我们看到，通过选择

$$p(x) = \frac{q(x)\, |\langle \varphi^x|_{AB}|\psi^x\rangle_A |\phi^x\rangle_B|^2}{\sum_x q(x)\, |\langle \varphi^x|_{AB}|\psi^x\rangle_A |\phi^x\rangle_B|^2}. \tag{47}$$

通过为量子态 $|\psi^x\rangle_A$ 调整全局相位，即可使第一个不等式取等号，这相当于在（38）中引入相对相位。综合以上结果，我们得出

$$\max_{\sigma_{AB}\in\mathrm{SEP}} F(\rho_{AB},\sigma_{AB}) = \max_{\{(q(x),\varphi^x_{AB})\}_x} \sum_x q(x) \max_{(|\psi^x\rangle_A|\phi^x\rangle_B)_x,} \left|\langle\varphi^x|_{AB}|\psi^x\rangle_A|\phi^x\rangle_B\right|^2, \tag{48}$$

这等价于所需的等式 (19)。 ■

C 式 (20) 的证明

在本附录中，我们证明，双体态的可分性保真度可以用谱范数表示； [62, 第 6 节2]中也观察到了这一点。

命题 5 对于双体态 ρ_{AB}，以下等式成立

$$F_s(\rho_{AB}) = \max_{\left\{(p(x),\psi^x_{AB})\right\}_x} \left\{ \sum_x p(x) \left\|\psi^x_A\right\|_\infty : \rho_{AB} = \sum_x p(x)\psi^x_{AB} \right\}. \tag{49}$$

证明。 对于纯双部态 ψ_{AB}，以下关系成立：

$$\begin{aligned}
F_s(\psi_{AB}) &= \max_{|\phi\rangle_A,|\varphi\rangle_B} \left|\langle\psi|_{AB}|\phi\rangle_A \otimes |\varphi\rangle_B\right|^2 && (50)\\
&= \max_{|\phi\rangle_A,|\varphi\rangle_B} \left|\langle\phi|_A \otimes \langle\varphi|_B|\psi\rangle_{AB}\right|^2 && (51)\\
&= \max_{|\phi\rangle_A} \left\|\langle\phi|_A \otimes I_B|\psi\rangle_{AB}\right\|_2^2 && (52)\\
&= \max_{|\phi\rangle_A} \mathrm{Tr}[(|\phi\rangle\langle\phi|_A \otimes I_B)\psi_{AB}] && (53)\\
&= \max_{|\phi\rangle_A} \mathrm{Tr}[|\phi\rangle\langle\phi|_A\psi_A] && (54)\\
&= \left\|\psi_A\right\|_\infty . && (55)
\end{aligned}$$

前两个等式由定义和改写得出。第三个等式源于向量欧几里得范数的变分刻画。第四个等式成立是因为

$$\begin{aligned}
\left\|\langle\phi|_A \otimes I_B|\psi\rangle_{AB}\right\|_2^2 &= \left(\langle\psi|_{AB}|\phi\rangle_A \otimes I_B\right)\left(\langle\phi|_A \otimes I_B|\psi\rangle_{AB}\right) && (56)\\
&= \langle\psi|_{AB}|\phi\rangle\langle\phi|_A \otimes I_B|\psi\rangle_{AB} && (57)\\
&= \mathrm{Tr}[(|\phi\rangle\langle\phi|_A \otimes I_B)\psi_{AB}]. && (58)
\end{aligned}$$

下一步可通过取偏迹得到，而最后一个等式则来自谱范数的变分刻画。因此，应用 (19). ■

定理2的证明

在本附录中，我们证明，如果参数化酉电路能够表示各自系统的所有可能酉算子，那么我们的 VQSA 的接受概率确实等于 $F_s(\rho_{AB})$。为此，让我们追踪 VQSA 在图 9所示各点处的量子态。

- 在步骤（1）中，酉算子 U^ρ 制备出纯态 ψ_{RAB}。这是 ρ_{AB} 的一个特定初始纯化。

•在步骤（2）中，我们将参数化幺正电路 $W_R(\Theta)$ 应用于 ψ_{RAB}。将$W_R(\Theta)|\psi^\rho\rangle_{RAB}$ 按标准基 $\{|x\rangle\}_x$ 展开，可得

$$W_R(\Theta)|\psi\rangle_{RAB} = \sum_{x\in\mathcal{X}} \sqrt{q(x)}|x\rangle_R|\varphi^x\rangle_{AB}. \tag{59}$$

• 在步骤（3）中，测量结果 x 以概率 $q(x)$ 出现，此时寄存器 A和 B 的状态向量变为 $|\varphi^x\rangle_{AB}$。

• 在步骤（4）中，根据测量结果 x，我们对寄存器 A应用参数化幺正电路 $U_A^x(\Theta^x)$。此时状态向量为 $U_A^x(\Theta^x)|\varphi^x\rangle_{AB}$。

• 在步骤（5）中，我们对 B 求迹，并在标准基下测量 A 。当得到全零结果时，我们接受。因此，接受概率等于

$$\sum_{x\in\mathcal{X}} q(x)\langle 0|U_A^x(\Theta^x)\varphi_A^x(U_A^x)^\dagger|0\rangle = \sum_{x\in\mathcal{X}} q(x)\langle\phi^x|_A\varphi_A^x|\phi^x\rangle_A, \tag{60}$$

其中，我们定义了 $|\phi^x\rangle_A := (U_A^x)^\dagger|0\rangle$。

• 最大化接受概率对应于对 $W_R(\Theta)$ 和 $U_A^x(\Theta^x)$ 的参数进行最大化。

• 对 W_R 的参数进行最大化，等价于对 ρ_{AB} 的所有可能纯态分解进行最大化。

• 对 $U_A^x(\Theta^x)$ 的参数进行最大化，就是最大化 $\langle\phi^x|\varphi_A^x|\phi^x\rangle$，其结果为 $\|\varphi_A^x\|_\infty$。

• 最大接受概率等于

$$\max_{\{(p(x),\psi_{AB}^x)\}_x}\left\{\sum_x p(x)\|\varphi_A^x\|_\infty : \rho_{AB} = \sum_x p(x)\psi_{AB}^x\right\}, \tag{61}$$

根据命题 5，这又等于 $F_s(\rho_{AB})$。

这证明，如果参数化酉电路能够表示作用于各自系统的所有可能酉算子，那么最大接受概率等于 $F_s(\rho_{AB})$。不过，我们注意到，用于参数化酉电路的任何试探形式，其表达能力都是有限的。因此，原则上，如果使用表达能力更强的试探形式，通过 VQSA 得到的最大接受概率也会更接近 $F_s(\rho_{AB})$ 的实际值。

E 首个基准测试半定规划 $\widetilde{F}_s^1$ 与方程 (21) 的证明

本附录详细推导了我们的第一个基准测试半定规划 $\widetilde{F}_s^1$，该规划基于保真度的半定规划 [74]。设 ρ_{AB} 和 σ_{AB} 为双体态。根保真度 $\sqrt{F}(\rho_{AB},\ \sigma_{AB})$ 的半定规划利用了乌尔曼定理 [52], ，如下所示：

$$\sqrt{F}(\rho_{AB},\sigma_{AB}) = \max_{X_{AB}\in\mathcal{L}(\mathcal{H}_{AB})}\left\{\ \mathrm{Re}[\mathrm{Tr}[X_{AB}]] : \begin{bmatrix}\rho_{AB} & X_{AB}\\ X_{AB}^\dagger & \sigma_{AB}\end{bmatrix}\geq 0\ \right\}, \tag{62}$$

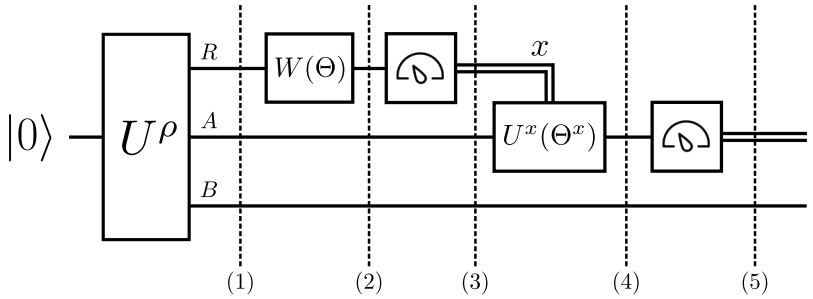


图 9：用于估计可分性保真度 $F_s(\rho_{AB})$ 的 VQSA。酉电路 U^ρ 生成量子态 ψ_{RAB}，这是 ρ_{AB} 的一种纯化。参数化电路 $W_R(\Theta)$ 作用于 R，使 ψ_{RAB} 演化为 ρ_{AB} 的另一种纯态分解。随后进行测量；若测量结果 x 出现，系统 AB 将被引导至纯态 ψ^x_{AB}。在测量结果 x的条件下，最终的参数化电路 $U^x_A(\Theta^x)$及其后的测量用于估计 $\|\psi^x_A\|_\infty$。

其中 $\mathcal{L}(\mathcal{H}_{AB})$ 是作用于希尔伯特空间 $\mathcal{H}_{AB}$ 上的所有线性算子的集合 .

理想情况下，我们希望在所有可分态构成的集合上进行最大化，但众所周知，在该集合上进行优化在计算上具有挑战性 [3, 4]。此外，通常无法用半定约束来刻画可分态集合 [75]。因此，我们通过约束 σ_{AB} 具有正偏转置（PPT） [27,28] 且为 k-可扩展的 [29, 30], 来近似该集合，因为所有可分态都满足这些约束。令 $\widetilde{F}^1_s(\rho_{AB})$表示由此得到的量，其平方根定义如下：

$$\sqrt{\widetilde{F}^1_s}(\rho_{AB},k) := \max_{\substack{X_{AB}\in\mathcal{L}(\mathcal{H}_{AB}),\\ \sigma_{AB^k}\geq 0}} \left\{ \begin{array}{c} \mathrm{Re}[\mathrm{Tr}[X_{AB}]]: \\ \begin{bmatrix} \rho_{AB} & X_{AB} \\ X^\dagger_{AB} & \sigma_{AB_1} \end{bmatrix} \geq 0, \\ \mathrm{Tr}[\sigma_{AB^k}] = 1, \\ \sigma_{AB^k} = \mathcal{P}_{B^k}(\sigma_{AB^k}), \\ T_{B_{1\cdots j}}(\sigma_{AB_{1\cdots j}}) \geq 0 \quad \forall j \in \{1,\ldots,k\} \end{array} \right\}, \tag{63}$$

其中 $B^k \equiv B_1 \cdots B_k$，记号 T_R 表示作用于系统 R上的偏转置映射，并且$\mathcal{P}_{B^k}$ 表示对系统 B_1 至 B_k 执行均匀随机置换的信道。现在证明 (21) 中的不等式。根据上文讨论的包含关系，注意到

$$F_s(\rho_{AB}) \leq \widetilde{F}^1_s(\rho_{AB},k). \tag{64}$$

关于 $\widetilde{F}^1_s(\rho_{AB},k)$ 的另一个界，可用 $F_s(\rho_{AB})$ 表示如下：

$$\sqrt{1-F_s(\rho_{AB})} \leq \sqrt{1-\widetilde{F}^1_s(\rho_{AB},k)} + 2\sqrt{\frac{|B|^2}{k}\left(1-\frac{|B|^2}{k}\right)}, \tag{65}$$

可将其改写为(21)中的形式：

$$\widetilde{F}^1_s(\rho_{AB},k) \leq 1 - \left[\sqrt{1-F_s(\rho_{AB})} - 2\sqrt{\frac{|B|^2}{k}\left(1-\frac{|B|^2}{k}\right)}\right]^2. \tag{66}$$

这是 [68, 定理 II.7'], 正弦距离三角不等式 [84], 以及 Fuchs-van-de-Graaf不等式 [85]的推论。具体而言，考虑

$$\widetilde{F}^1_s(\rho_{AB},k) = \max_{\sigma_{AB}\in\text{EXT-PPT}_k} F(\rho_{AB},\sigma_{AB}) \tag{67}$$

$$\leq \max_{\sigma_{AB}\in \mathrm{EXT}_k} F(\rho_{AB},\sigma_{AB}), \tag{68}$$

其中 $\mathbf{EXT\text{-}PPT}_k$ 表示 σ_{AB} 在(63) 中优化的集合，而 $\mathbf{EXT}_k$ 是k-可延拓量子态的集合。现在回想一下，对于所有 $\omega_{AB}^k \in \mathrm{EXT}_k$ (参见 [68, 定理 II.7'] 以及上文紧接 [68,定理 II.2] 中关于范数约定的说明)

$$\min_{\sigma_{AB}\in \mathrm{SEP}(A:B)} \frac{1}{2}\left\|\omega_{AB}^k-\sigma_{AB}\right\|_1 \leq \frac{2\left|B\right|^2}{k}, \tag{69}$$

正弦距离满足三角不等式 [84]:

$$\sqrt{1-F(\omega,\tau)} \leq \sqrt{1-F(\omega,\xi)}+\sqrt{1-F(\xi,\tau)}, \tag{70}$$

以及 Fuchs-van-de-Graaf 不等式 [85]:

$$1-\sqrt{F}(\omega,\tau) \leq \frac{1}{2}\left\|\omega-\tau\right\|_1, \tag{71}$$

其中 ω、 τ 和 ξ 是量子态。若 $\frac{1}{2}\left\|\omega-\tau\right\|_1 \leq \varepsilon$，则后者意味着

$$1-\sqrt{F}(\omega,\tau)\leq\varepsilon \;\Leftrightarrow\; \sqrt{1-F(\omega,\tau)} \leq \sqrt{\varepsilon\,(2-\varepsilon)}. \tag{72}$$

令 σ_{AB}^k 为（68）中的最优选择，并令 σ'_{AB} 为 $\min_{\sigma_{AB}\in \mathrm{SEP}(A:B)} \frac{1}{2}\left\|\omega_{AB}^k-\sigma_{AB}\right\|_1$ 的最优选择，则这意味着

$$\min_{\sigma_{AB}\in \mathrm{SEP}(A:B)} \sqrt{1-F(\rho_{AB},\sigma_{AB})} \leq \sqrt{1-F(\rho_{AB},\sigma'_{AB})} \tag{73}$$

$$\leq \sqrt{1-F(\rho_{AB},\sigma_{AB}^k)}+\sqrt{1-F(\sigma'_{AB},\sigma_{AB}^k)} \tag{74}$$

$$\leq \sqrt{1-F(\rho_{AB},\sigma_{AB}^k)}+2\sqrt{\frac{\left|B\right|^2}{k}\left(1-\frac{\left|B\right|^2}{k}\right)}. \tag{75}$$

重新整理并应用 (67)–(68)，即可得到 (65) 中所述的不等式。

F 第二部分：半定规划基准测试 $\widetilde{F}_s^2$ 及方程 (23) 的证明

在本附录中，我们详细推导第二个基准半定规划 $\widetilde{F}_s^2$，这是一个用于近似正文中(4) 的半定规划。考虑导致(4) 的分布式量子计算的一种变体：此时，我们不再将证明者限制为只能使用纠缠破坏信道，而是要求证明者发送回 k 个标记为 $A_1\cdots A_k$的系统。然后，验证者随机选择其中一个 k 系统，并对量子态 ψ_{RAB}的 A 系统执行交换测试。随机选择的目的，是有效地将证明者的输出约化为一个近似的纠缠破坏信道。注意，由此得到的交互式证明属于 QIP(2)。更具体地说，该交互式证明系统的接受概率为

$$\max_{\mathcal{P}_{R\to A'_1\cdots A'_k}} \mathrm{Tr}[\Pi^{\mathrm{sym}}_{A'A}\overline{\mathcal{P}}_{R\to A'}(\psi_{RAB})], \tag{76}$$

其中

$$\overline{\mathcal{P}}_{R\to A'} := \frac{1}{k}\sum_{i=1}^{k}\mathrm{Tr}_{A_1^{k\prime}\setminus A_i}\circ\mathcal{P}_{R\to A'_1\cdots A'_k}, \tag{77}$$

且$\mathcal{P}$ 是任意信道。注意到$\mathcal{P}_{R\to A'}$ 是一个 k-可扩展信道 [78, 79, 80, 81], 由此可知

$$\max_{\mathcal{P}_{R\to A'_1\cdots A'_k}} \operatorname{Tr}[\Pi^{\mathrm{sym}}_{A'A}\overline{\mathcal{P}}_{R\to A'}(\psi_{RAB})] = \max_{\mathcal{E}^k_{R\to A'}\in \mathrm{EXT}_k} \operatorname{Tr}[\Pi^{\mathrm{sym}}_{A'A}\mathcal{E}^k_{R\to A'}(\psi_{RAB})], \tag{78}$$

其中 $\mathbf{EXT}_k$ 表示 k-可扩展信道的集合。其定义为$\mathcal{E}^k_{R\to A'}(\rho_{SR}) \in \mathrm{EXT}_k(S{:}A')$ 对每个输入态 ρ_{SR}都成立，其中 $\mathbf{EXT}_k(S:A')$ 表示 k- 可扩展态的集合。因此，式 (78) 中的量是式 (4) 的一个上界，由以下半定规划给出:

$$\max_{\Gamma^{\mathcal{E}^k}_{RA'^k}\geq 0} \left\{ \begin{array}{c} \operatorname{Tr}[\Pi^{\mathrm{sym}}_{A'A}\operatorname{Tr}_R[T_R(\psi_{RAB})\Gamma^{\mathcal{E}^k}_{RA'_1}]] : \\ \operatorname{Tr}_{A'^k}[\Gamma^{\mathcal{E}^k}_{RA'^k}] = I_R, \\ \Gamma^{\mathcal{E}^k}_{RA'^k} = \mathcal{P}_{A'^k}(\Gamma^{\mathcal{E}^k}_{RA'^k}) \end{array} \right\}, \tag{79}$$

其中 $\Gamma^{\mathcal{E}^k}_{RA'}$ 是$\mathcal{E}^k$ 的 Choi算子，且$\mathcal{P}_{A'^k}$ 是对各系统进行随机置换的信道 A'^k。我们可以在这个半定规划中加入更多正偏转置约束；所得结果仍是式(4)的上界，并由此得到我们的第二个基准 $\widetilde{F}^2_s(\rho_{AB},k)$:

$$\frac{1}{2}(1+\widetilde{F}^2_s(\rho_{AB},k)) \coloneqq \max_{\Gamma^{\mathcal{E}^k}_{RA'^k}\geq 0} \left\{ \begin{array}{c} \operatorname{Tr}[\Pi^{\mathrm{sym}}_{A'A}\operatorname{Tr}_R[T_R(\psi_{RAB})\Gamma^{\mathcal{E}^k}_{RA'_1}]] : \\ \operatorname{Tr}_{A'^k}[\Gamma^{\mathcal{E}^k}_{RA'^k}] = I_R, \\ \Gamma^{\mathcal{E}^k}_{RA'^k} = \mathcal{P}_{A'^k}(\Gamma^{\mathcal{E}^k}_{RA'^k}), \\ T_{A'_{1\cdots j}}(\Gamma^{\mathcal{E}^k}_{RA'^k}) \geq 0 \quad \forall j\in\{1,\ldots,k\} \end{array} \right\} \tag{80}$$

其中，映射 T_R 是作用于系统 R上的偏转置映射。

以下定理说明了 $\widetilde{F}^2_s$ 如何逼近 $F_s(\rho_{AB})$。

命题 6 对于双体态 ρ_{AB}，以下上界成立:

$$F_s(\rho_{AB}) \leq \widetilde{F}^2_s(\rho_{AB},k) \leq F_s(\rho_{AB}) + \frac{4\left|A\right|^3\left|B\right|}{k}. \tag{81}$$

证明。 由于每个纠缠破坏信道都是 k-可扩展的，我们可以直接得到

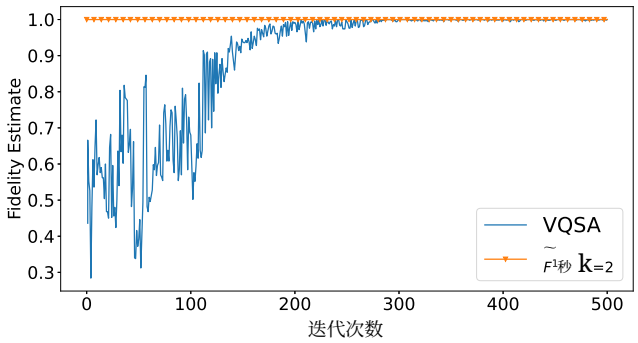
$$\begin{aligned} \frac{1+F_s(\rho_{AB})}{2} &= \max_{\mathcal{E}\in\mathrm{EB}} \operatorname{Tr}[(\Pi^{\mathrm{sym}}_{A'A}\otimes I_{RB})\mathcal{E}_{R\to A'}(\psi_{RAB})] &(82)\\ &\leq \max_{\mathcal{E}^k_{R\to A'}\in \text{EXT-PPT}_k} \operatorname{Tr}[(\Pi^{\mathrm{sym}}_{A'A}\otimes I_{RB})\mathcal{E}^k_{R\to A'}(\psi_{RAB})] &(83)\\ &= \frac{1+\widetilde{F}^2_s(\rho_{AB},k)}{2}, &(84)\end{aligned}$$

其中 $\mathbf{EXT\text{-}PPT}_k$ 表示满足 (80) 中约束条件的信道集合。考虑以下针对 k-可扩展量子态 ω^k_{AB} [68, 定理 II.7'] （关于其范数约定，另见 [68, 定理 II.2]之前）：

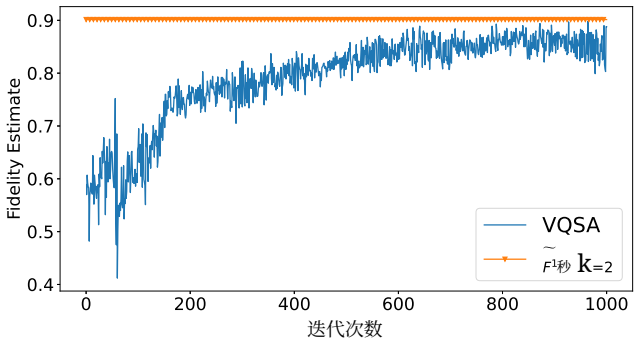
$$\min_{\sigma_{AB}\in\mathrm{SEP}(A:B)} \frac{1}{2}\left\|\omega^k_{AB}-\sigma_{AB}\right\|_1 \leq \frac{2\left|B\right|^2}{k}. \tag{85}$$

我们可以利用它以及 [86, 引理 7] 的结果得出

$$\min_{\mathcal{E}\in\mathrm{EB}} \frac{1}{2}\left\|\mathcal{E}^k-\mathcal{E}\right\|_\diamond \leq \frac{2\left|R\right|\left|A'\right|^2}{k}. \tag{86}$$



(a) 使用 VQSA 的局部奖励函数计算随机乘积态的可分性保真度，并与 F_s^1 进行基准比较$\widetilde{}$。



(b) 使用 VQSA 的局部奖励函数计算随机纠缠态的可分性保真度，并与 F_s^1 进行基准比$\widetilde{}$较。

图 10: 可分性保真度 使用 VQSA 的局部奖励函数估计，并以 $\widetilde{F}_s^1$ 为基准的可分性保真度 .

然后考虑，对于每个固定的 $\mathcal{E}_{R\to A'}^k \in$ EXT-正偏转置$_k$，都存在一个纠缠破坏信道 $\mathcal{E}$ 满足

$$\frac{1}{2}\left\|\mathcal{E}^k-\mathcal{E}\right\|_\diamond \leq \frac{2\left|R\right|\left|A'\right|^2}{k}. \tag{87}$$

然后我们发现

$$\begin{aligned}
&\mathrm{Tr}[(\Pi_{A'A}^{\mathrm{sym}}\otimes I_{RB})\mathcal{E}_{R\to A'}^k(\psi_{RAB})] \\
&\leq \mathrm{Tr}[(\Pi_{A'A}^{\mathrm{sym}}\otimes I_{RB})\mathcal{E}_{R\to A'}(\psi_{RAB})]+\frac{2\left|R\right|\left|A'\right|^2}{k} &(88)\\
&\leq \max_{\mathcal{E}\in\mathrm{EB}}\mathrm{Tr}[(\Pi_{A'A}^{\mathrm{sym}}\otimes I_{RB})\mathcal{E}_{R\to A'}(\psi_{RAB})]+\frac{2\left|R\right|\left|A'\right|^2}{k} &(89)\\
&= \frac{1+F_s(\rho_{AB})}{2}+\frac{2\left|R\right|\left|A'\right|^2}{k}. &(90)
\end{aligned}$$

由于该不等式对每个 $\mathcal{E}_{R\to A'}^k \in$ EXT-PPT$_k$ 都成立，因此可得

$$\max_{\mathcal{E}_{R\to A'}^k\in\mathrm{EXT\text{-}PPT}_k}\mathrm{Tr}[(\Pi_{A'A}^{\mathrm{sym}}\otimes I_{RB})\mathcal{E}_{R\to A'}^k(\psi_{RAB})] \leq \frac{1+F_s(\rho_{AB})}{2}+\frac{2\left|R\right|\left|A'\right|^2}{k}. \tag{91}$$

回顾 $|R|\leq|A||B|$，注意到 $|A|=|A'|$，并进行一些简单的代数运算后，即完成证明。 ■

注 7 尽管命题 6中的上界修正项会随着 k的增加而减小，但显然，若要使其任意小， k 需要大于 $|A|^3|B|$；对于量子态 ρ_{AB}而言，该值相对于量子比特数呈指数增长。因此，这种方法无法高效地将可分性保真度估计问题纳入 *QIP(2)*，甚至 *QIP*。

G 更多模拟与细节

本文所有模拟中的输入态和参数化酉算子均使用硬件高效拟设（HEA） [87]生成。HEA 由若干层组成，每层包含

图	量子比特数	量子态 ρ_{AB}	层数
3	$R=2,\ A=1,\ B=1$	$(3/4)\lvert\Phi^+\rangle\langle\Phi^+\rvert + (1/4)\lvert\Phi^-\rangle\langle\Phi^-\rvert$	W_R 层数 $=2$ U_A^x 层数 $=2$
4	$R=4,\ A=2,\ B=2$	$(\mathcal{D}_{p,A_1}\otimes\mathcal{D}_{p,A_2}\otimes\mathbb{I}_B)(\lvert\psi\rangle\langle\psi\rvert)$ $\lvert\psi\rangle = \frac{1}{\sqrt{2}}(\lvert 0\rangle_{A_1}\lvert 0\rangle_{A_2}\lvert 00\rangle_B + \lvert 1\rangle_{A_1}\lvert 1\rangle_{A_2}\lvert 11\rangle_B)$	W_R 层数 $=4$ U_A^x 层数 $=4$
10(a)	$R=3,\ A=2,\ B=2$	使用硬件高效拟设的随机乘积态 [87]	W_R 层数 $=4$ U_A^x 层数 $=4$
10(b)	$R=3,\ A=2,\ B=2$	使用硬件高效拟设生成的随机纠缠态 [87]	W_R 层数 $=4$ U_A^x 层数 $=4$

表 1：所有 VQSA 模拟的详细信息。

每个量子比特对应两个参数，用于指定绕 x 轴和 y 轴的旋转。每层旋转之后，都会接上一系列相邻量子比特之间的受控非门。使用 HEA 生成输入态时，我们将旋转角固定，因此得到固定的输入态。对于参数化酉算子，旋转角作为参数，并通过优化来确定。

在图10(a)中，我们报告了生成随机二部乘积态后的模拟结果，其中每个分区包含两个量子比特。我们从生成输入态 ρ 的硬件高效拟设中移除所有受控非门，以确保得到乘积态。我们使用 VQSA 的局部奖励函数和基准 $\widetilde{F}_s^1$计算可分性保真度；后者见附录E。

在图10(b)中，我们对随机双体态进行了相同的处理，其中分区 A 和 B分别包含两个和一个量子比特，参考系统包含三个量子比特。

我们按以下方式生成所有参数化酉电路。我们使用 Qiskit Aer 模拟器和 Qiskit 的同时扰动随机近似（SPSA）优化器进行经典优化。其他所有细节见表1。VQSA 的局部奖励函数需要更多经典处理（例如随机挑选一个量子比特进行测量），而且似乎需要更多迭代次数才能达到正确值。不过，这些缺点被其较不易出现贫瘠高原这一优势所抵消。关于局部代价函数的更多细节见附录L。

H 软件

我们的所有 Python 源文件均可从本文的 arXiv 页面获取。我们使用含噪 Qiskit Aer 模拟器进行了所有模拟。我们使用 Picos Python 软件包 [88] 调用 CVXOPT 求解器 [89] 来求解半定规划，并使用 toqito Python 软件包 [90] 对表示量子系统的矩阵执行特定操作。

I 多部情形

本附录讨论 混合态可分性检验的多部推广 .

定义 8 若量子态 $\rho_{A_1\cdots A_M}\in D(H_{A_1\cdots A_M}) = D(H_{A_1}\otimes\cdots\otimes H_{A_M})$ 可以写成如下形式，则称其为可分量子态：

$$\rho_{A_1\cdots A_M} = \sum_{x\in\mathcal{X}} p(x)\psi_{A_1}^{x,1}\otimes\cdots\otimes\psi_{A_M}^{x,M}, \tag{92}$$

其中 $\{p(x)\}_{x\in\mathcal{X}}$ 是一个概率分布，而对于所有 $x \in X$ 和 $i \in\{1,\ldots,M\}$，$\psi^{x,i}_{A_i}$ 都是纯态。

令 M-SEP 表示所有满足 $\rho_{A_1\cdots A_M}$ 可分的 $\rho_{A_1\cdots A_M} \in\mathcal{D}(\mathcal{H}_{A_1\cdots A_M})$ 的集合。以下定理对后续分析至关重要。

定理 9 ([62]) 以下公式成立

$$\max_{\sigma_{A_1\cdots A_M}\in M\text{-SEP}} F(\rho_{A_1\cdots A_M},\sigma_{A_1\cdots A_M}) = \max_{\{(q(x),\varphi^x_{A_1\cdots A_M})\}_x} \sum_x q(x)F_s(\varphi^x_{A_1\cdots A_M}), \tag{93}$$

其中，优化遍历 $\{(q(x)\,\varphi^x_{A_1\cdots A_M})\}_x$ 的所有纯态分解 $\rho_{A_1\cdots A_M}$（类似于定理 4中的分解），并且

$$F_s(\varphi^x_{A_1\cdots A_M}) = \max_{\left\{|\phi^{x,i}\rangle_{A_i}\right\}_{i=1}^M} \left|\langle\varphi^x|_{A_1\cdots A_M}|\phi^{x,1}\rangle_{A_1}\otimes\cdots\otimes|\phi^{x,M}\rangle_{A_M}\right|^2. \tag{94}$$

对于分布式量子计算的多体情形，验证者制备 $\psi^\rho_{RA_1\cdots A_M}$ 的纯化态，其中 $\rho_{A_1\cdots A_M}$。证明者对系统 R 应用多体纠缠破坏信道，该信道可写为

$$\mathcal{E}_{R\to A'_1\cdots A'_{M-1}}(\cdot) = \sum_x \mathrm{Tr}[\mu^x_R(\cdot)]\left(\phi^{x,1}_{A'_1}\otimes\cdots\otimes\phi^{x,M-1}_{A'_{M-1}}\right), \tag{95}$$

其中 $\{\mu^x_R\}_x$ 是一个秩一正算子值测度，且 $\{\phi^{x,i}_{A'_i}\}_{x,i}$ 是一组纯态。证明者将系统$(A^{M-1})' \equiv A'_1\cdots A'_{M-1}$ 发送给验证者。随后，验证者对这些系统与 $A_1\cdots A_M$ 进行集体交换测试，如图 11 所示。该分布式量子计算的接受概率为

$$\max_{\mathcal{E}\in\mathrm{EB}_{M-1}} \mathrm{Tr}[\Pi^{\mathrm{sym}}_{(A^{M-1})'A^{M-1}}\mathcal{E}_{R\to(A^{M-1})'}(\psi_{RA^{M-1}})], \tag{96}$$

其中，$\mathcal{E}\in\mathrm{EB}_{M-1}$ 表示式 (95)中定义的纠缠破坏信道集合。这导出以下定理:

定理 10 对于纯态 $\psi_{RA^M}\equiv\psi_{RA_1\cdots A_M}$，有以下等式成立:

$$\max_{\mathcal{E}\in\mathrm{EB}_{M-1}} \mathrm{Tr}[\Pi^{\mathrm{sym}}_{(A^{M-1})'(A^{M-1})}\mathcal{E}_{R\to A'_1\cdots A'_{M-1}}(\psi_{RA^M})] = \frac{1}{2}\left(1+\max_{\sigma_{A_1\cdots A_M}\in M\text{-SEP}} F(\rho_{A_1\cdots A_M},\sigma_{A_1\cdots A_M})\right). \tag{97}$$

证明。 电路图如图11所示。验证者制备$\psi^\rho_{RA_1\cdots A_M}$的纯化，其中$\rho_{A_1\cdots A_M}$。证明者在 R上施加一个多体纠缠破坏信道，该信道可写为

$$\mathcal{E}_{R\to A'_1\cdots A'_{M-1}}(\cdot) = \sum_x \mathrm{Tr}[\mu^x_R(\cdot)]\left(\phi^{x,1}_{A'_1}\otimes\cdots\otimes\phi^{x,M-1}_{A'_{M-1}}\right), \tag{98}$$

其中$\{\mu^x_R\}_x$ 是一个秩一正算子值测度，而$\{\phi^{x,i}_{A'_i}\}_{x,i}$ 是一组纯态。证明者将系统 $(A^{M-1})' = A'_1\cdots A'_{M-1}$ 发送给验证者。现在，验证者对 $A_1\cdots A_M$ 执行集体交换测试，如图 11 所示电路图的最后部分。因此，该交互式证明系统的接受概率为

$$\max_{\mathcal{E}\in\mathrm{EB}} \mathrm{Tr}[\Pi^{\mathrm{sym}}_{(A_1\cdots A_{M-1})'A_1\cdots A_{M-1}}\mathcal{E}_{R\to(A_1\cdots A_{M-1})'}(\psi_{RA_1\cdots A_M})], \tag{99}$$

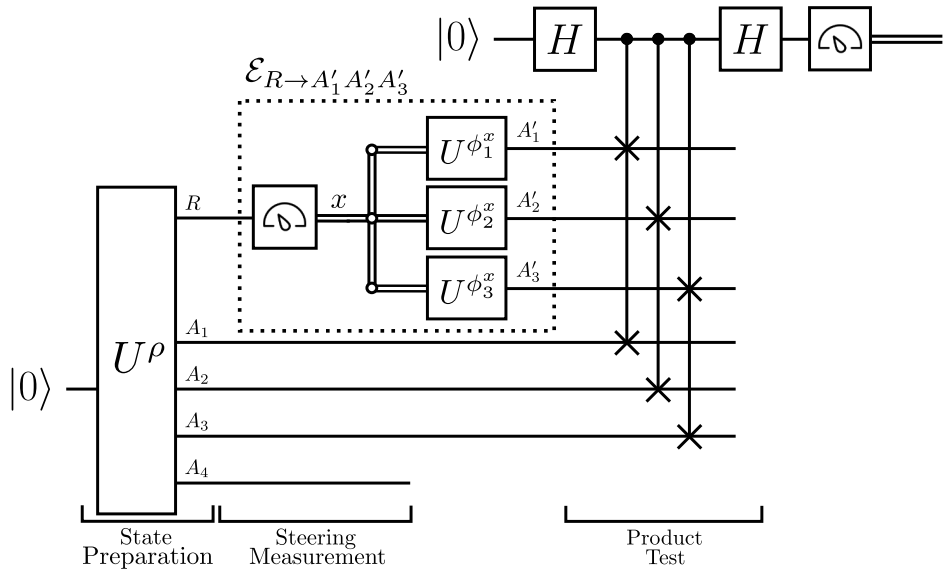


图 11：用于检验多体混合态可分性的测试。验证者使用酉电路 U^ρ 生成量子态 $\psi_{RA_1A_2A_3A_4}$，它是 $\rho_{A_1A_2A_3A_4}$的一个纯化。证明者（由虚线框标示）通过测量秩一正算子值测度 $\{\mu_R^x\}$，对 R 施加纠缠破坏信道 $\mathsf{E}^{R\to A_1'A_2'A_3'}$，然后根据结果 x，从集合 $\{\phi^x, {}_{A_1'}{}^{1}\otimes\phi^x, {}_{A_2'}{}^{2}\otimes\phi^x, {}_{A_3'}{}^{3}\}_x$中制备一个量子态。最终的量子态被发送给验证者，由验证者执行集体交换测试。定理 10 指出，此交互式证明的最大接受概率等于 $\frac{1}{2}(1+F_{\mathrm{s}}(\rho_{A_1A_2A_3A_4}))$，即多体可分性保真度的一个简单函数。

其中

$$\Pi^{\mathrm{sym}}_{(A_1\cdots A_{M-1})'A_1\cdots A_{M-1}} := \frac{1}{2}\left(I_{(A_1\cdots A_{M-1})'A_1\cdots A_{M-1}} + F_{(A_1\cdots A_{M-1})'A_1\cdots A_{M-1}}\right) \tag{100}$$

是作用于 A'、A 和 $F_{(A_1\cdots A_{M-1})'A_1\cdots A_{M-1}}$ 的对称子空间上的投影算子，是各个交换算子 $F_{A_i'A_i}$ 的张量积，其中 $i\in\{1,\ldots,M-1\}$。也就是说，

$$F_{(A_1\cdots A_{M-1})'A_1\cdots A_{M-1}} = \bigotimes_{i=1}^{M-1} F_{A_i'A_i}. \tag{101}$$

于是，对于固定的 $\mathcal{E}_{R\to A_1'\cdots A_{M-1}'}$，我们得到

$$\begin{aligned}
&\mathrm{Tr}[\Pi^{\mathrm{sym}}_{(A_1\cdots A_{M-1})'(A_1\cdots A_{M-1})}\mathcal{E}_{R\to A_1'\cdots A_{M-1}'}(\psi_{RA_1\cdots A_M})] \\
&= \frac{1}{2}\,\mathrm{Tr}[(I_{(A_1\cdots A_{M-1})'(A_1\cdots A_{M-1})} + F_{(A_1\cdots A_{M-1})'(A_1\cdots A_{M-1})})\mathcal{E}_{R\to A_1'\cdots A_{M-1}'}(\psi_{RA_1\cdots A_M})] && (102)\\
&= \frac{1}{2} + \frac{1}{2}\,\text{迹}[F_{(A_1\cdots A_{M-1})'(A_1\cdots A_{M-1})}\mathcal{E}_{R\to A_1'\cdots A'}(\psi_{RA^M})] && (103)\\
&= \frac{1}{2} + \frac{1}{2}\,\text{迹}\left[F_{(A_1\cdots A_{M-1})'(A_1\cdots A_{M-1})}\sum_x \text{迹}[\mu_R^x(\psi_{RA^M})]\phi^{x,1}_{A_1'}\otimes\cdots\otimes\phi^{x,M-1}_{A_{M-1}'}\right], && (104)\\
&= \frac{1}{2} + \frac{1}{2}\,\text{迹}\left[F_{(A_1\cdots A_{M-1})'(A_1\cdots A_{M-1})}\sum_x p(x)(\psi^x_{A_1\cdots A_M})\phi^{x,1}_{A_1'}\otimes\cdots\otimes\phi^{x,M-1}_{A_{M-1}'}\right], && (105)\\
&= \frac{1}{2} + \frac{1}{2}\sum_x p(x)\,\mathrm{Tr}\left[\left(\phi^{x,1}_{A_1}\otimes\cdots\otimes\phi^{x,M-1}_{A_{M-1}}\right)\psi^x_{A_1\cdots A_{M-1}}\right], && (106)
\end{aligned}$$

其中

$$p(x) \coloneqq \mathrm{Tr}[\mu_R^x\psi_{RA^M}], \tag{107}$$

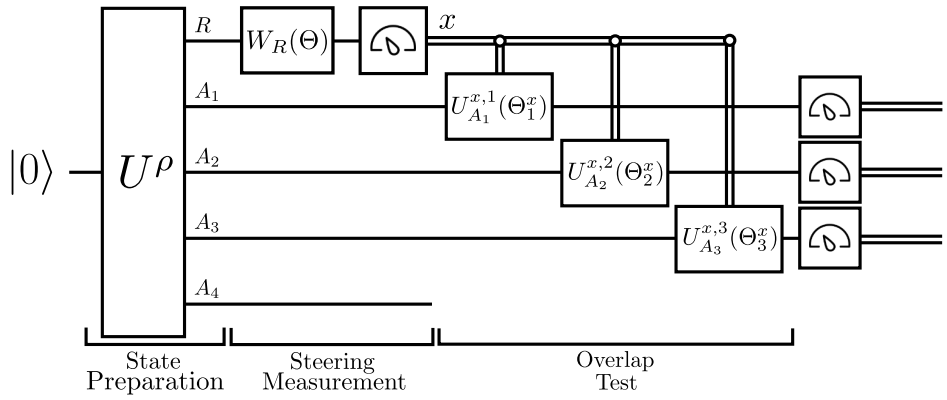


图12：用于估计多体可分性保真度 $F_s(\rho_{A_1A_2A_3A_4})$ 的 VQSA。酉电路 U^ρ 制备量子态 $\psi_{RA_1A_2A_3A_4}$，它是 $\rho_{A_1A_2A_3A_4}$ 的纯化。参数化电路 $W_R(\Theta)$ 作用于 R，使量子态演化为 $\rho_{A_1A_2A_3A_4}$ 的另一种纯化。随后进行标记为“导引测量”的测量，将其余系统导引至量子态 $\psi^x_{A_1A_2A_3A_4}$，前提是测量结果为 x。在测量结果为 x 的条件下，应用最终的参数化电路 $U^{x,1}_{A_1}(\Theta^x_1)$、$U^{x,2}_{A_2}(\Theta^x_2)$ 和 $U^{x,3}_{A_3}(\Theta^x_3)$，随后进行测量以估计量 $\mathrm{Tr}\left[\left(\phi^{x,1}_{A_1}\otimes\phi^{x,2}_{A_2}\otimes\phi^{x,3}_{A_3}\right)\psi^x_{A_1A_2A_3}\right]$。

$$\psi^x_{A_1\cdots A_M} \coloneqq \frac{1}{p(x)}\,\mathrm{Tr}_R[\mu^x_R\psi_{RA^M}]. \tag{108}$$

对于给定的 x，我们将 $F_s(\varphi_{A_1\cdots A_M})$ 按(94)中的定义进行简化，

$$\begin{aligned}
F_s(\varphi_{A_1\cdots A_M}) &= \max_{\{|\phi^i\rangle_{A_i}\}_{i=1}^M} \left|\langle\varphi|_{A_1\cdots A_M}|\phi^1\rangle_{A_1}\otimes\cdots\otimes|\phi^M\rangle_{A_M}\right|^2 && (109)\\
&= \max_{\{|\phi^i\rangle_{A_i}\}_{i=1}^M} \left|\langle\phi^1|_{A_1}\otimes\cdots\otimes\langle\phi^M|_{A_M}|\varphi\rangle_{A_1\cdots A_M}\right|^2 && (110)\\
&= \max_{\{|\phi^i\rangle_{A_i}\}_{i=1}^{M-1}} \left\|\langle\phi^1|_{A_1}\otimes\cdots\otimes\langle\phi^{M-1}|_{A_{M-1}}\otimes I_{A_M}|\varphi\rangle_{A^M}\right\|_2^2 && (111)\\
&= \max_{\{|\phi^i\rangle_{A_i}\}_{i=1}^{M-1}} \mathrm{Tr}[(|\phi^1\rangle\langle\phi^1|_{A_1}\otimes\cdots\otimes|\phi^{M-1}\rangle\langle\phi^{M-1}|_{A_{M-1}}\otimes I_{A_M})\varphi_{A_1\cdots A_M}] && (112)\\
&= \max_{\{|\phi^i\rangle_{A_i}\}_{i=1}^{M-1}} \mathrm{Tr}[(|\phi^1\rangle\langle\phi^1|_{A_1}\otimes\cdots\otimes|\phi^{M-1}\rangle\langle\phi^{M-1}|_{A_{M-1}})\varphi_{A_1\cdots A_{M-1}}]. && (113)
\end{aligned}$$

前两个等式来自定义和一次改写。第三个等式由向量欧几里得范数的变分刻画得出。注意到 (113) 中的形式，并将(95)中所述形式的纠缠破坏信道上的最大化应用于(106)，即可得到(97)中的所需结论。

■

接下来，我们可以利用混合态广义可分性检验，为多体情形构建一个 VQSA。见图12。具体而言，将图11中的集体交换测试替换为重叠测量，类似于我们如何根据正文中的图1 得到正文中的图2 。

J 复杂度类 $\mathrm{QIP}_{\mathrm{EB}}(2)$

在本附录中，我们为 $\mathrm{QIP}_{\mathrm{EB}}(2)$建立一个完全问题，并在备注 13中对该问题进行解读。参见 [41, 42] ，了解量子计算复杂性理论的更多背景知识。

首先定义复杂度类 $\mathrm{QIP}_{\mathrm{EB}}(2)$。设 $A=(A_{\mathrm{yes}},A_{\mathrm{no}})$ 是一个承诺问题，且 $a,b\colon \mathbb{N}\to[0,1]$ 和 p 是多项式函数。验证者 V 由一族通过多项式时间生成的量子电路描述。证明者 P 是一族任意的纠缠破坏信道，能够与给定的验证者自然交互。若存在一个具有以下性质的双消息验证者，则 $A\in \mathrm{QIP}_{\mathrm{EB}}(2)(a,b)$：

1. 完备性：对于所有 $x\in A_{\mathrm{yes}}$，存在一个证明者 P，使验证者 V 以至少 $a(|x|)$ 的概率接受 x。

2. 可靠性：对于所有 $x\in A_{\mathrm{no}}$，任意证明者 P 都会使验证者 V 以至多 $b(|x|)$ 的概率接受 x。

上述定义中，接受是指测量判定量子比特寄存器后得到结果 1。

问题 11 给定用于生成信道 $N_{G\to S}$ 和量子态 ρ_S的电路。固定 α 和 β，使得$0\le\alpha<\beta\le 1$。判断以下哪项成立：

$$\textit{Yes:}\quad f(\mathcal{N}_{G\to S},\rho_S)\ge\beta, \tag{114}$$

$$\textit{No:}\quad f(\mathcal{N}_{G\to S},\rho_S)\le\alpha, \tag{115}$$

其中

$$f(\mathcal{N}_{G\to S},\rho_S):=\max_{\{(p(x),\psi^x)\}_x,\{\varphi^x\}_x}\left\{\sum_x p(x)F(\psi_S^x,\mathcal{N}_{G\to S}(\varphi_G^x)):\sum_x p(x)\psi_S^x=\rho_S\right\} \tag{116}$$

其中，优化遍历 ρ_S 的所有纯态分解 $\sum_x p(x)\psi_S^x=\rho_S$。此外，$\{\varphi^x\}_x$ 是一个纯态集合。

定理 12 问题 *11* 是 $\mathrm{QIP}_{\mathrm{EB}}(2)$ 的完全问题。

证明。 证明的核心思路是表明，一般 $\mathrm{QIP}_{\mathrm{EB}}(2)$ 问题的接受概率可以精确地写成 $f(\mathcal{N}_{G\to S},\rho_S)$。这意味着，任意 $\mathrm{QIP}_{\mathrm{EB}}(2)$ 问题都可以归约为问题 11的一个实例；我们将在最后论证，这也意味着问题11 可以归约为 $\mathrm{QIP}_{\mathrm{EB}}(2)$ 中某个问题的实例。

考虑一个一般的 $\mathrm{QIP}_{\mathrm{EB}}(2)$ 交互式证明系统：验证者首先制备一个双部纯态 ψ_{RS}，然后将系统 R 发送给证明者，证明者随后执行一个纠缠破坏信道。接着，验证者执行酉算子 $V_{R'S\to DG}$，并将判定量子比特投影到 $|1\rangle\langle 1|$ 态上。事实上，接受概率为

$$\max_{\mathcal{E}\in\mathrm{EB}}\mathrm{Tr}[(|1\rangle\langle 1|_D\otimes I_G)\mathcal{V}_{R'S\to DG}(\mathcal{E}_{R\to R'}(\psi_{RS}))], \tag{117}$$

其中 $\mathcal{V}_{R'S\to DG}$ 是与酉算符 $V_{R'S\to DG}$对应的酉信道。通过类似于 (25)、(32)和 (33)中的推理，我们得到

$$\mathcal{E}_{R\to R'}(\psi_{RS})=\sum_x p(x)\phi_{R'}^x\otimes\psi_S^x, \tag{118}$$

使得接受概率等于

$$\max_{\substack{\{(p(x),\psi^x)\}_x,\\ \{\phi^x\}_x,\\ \sum_x p(x)\psi_S^x=\psi_S}}\mathrm{Tr}\left[(|1\rangle\langle 1|_D\otimes I_G)\mathcal{V}\left(\sum_x p(x)\phi_{R'}^x\otimes\psi_S^x\right)\right]$$

$$= \max_{\substack{\{(p(x),\psi^x)\}_x,\\ \{\phi^x\}_x,\\ \sum_x p(x)\psi_S^x=\psi_S}} \sum_x p(x)\operatorname{Tr}[(|1\rangle\langle 1|_D \otimes I_G)\mathcal{V}\left(\phi_{R'}^x \otimes \psi_S^x\right)], \quad (119)$$

其中我们使用了简写 $\mathcal{V} \equiv \mathcal{V}_{R'S\to DG}$。注意，对于所有 x，

$$\operatorname{Tr}[(|1\rangle\langle 1|_D \otimes I_G)\mathcal{V}\left(\phi_{R'}^x \otimes \psi_S^x\right)] = \|\langle 1|_D \otimes I_G)V|\phi^x\rangle_{R'} \otimes |\psi^x\rangle_S\|_2^2 \quad (120)$$

$$= \max_{|\varphi^x\rangle_G} |\langle 1|_D \otimes \langle\varphi^x|_G)V|\phi^x\rangle_{R'} \otimes |\psi^x\rangle_S|^2 \quad (121)$$

$$= \max_{|\varphi^x\rangle_G} \operatorname{Tr}\left[V^\dagger(|1\rangle\langle 1|_D \otimes |\varphi^x\rangle\langle\varphi^x|_G)V\phi_{R'}^x \otimes |\psi^x\rangle\langle\psi^x|_S\right] \quad (122)$$

$$= \max_{|\varphi^x\rangle_G} \operatorname{Tr}[\mathcal{W}_{G\to R'S}(|\varphi^x\rangle\langle\varphi^x|_G)\phi_{R'}^x \otimes |\psi^x\rangle\langle\psi^x|_S], \quad (123)$$

其中，等距信道 $\mathcal{W}_{G\to R'S}$ 定义为

$$\mathcal{W}_{G\to R'S}(\cdot) \coloneqq (V_{R'S\to DG})^\dagger(|1\rangle\langle 1|_D \otimes (\cdot)_G)V_{R'S\to DG}, \quad (124)$$

相应的等距变换 $W_{G\to R'S}$ 为 $W_{G\to R'S} \coloneqq (V_{R'S\to DG})^\dagger|1\rangle_D$。因此，接受概率为

$$\max_{\substack{\{(p(x),\psi^x)\}_x,\\ \{\phi^x\}_x,\{\varphi^x\}_x}} \left\{ \begin{array}{c} \sum_x p(x)\operatorname{Tr}[\mathcal{W}_{G\to R'S}(|\varphi^x\rangle\langle\varphi^x|_G)\phi_{R'}^x \otimes |\psi^x\rangle\langle\psi^x|_S] : \\ \sum_x p(x)\psi_S^x = \psi_S \end{array} \right\}. \quad (125)$$

由于对 $\phi_{R'}^x$ 的优化是任意的，我们也可以写成

$$\max_{|\phi^x\rangle_{R'}} \operatorname{Tr}[\mathcal{W}_{G\to R'S}(|\varphi^x\rangle\langle\varphi^x|_G)\phi_{R'}^x \otimes |\psi^x\rangle\langle\psi^x|_S]$$

$$= \max_{|\phi^x\rangle_{R'}} |\langle\phi^x|_{R'} \otimes \langle\psi^x|_S W_{G\to R'S}|\varphi^x\rangle_G|^2 \quad (126)$$

$$= \|I_{R'} \otimes \langle\psi^x|_S W_{G\to R'S}|\varphi^x\rangle_G\|_2^2 \quad (127)$$

$$= \left(\langle\varphi^x|_G \left(W_{G\to R'S}\right)^\dagger I_{R'} \otimes |\psi^x\rangle_S\right)\left(I_{R'} \otimes \langle\psi^x|_S W_{G\to R'S}|\varphi^x\rangle_G\right) \quad (128)$$

$$= \langle\varphi^x|_G \left(W_{G\to R'S}\right)^\dagger \left(I_{R'} \otimes |\psi^x\rangle\langle\psi^x|_S\right) W_{G\to R'S}|\varphi^x\rangle_G \quad (129)$$

$$= \operatorname{Tr}\left[\left(I_{R'} \otimes |\psi^x\rangle\langle\psi^x|_S\right) W_{G\to R'S}|\varphi^x\rangle\langle\varphi^x|_G \left(W_{G\to R'S}\right)^\dagger\right] \quad (130)$$

$$= \text{迹}[|\psi^x\rangle\langle\psi^x|_S \boldsymbol{N}_{G\to S}(|\varphi^x\rangle\langle\varphi^x|_G)], \quad (131)$$

其中，我们将信道 $\mathcal{N}_{G\to S}$ 定义为

$$\mathcal{N}_{G\to S}(\cdot) \coloneqq \operatorname{Tr}_{R'}[(V_{R'S\to DG})^\dagger(|1\rangle\langle 1|_D \otimes (\cdot)_G)V_{R'S\to DG}]. \quad (132)$$

因此，我们发现接受概率为

$$\max_{\substack{\{(p(x),\psi^x)\}_x,\\ \{\varphi^x\}_x,\\ \sum_x p(x)\psi_S^x=\psi_S}} \sum_x p(x)\operatorname{Tr}[|\psi^x\rangle\langle\psi^x|_S \mathcal{N}_{G\to S}(|\varphi^x\rangle\langle\varphi^x|_G)] = \max_{\substack{\{(p(x),\psi^x)\}_x,\{\varphi^x\}_x\\ \sum_x p(x)\psi_S^x=\psi_S}} \sum_x p(x)F(\psi_S^x, \mathcal{N}_{G\to S}(\varphi_G^x)). \quad (133)$$

第一部分的证明到此结束。

要了解这如何意味着问题 11 可以在 QIP 中实现$_{\text{EB}}(2)$，注意，制备量子态 ρ_S 的电路会制备一个纯化，并对参考系统进行偏迹，而该电路

要生成 $\mathcal{N}_{G\to S}$，可以通过在量子态为 $|0\rangle\langle 0|$的环境系统上附加一个系统，执行一个酉算子，然后对环境系统进行偏迹来实现。因此，我们让验证者制备 ρ_S 的纯化，并让它扮演上文中 ψ_{RS} 的角色；信道 $\mathcal{N}_{G\to S}$ 则可通过适当替换，完全按照 (132) 来实现。

注释 *13* 式 *(116)* 中的量可以这样理解：给定一个信道 N 和一个源量子态 ρ，计算在该信道输出端重现该源时所能达到的最大平均系综保真度。这意味着需要找到 ρ 的系综分解 $\{(p(x),\psi^x)\}_x$，以及一组能够使系综保真度达到最大的编码态 $\{\varphi^x\}_x$（这部分工作留给证明者完成）。这一准则与 *Schumacher* 数据压缩 *[91],* 中使用的准则相似，但它似乎更接近信源-信道分离定理 *[92],*中的设定；该定理的目标是通过量子信道传输一个信息源。这里的信道 N 可以由固定编码 E、噪声信道 M 和固定解码 D 构成（即 $N = D \circ M \circ E$），此时目标是根据系综保真度准则，检验给定的固定方案 (E, D) 通过信道 M 传输信息源 ρ 的效果。

备注14 我们还可以将 (116) 中的表达式写作

$$\text{Eq. (116)} = \max_{\substack{\{(p(x),\psi^x)\}_x,\\ \sum_x p(x)\psi_S^x=\rho_S}} \sum_x p(x) \left\|(\mathcal{N}_{G\to S})^\dagger(\psi_S^x)\right\|_\infty , \tag{134}$$

其中 $(N_{G\to S})^\dagger$ 是信道 $(N_{G\to S})^\dagger$的希尔伯特–施密特伴随。使用简写$\psi_S^x \equiv |\psi^x\rangle\langle\psi^x|_S$ 和 $\varphi_G^x \equiv |\varphi^x\rangle\langle\varphi^x|_G$，可得

$$\begin{aligned}
&\max_{\substack{\{(p(x),\psi^x)\}_x,\\ \{\varphi^x\}_x,\\ \sum_x p(x)\psi_S^x=\psi_S}} \sum_x p(x)\,\mathrm{Tr}[\psi_S^x \mathcal{N}_{G\to S}(\varphi_G^x)] \\
&= \max_{\substack{\{(p(x),\psi^x)\}_x,\\ \{\varphi^x\}_x,\\ \sum_x p(x)\psi_S^x=\psi_S}} \sum_x p(x)\,\mathrm{Tr}[(\mathcal{N}_{G\to S})^\dagger(\psi_S^x)\varphi_G^x] &(135)\\
&= \max_{\substack{\{(p(x),\psi^x)\}_x,\\ \{\varphi^x\}_x,\\ \sum_x p(x)\psi_S^x=\psi_S}} \sum_x p(x) \max_{\{\varphi^x\}_x} \mathrm{Tr}[(\mathcal{N}_{G\to S})^\dagger(\psi_S^x)\varphi_G^x] &(136)\\
&= \max_{\substack{\{(p(x),\psi^x)\}_x,\\ \sum_x p(x)\psi_S^x=\rho_S}} \sum_x p(x) \left\|(\mathcal{N}_{G\to S})^\dagger(\psi_S^x)\right\|_\infty . &(137)
\end{aligned}$$

如果我们定义函数

$$g_{\mathcal{N}}(\rho) := \left\|(\mathcal{N}_{G\to S})^\dagger(\rho_S)\right\|_\infty , \tag{138}$$

那么，(134) 中的函数称为 $g_{\mathcal{N}}(\rho)$ 的凹闭包，并已在量子信息论的其他背景下得到研究 *[93,* 第 *2]*节。它还有一个有趣的对偶表述，如 *[93,* 式（*15*）*]*所示。根据(134)中的观察，我们可以得出结论：给定用于实现信道$\mathcal{N}$和量子态 ρ的电路，在加性误差范围内估计函数 $g_{\mathcal{N}}(\rho)$的凹闭包是$\mathrm{QIP}_{\mathrm{EB}}(2)$的完全问题。

注释 15 运用注释 *14*中的推理，我们发现，式 (35) 中的接受概率等于以下函数的凹闭包：

$$f(\rho_{AB}) := \|\Pi_{AA'}^{\mathrm{sym}}(\rho_{AB}\otimes I_{A'})\Pi_{AA'}^{\mathrm{sym}}\|_\infty , \tag{139}$$

其中我们用到了这样一个事实：注释 ρ_S **14** 中的量子态是 ρ_{AB}，而映射 $\mathcal{N}_{G\to S}$ 来自注释 *14*是

$$\mathcal{N}(\sigma_{AA'B}) = \mathrm{Tr}_{A'}[\Pi^{\mathrm{sym}}_{AA'}\sigma_{AA'B}\Pi^{\mathrm{sym}}_{AA'}], \tag{140}$$

及其伴随算子

$$\mathcal{N}^{\dagger}(\omega_{AB}) = \Pi^{\mathrm{sym}}_{AA'}(\omega_{AB}\otimes I_{A'})\Pi^{\mathrm{sym}}_{AA'}. \tag{141}$$

注意，映射 $\rho_{AB}\mapsto\Pi^{\mathrm{sym}}_{AA'}(\rho_{AB}\otimes I_{A'})\Pi^{\mathrm{sym}}_{AA'}$ 与 $1\to 2$ 通用克隆机 *[94,* 式（*17*）*]*中使用的映射成正比。若 ρ_{AB} 是纯态，即可将其写作 ψ_{AB}，则有以下不等式：

$$\|\Pi^{\mathrm{sym}}_{AA'}(\psi_{AB}\otimes I_{A'})\Pi^{\mathrm{sym}}_{AA'}\|_\infty \le \|\Pi^{\mathrm{sym}}_{AA'}\|_\infty \|\psi_{AB}\otimes I_{A'}\|_\infty \|\Pi^{\mathrm{sym}}_{AA'}\|_\infty \le 1, \tag{142}$$

这里我们应用了谱范数的可乘性。因此，$f(\rho_{AB})$的凹闭包满足 $f(\rho_{AB})\in[0,1]$。此外，根据下文引理 *16*，我们知道

$$\|\Pi^{\mathrm{sym}}_{AA'}(\psi_{AB}\otimes I_{A'})\Pi^{\mathrm{sym}}_{AA'}\|_\infty = \frac{1}{2}\left(1+\|\psi_A\|_\infty\right), \tag{143}$$

这表明上述主张 (139) 与正文中的定理 *1* 以及公式 (19) 和 (20) 相一致。若 ρ_{AB} 是纯乘积态，即可将其写作 $\rho_{AB}=\phi_A\otimes\varphi_B$，则有

$$\|\Pi^{\mathrm{sym}}_{AA'}(\phi_A\otimes\varphi_B\otimes I_{A'})\Pi^{\mathrm{sym}}_{AA'}\|_\infty = \|\Pi^{\mathrm{sym}}_{AA'}(\phi_A\otimes I_{A'})\Pi^{\mathrm{sym}}_{AA'}\|_\infty, \tag{144}$$

并且，选择向量 $|\phi\rangle_A\otimes|\phi\rangle_{A'}$即可达到 (144) 右侧的谱范数，因此

$$\begin{aligned}&(\langle\phi|_A\otimes\langle\phi|_{A'})\Pi^{\mathrm{sym}}_{AA'}(\phi_A\otimes I_{A'})\Pi^{\mathrm{sym}}_{AA'}(|\phi\rangle_A\otimes|\phi\rangle_{A'})\\ &=(\langle\phi|_A\otimes\langle\phi|_{A'})(\phi_A\otimes I_{A'})(|\phi\rangle_A\otimes|\phi\rangle_{A'}) &(145)\\ &=1. &(146)\end{aligned}$$

引理16 对于纯态 ψ_{AB}，有以下等式成立：

$$\|\Pi^{\mathrm{sym}}_{AA'}(\psi_{AB}\otimes I_{A'})\Pi^{\mathrm{sym}}_{AA'}\|_\infty = \frac{1}{2}\left(1+\|\psi_A\|_\infty\right), \tag{147}$$

其中 $\psi_A\equiv\mathrm{Tr}_B[\psi_{AB}]$。

证明。考虑

$$\begin{aligned}&\left\|\left(\Pi^{\mathrm{sym}}_{AA'}\otimes I_B\right)\left(|\psi\rangle\langle\psi|_{AB}\otimes I_{A'}\right)\left(\Pi^{\mathrm{sym}}_{AA'}\otimes I_B\right)\right\|_\infty\\ &\qquad=\left\|\left(|\psi\rangle\langle\psi|_{AB}\otimes I_{A'}\right)\left(\Pi^{\mathrm{sym}}_{AA'}\otimes I_B\right)\left(|\psi\rangle\langle\psi|_{AB}\otimes I_{A'}\right)\right\|_\infty. &(148)\end{aligned}$$

现在考虑

$$\begin{aligned}&\left(|\psi\rangle\langle\psi|_{AB}\otimes I_{A'}\right)\left(\Pi^{\mathrm{sym}}_{AA'}\otimes I_B\right)\left(|\psi\rangle\langle\psi|_{AB}\otimes I_{A'}\right)\\ &=\left(|\psi\rangle\langle\psi|_{AB}\otimes I_{A'}\right)\left(\frac{I_{AA'}+F_{AA'}}{2}\otimes I_B\right)\left(|\psi\rangle\langle\psi|_{AB}\otimes I_{A'}\right) &(149)\\ &=\frac{1}{2}\left(|\psi\rangle\langle\psi|_{AB}\otimes I_{A'}\right)+\frac{1}{2}\left(|\psi\rangle\langle\psi|_{AB}\otimes I_{A'}\right)\left(F_{AA'}\otimes I_B\right)\left(|\psi\rangle\langle\psi|_{AB}\otimes I_{A'}\right). &(150)\end{aligned}$$

接着，将 $|\psi\rangle_{AB}$ 的施密特分解写作 $|\psi\rangle_{AB}=\sum_i\sqrt{\lambda_i}|i\rangle_A|i\rangle_B$，我们得到

$$\left(|\psi\rangle\langle\psi|_{AB}\otimes I_{A'}\right)\left(F_{AA'}\otimes I_B\right)\left(|\psi\rangle\langle\psi|_{AB}\otimes I_{A'}\right)$$

$$= \sum_{i,i',j,j'} \sqrt{\lambda_i \lambda_{i'}} \left(|\psi\rangle\langle i|_A \langle i|_B \otimes |j\rangle\langle j|_{A'}\right) \left(F_{AA'} \otimes I_B\right) \left(|i'\rangle_A |i'\rangle_B \langle\psi|_{AB} \otimes |j'\rangle\langle j'|_{A'}\right) \tag{151}$$

$$= \sum_{i,i',j,j'} \sqrt{\lambda_i \lambda_{i'}} \left(|\psi\rangle\langle i|_A \langle i|_B \otimes |j\rangle\langle j|_{A'}\right) \left(|j'\rangle_A |i'\rangle_B \langle\psi|_{AB} \otimes |i'\rangle\langle j'|_{A'}\right) \tag{152}$$

$$= \sum_{i,i',j,j'} \sqrt{\lambda_i \lambda_{i'}} |\psi\rangle\langle i|j'\rangle_A \langle i|i'\rangle_B \langle\psi|_{AB} \otimes |j\rangle\langle j|i'\rangle\langle j'|_{A'} \tag{153}$$

$$= \sum_i \lambda_i |\psi\rangle\langle\psi|_{AB} \otimes |i\rangle\langle i|_{A'} \tag{154}$$

$$= |\psi\rangle\langle\psi|_{AB} \otimes \sum_i \lambda_i |i\rangle\langle i|_{A'} \tag{155}$$

$$= |\psi\rangle\langle\psi|_{AB} \otimes \psi_{A'}. \tag{156}$$

Then

$$\begin{aligned} &\left(|\psi\rangle\langle\psi|_{AB} \otimes I_{A'}\right) \left(\Pi^{\mathrm{sym}}_{AA'} \otimes I_B\right) \left(|\psi\rangle\langle\psi|_{AB} \otimes I_{A'}\right) \\ &= \frac{1}{2} \left(|\psi\rangle\langle\psi|_{AB} \otimes I_{A'}\right) + |\psi\rangle\langle\psi|_{AB} \otimes \frac{1}{2} \psi_{A'} \qquad (157) \\ &= |\psi\rangle\langle\psi|_{AB} \otimes \frac{1}{2} \left(I_{A'} + \psi_{A'}\right), \qquad (158) \end{aligned}$$

由此我们得出

$$\begin{aligned} &\left\| \left(\Pi^{\mathrm{sym}}_{AA'} \otimes I_B\right) \left(|\psi\rangle\langle\psi|_{AB} \otimes I_{A'}\right) \left(\Pi^{\mathrm{sym}}_{AA'} \otimes I_B\right) \right\|_\infty \\ &= \left\| |\psi\rangle\langle\psi|_{AB} \otimes \frac{1}{2} \left(I_{A'} + \psi_{A'}\right) \right\|_\infty \qquad (159) \\ &= \frac{1}{2} \left(1 + \|\psi_{A'}\|_\infty\right) \qquad (160) \\ &= \frac{1}{2} \left(1 + \|\psi_A\|_\infty\right). \qquad (161) \end{aligned}$$

证明至此完成。 ■

K $\mathrm{QIP}_{\mathrm{EB}}(2)$ 的位置

在本附录中，我们证明以下包含关系：

$$\mathrm{QAM}, \mathrm{QSZK} \subseteq \mathrm{QIP}_{\mathrm{EB}}(2). \tag{162}$$

详见图 7，其中展示了详细示意图。

K.1 $\mathrm{QAM} \subseteq \mathrm{QIP}_{\mathrm{EB}}(2)$

首先，回顾一下，QAM 包含如下过程：验证者均匀随机地选择一个经典字母 x，并将该选择发送给证明者；随后，证明者将一个纯态 ψ_x 发回给验证者，验证者最终执行高效测量，以决定是否接受该计算 [55]。注意，QAM 包含 QMA [55]。

要看出 $\mathrm{QAM} \subseteq \mathrm{QIP}_{\mathrm{EB}}(2)$ 的包含关系，可以考虑 $\mathrm{QIP}_{\mathrm{EB}}(2)$ 中验证者的第一个电路：它可以在系统 R中制备一个随机的经典比特串。验证者将系统 R发送给证明者。随后，证明者的操作相当于制备某个态并将其送回验证者。之后的协议部分便模拟了一个 QAM 协议。

K.2 QSZK $\subseteq$QIP$_{\mathrm{EB}}$(2)

量子统计零知识（QSZK）包含所有能够通过量子验证者与量子证明者之间的交互来解决的问题：验证者会积累有关判定答案的统计证据，但与证明者交互不会让验证者学到答案以外的任何信息 [95, 56]。该复杂度类的一个完全问题是量子态可区分性，其目标是判定由量子电路生成的两个态 ρ_0 和 ρ_1在迹距离上相距甚远还是非常接近 [95]。这是一个有助于理解 QSZK 复杂度类基础知识的有趣问题：交互从验证者以均匀随机的方式选取其中一个态开始，并将选择记录为比特 x，然后通过量子信道将选中的态 ρ_x 发送给证明者。随后，证明者可以执行最优的海尔斯特伦测量 [96, 97] 来区分这些态，其成功概率等于

$$p_{\mathrm{succ}} \coloneqq \frac{1}{2}\left(1+\frac{1}{2}\left\|\rho_0-\rho_1\right\|_1\right). \tag{163}$$

海尔斯特伦测量会产生一个判定比特 y，证明者通过量子信道将其发送回验证者（此处，单个经典比特信道就足够了）。随后，如果 $x=y$，验证者便接受，而这一情况发生的概率等于 p_{succ}。通过重复该协议多项式次，并调用 [95], 中的错误缩减协议，可以使验证者将完备性和可靠性概率分别调至任意接近一和零，从而在最终判定这些态在迹距离上是近还是远时，基本消除错误概率。最后，这种交互具有“零知识”性质，因为验证者只会获知证明者给出的比特，而不会了解如何区分这些态。

由于量子态可区分性是 QSZK 的完全问题，且上述交互可以在 QIP$_{\mathrm{EB}}$(2) 中完成，因此可得包含关系 QSZK $\subseteq$ QIP$_{\mathrm{EB}}$(2)。

L 局部奖励函数

在本附录中，我们将构造一种局部奖励函数，作为正文中所讨论的全局奖励函数的替代方案，即定理 2 中的接受概率。定理 2 中的接受概率可视为全局奖励函数，因为它对应于在每个寄存器中测得 0 的概率。如 [44], 所示，采用局部奖励函数有助于缓解贫瘠高原问题 [43], ，而该问题困扰着所有变分量子算法。

下面定义局部和全局奖励函数。令 Z_i 表示在第i个寄存器中测得 0 的事件。接着，我们将局部奖励函数定义为在均匀随机选取的一个寄存器中测得 0 的概率；也就是说，它由下式给出：

$$L \equiv \frac{1}{n}\sum_i \Pr(Z_i). \tag{164}$$

测得全零的事件表示为 $\bigcap_i Z_i$，该事件发生的概率为$G \equiv \Pr(\bigcap_i Z_i)$，这正是我们在正文中用作全局奖励函数的量。

我们希望确定与全局和局部奖励函数相关的不等式，以下分析采用了与 [82, 附录 C]中相同的思路。运用德摩根定律

，我们得到

$$\Pr\left(\bigcap_i Z_i\right) = \Pr\left(\left(\bigcup_i Z_i^c\right)^c\right) = 1 - \Pr\left(\bigcup_i Z_i^c\right). \tag{165}$$

然后，我们可以利用并集界得出

$$\Pr\left(\bigcap_i Z_i\right) = 1 - \Pr\left(\bigcup_i (Z_i)^c\right) \geq 1 - \sum_i \Pr((Z_i)^c). \tag{166}$$

最后，考虑

$$\begin{aligned} G &= \Pr\left(\bigcap_i Z_i\right) && (167)\\ &\geq 1 - \sum_i \Pr(Z_i^c) && (168)\\ &= \sum_i \Pr(Z_i) - (n-1) && (169)\\ &= nL - (n-1) && (170)\\ &= n(L-1) + 1. && (171) \end{aligned}$$

我们还可以用局部奖励函数表示全局奖励函数的一个上界。回顾以下不等式，它对每个事件集合 $\{A_1,\ A_2,\ \ldots\ldots,\ A_n\}$ 都成立：

$$\Pr\left(\bigcup_i A_i\right) \geq \frac{1}{n}\sum_i \Pr(A_i). \tag{172}$$

令 $A_i = Z_i^c$，得到

$$\Pr\left(\bigcup_i Z_i^c\right) \geq \frac{1}{n}\sum_i \Pr(Z_i^c). \tag{173}$$

利用德摩根定律，我们可以得到所需的上界：

$$\begin{aligned} G = \Pr\left(\bigcap_i Z_i\right) &\leq 1 - \frac{1}{n}\sum_i (1 - \Pr(Z_i)) && (174)\\ &= \frac{1}{n}\sum_i \Pr(Z_i) = L. && (175) \end{aligned}$$

总之，我们得到了以下界：

$$n(L-1) + 1 \leq G \leq L, \tag{176}$$

因此，$G = 1$ 当且仅当 $L = 1$。由于我们始终有 $G \in [0,1]$，只有当 L 足够大时，下界才是非平凡的，也就是说，当 $L \geq 1 - \frac{1}{n}$ 时。

已于 2024-05-29 接收，点击标题进行验证。根据 CC-BY 4.0 许可发布。