arXiv:2611.30876v1 [quant-ph] 23 Nov 2026

利用一个额外量子比特实现量子观测的指数级优势

Zhenyu Du，[1] Xiongfeng Ma，[1]，* Vlatko Vedral，[2] 和 Jinzhao Sun[3]，†[1]清华大学交叉信息科学研究院量子信息中心，中国北京 *100084*[2]英国牛津大学克拉伦登实验室，*Parks Road*，牛津，*OX1 3PU*[3]伦敦玛丽女王大学物理与化学科学学院，英国伦敦，*E1 4NS*

尽管量子技术有望彻底改变我们观测物理世界的方式，但如何以最小的开销实现显著优势，仍是核心目标。在此，我们展示，只需为量子机器增加一个额外量子比特，就能在探测量子多体动力学时获得指数级优势。我们提出一种算法，利用该量子比特对动力学轨迹进行相干干涉，从而同时估计数量呈指数级增长的多时间关联函数，而所需演化次数比任何无辅助量子比特方案都少得多，且差距呈指数级。值得注意的是，即使无辅助量子比特机器具有不受限的相干时间和任意自适应控制，这一优势依然成立；即便只估计单个关联函数，优势也依然存在。我们进一步证明，延长相干时间能够以指数级幅度提升观测能力，从而确立了该协议在空间和时间上的最优性。最后，我们通过数值计算展示了这一方法：与以往方法相比，只需少几个数量级的实验运行次数，就能预测多体系统中的高阶探针信号。这些结果凸显了该框架在量子学习、量子传感和量子模拟中的广泛用途。

I. 引言

科学发现依赖于我们观测物理世界并从中提取信息的能力。在量子多体系统中，这些信息编码于其广泛自由度之间复杂的相关性之中。自量子技术诞生以来，获取这些相关性一直是主要目标， [1, 2],推动了量子动力学模拟 [3–6], 、量子器件表征 [7–13], 以及材料性质探测 [14–18]等工作。为此，现代实验确立了一种变革性范式：部署受控辅助探针，使其与目标系统发生相干耦合，并且能够以高保真度对其自身进行测量。这种方法如今已广泛应用于原子 [19], 、固态 [12, 20, 21],和光子平台 [14, 22],„ 在量子计算 [23], 、学习 [24], 和量子传感 [7–11, 13, 25], , 以及量子混沌和热化的诊断 [26–28]方面均已证明极为有效。

尽管辅助探针发挥着核心作用，但其在量子观测中的基本优势仍然难以捉摸。一方面，与传统方法相比，基于探针的协议可以将实验次数指数级减少 [24, 29–31]。然而，实现这种缩减需要大量辅助量子比特——其数量通常与目标系统的规模相当——以及高度纠缠的测量，这对实验提出了严峻要求。另一方面，将一个小型、可控的探针耦合到目标系统，是量子模拟、量子传感和多体物理中一种自然且重要的实验范式 [25, 32–36]。然而，这类极简辅助系统能否真正胜过直接测量系统本身，仍是一个悬而未决的问题。事实上，直接测量系统已经能够获取其动力学信息，并解析跨越多个时空位置的复杂相关性 [34, 35, 37], , 因此要为小型探针确立严格优势极具挑战性。这引出了一个核心问题：

小型量子探针能否在观测量子多体动力学方面提供指数级优势?

在这里，我们通过证明以下事实，对这一问题给出肯定回答：为量子机器增添一个辅助量子比特，可以将观测量子多体动力学的实验成本降低一个指数级。我们通过形式化刻画未知 n量子比特的幺正演化 U这一任务，确立了这些优势；这一场景在原生物理环境 [24, 38–40] 以及量子模拟中无处不在 [32, 41, 42] （图1a）。通过比较由单量子比特探针区分的两种操作模型（图1b），我们揭示了查询复杂度上的显著差异。查询复杂度定义为量子机器与 U 之间的总交互次数，需在所有实验运行次数中累计计算（图1c）。首先，我们提出一种基于探针的量子算法，利用这一辅助系统提取跨越 2^k 多个时空位置的完整动力学关联函数族 $k+1$，其查询复杂度随 k 和演化时间线性增长。其次，我们证明，任何受限于原生仅作用于系统的协议

n-量子比特

* xma@tsinghua.edu.cn
† jinzhao.sun.phys@gmail.com

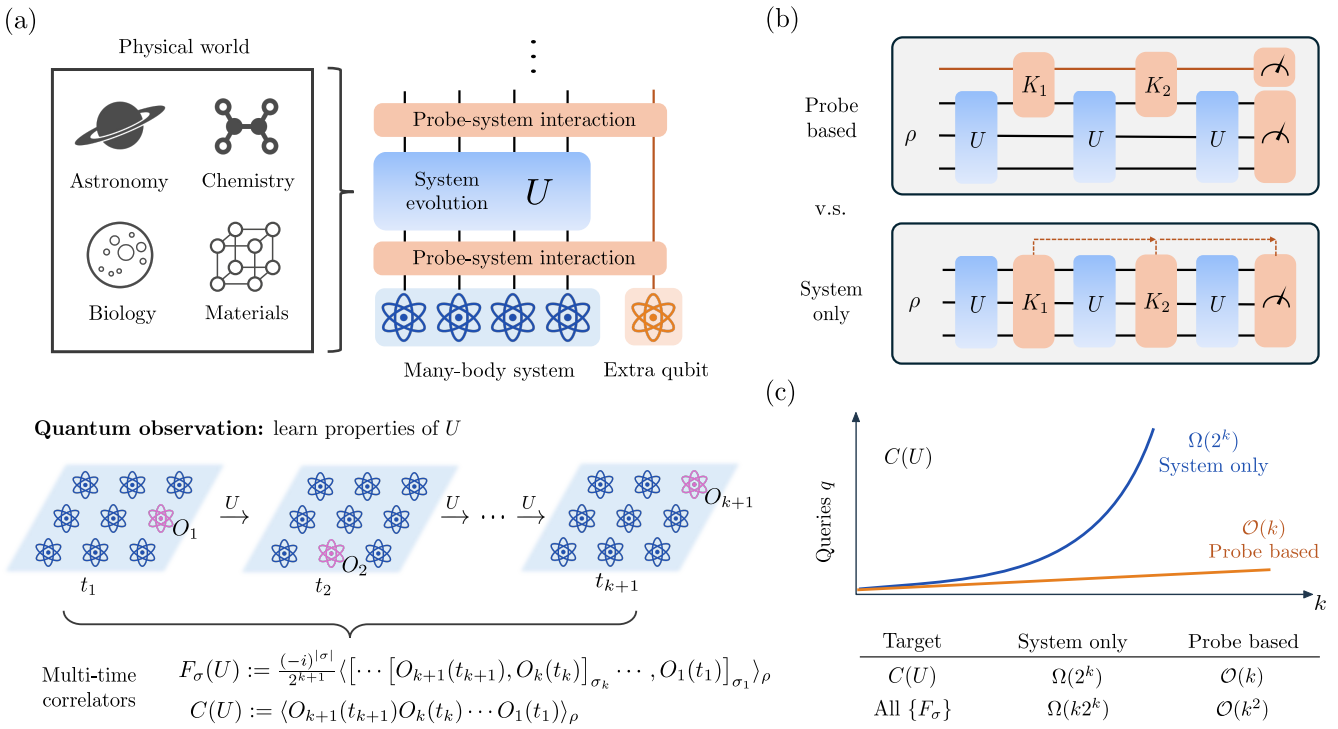

图1. 一个额外量子比特使观测量子动力学获得指数级优势。(a) 量子观测框架。物理世界中或量子模拟器内的复杂动力学由作用于多体系统的未知幺正演化 U 支配。目标是提取多个时空位置上的可观测量 O_1、.....、O_{k+1} 之间的相关性。我们考察两项任务：估计完整的一族 2^k 嵌套对易子和反对易子关联函数 $F_\sigma(U)$，以及估计单个有序多时间关联函数 $C(U)$。(b) 两种操作模型的比较。在两个电路中，未知酉算子 U 仅作用于原生的 n量子比特系统。在我们的基于探针的协议（上方）中，单个探针量子比特在各次查询之间保持相干；每次运行前选定探针-系统相互作用 K_j，并在最后分别测量探针和系统。相比之下，仅系统模型（下方）允许不受限制的相干时间和任意自适应电路中操作 K_j，虚线箭头表示经典前馈，同时将所有量子存储器和操作限制在原生系统内。(c) 查询复杂度的指数级差距。示意图展示了估计 $C(U)$时的差距，表格则总结了两项任务。对于总演化时间 $T = k \le n/5$，基于探针的协议需要 $O(k)$ 次查询来估计 $C(U)$，需要 $O(k^2)$ 次查询来估计所有 2^k 嵌套关联函数；而任何仅系统协议分别需要 $\Omega(2^k)$ 和 $\Omega(k2^k)$ 次查询。

寄存器不可避免地需要指数级数量的查询 k 才能学习这些相同的性质。证明这一下界是一项重大的技术挑战，因为即使赋予仅系统机器不受限的相干时间和任意的自适应电路中操作，该下界仍必须成立（图 1b）。与此前确立的量子存储器优势相比 [24, 25, 29, 30, 43, 44], 我们的分离结果将辅助存储器需求降至单个量子比特的最低限度，同时还能在明显更强的仅系统基线下保持成立。

我们进一步证明，单量子比特探针不仅能够同时估计指数多的性质，即使在提取单个多时间关联函数 [32, 37] 时，也能带来指数级优势。从概念上说，这些优势源于利用探针与动力学轨迹发生相干干涉，从而揭示量子干涉是观测多体动力学的一项关键资源 [6]。此外，我们的基于探针的协议在空间和时间（辅助量子比特数量与相干时间）方面均为最优：我们证明，任何无法在所需相互作用的整个过程中保持相干性的协议，即使拥有不受限制的量子存储器大小，其查询复杂度仍会呈指数级增长。因此，延长量子机器的相干时间本身就能带来指数级优势。最后，我们通过数值计算展示了该框架在多体量子传感任务中的实用价值：与仅系统基线相比，我们的方法使用的实验运行次数减少了两个数量级，便能预测高阶探针信号 [34, 35, 37]。

II. 结果

在本研究中，我们考虑表征 U 一个 n量子比特多体系统的物理演化（图1a）。在仅系统协议中，我们仅通过原生的 U 量子比特寄存器与 n进行交互。为了确立严格的优势，我们以最强的仅系统基线作为基准：实验者可不受限制地使用相干时间，并可执行任意自适应电路中操作——即后续操作取决于先前的经典结果——但所有保留的量子存储必须严格限于原生系统本身（图1b）。相比之下，我们的基于探针的协议将系统与一个辅助量子比特耦合，该比特在对 U进行多次查询期间始终保持相干；该协议只需简单的非自适应探针-系统相互作用，并分别对探针和系统进行最终测量。在这两种情形下，实验均以最终测量结束，实验者必须仅根据获得的经典数据，准确估计 U 的性质（正式的数学定义见方法）。

A. 估算多重关联函数的指数级优势

量子动力学的表征通常从标准的单时刻可观测量 [2–4], 开始；要全面了解多体动力学，则需要将这一范式扩展到多时间关联函数。通过在连续时刻 $0 \le t_1 \le \cdots \le t_{k+1} = T$（图1a）考察一系列可观测量 $O_1, \ldots, O_{k+1}$，可以揭示单时刻测量 [14, 45]无法捕捉的关键动力学指纹。这些多时间关联函数通常表现为嵌套对易子和反对易子，是非线性光谱学 [12, 15–17, 46, 47] 及非平衡物理学 [28, 48]的基础。形式上，考虑一个初始状态为 ρ的系统，其海森堡绘景中的可观测量表示为 $O_j(t_j) = (U^{t_j})^\dagger O_j U^{t_j}$。分别用 $[A,B]_0 = AB + BA$和 $[A,B]_1 = AB - BA$表示反对易子与对易子，则每个二进制字符串 $\sigma = (\sigma_1, \ldots, \sigma_k) \in \{0,1\}^k$指定一个 $(k+1)$时刻嵌套关联函数：

$$F_\sigma(U) = \frac{(-i)^{|\sigma|}}{2^{k+1}} \operatorname{Tr}\Big(\rho \left[\cdots \left[O_{k+1}(t_{k+1}), O_k(t_k)\right]_{\sigma_k} \cdots, O_1(t_1)\right]_{\sigma_1}\Big), \tag{1}$$

其中 $|\sigma| = \sum_{j=1}^k \sigma_j$ 表示对易子的数量。根据构造， $F_\sigma(U)$ 是一个满足以下条件的实数$|F_\sigma(U)| \le 1/2$。例如， $\sigma = (0, \ldots, 0)$ 和 $\sigma = (1, \ldots, 1)$ 分别将式（1）化简为纯嵌套反对易子和对易子。

我们的首要任务是通过准确估计整个 $M = 2^k$ 族嵌套关联函数（图 2a），来刻画系统的动力学。我们关注一种被广泛研究的情形：每个可观测量 O_j 都是酉算子，例如局域泡利算符。尽管人们已投入大量精力测量这些量，但现有的大多数协议都针对特定配置 σ [34, 35, 37, 46] 进行设计，因此每个目标量都需要单独的测量流程。即使采用能够同时估计多个关联函数的基于快照的协议， [49], 重构所有 $M = 2^k$关联函数也会产生指数级开销，其开销随 k而定。

在这里，我们提出一种量子算法，通过将系统与单个辅助探针量子比特耦合，并仅使用 2^k 次实验运行 $\mathcal{O}(k)$ ，同时重构所有关联函数（图2b）。我们的结果表明，这种基于探针的方法（1）优于现有的关联函数估计方案；（2）相较于所有仅系统协议，实现了指数级优势。

定理 1（估计多重关联函数时的指数级单量子比特优势，非正式表述）。考虑估计未知的 n 量子比特系统在连续时刻 $k+1$ 经历的幺正演化 U 所产生的所有2^k 嵌套关联函数 $\{F_\sigma(U)\}_{\sigma\in\{0,1\}^k}$，总演化时间不超过 T，并以高概率将每个关联函数的误差控制在加性误差 ε 以内。

1. 基于探针的 ：使用一个辅助量子比特，算法 1 仅需 $q = \mathcal{O}\big(T\varepsilon^{-2}k\big)$ 次查询 s.
2. 仅系统：对于 $T = k \le n/5$ 且误差为常数的情况 ε，任何无辅助量子比特协议都需要 $q = \Omega(k2^k)$ 次查询。

形式化陈述与证明见附录F和H，详细步骤见算法1。我们算法的核心见解是，利用探针量子比特，通过沃尔什–哈达玛谱使对不同嵌套关联函数的测量彼此兼容。具体而言，对于每个二进制字符串 $b = (b_1, \ldots, b_k) \in \{0,1\}^k$及其按位补码 $\bar{b} = 1 - b$，我们将动力学轨迹 W_b 和互补路径重叠 Q_b定义为

$$\begin{aligned} W_b &= U^{t_{k+1}-t_k} O_k^{b_k} \cdots U^{t_2-t_1} O_1^{b_1} U^{t_1}, \\ Q_b &= \operatorname{Tr}\left(O_{k+1} W_b \rho W_{\bar{b}}^\dagger\right). \end{aligned} \tag{2}$$

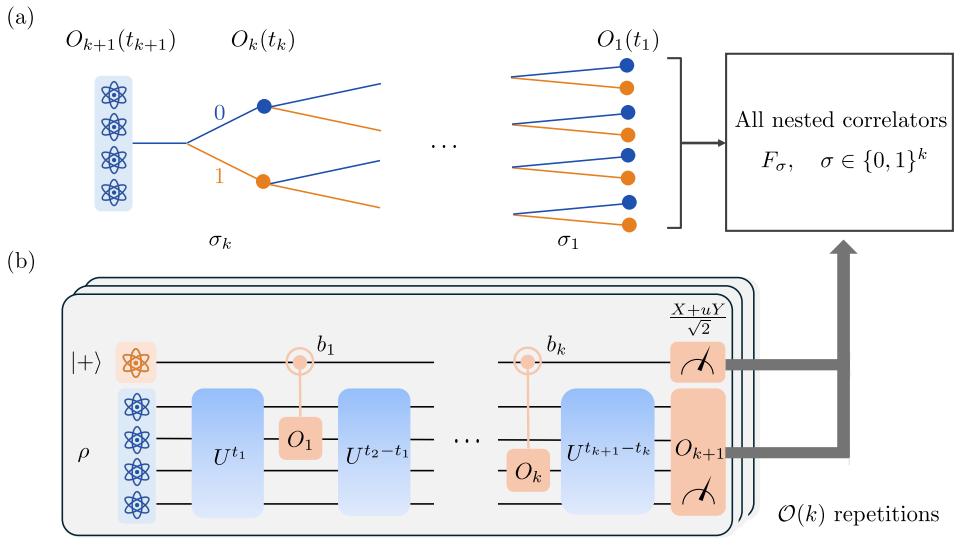

图 2. 同时估计多个嵌套关联函数的协议。(a) 嵌套关联函数的结构。系统的动力学生成一个由 2^k 嵌套对易子和反对易子组成的完整族。每个关联函数由一个二进制字符串 σ 指定，因此该族的规模会随时间段数量 k 的增加呈指数增长。(b) 基于探针的量子电路。在每次实验运行中，随机采样一个轨迹配置 b，并分别将系统和辅助探针量子比特初始化为 ρ 和 $|+\rangle$。在 U 下的演化与由 b 和可观测量 O_j 控制的条件性探针—系统相互作用交替进行，随后对两个寄存器执行最终测量。将这一单一随机化过程重复 $\mathcal{O}(k)$ 次，即足以同时重构全部 2^k 个嵌套关联函数。

对于纯初态 $\rho = |\psi\rangle\langle\psi|$，重叠 $Q_b = \langle\psi_{\bar{b}}|O_{k+1}|\psi_b\rangle$ 表示两个互补历史 $|\psi_b\rangle = W_b|\psi\rangle$ 与 $|\psi_{\bar{b}}\rangle = W_{\bar{b}}|\psi\rangle$之间的干涉振幅。我们的关键观察是，目标嵌套关联函数由这些轨迹重叠的沃尔什–哈达玛变换给出（见引理S12）：

$$F_\sigma(U) = \frac{i^{|\sigma|}}{2}\,\mathbb{E}_{b\sim\{0,1\}^k}\left[(-1)^{\sigma\cdot b}Q_b\right]. \tag{3}$$

至关重要的是，干涉振幅 Q_b 仅取决于路径字符串 b，而与目标配置无关 σ。因此，实验过程无需针对任何特定的嵌套关联函数进行定制，从而实现测量兼容性。将原生系统与单个探针量子比特耦合后，便可直接获取这些振幅：在每次实验运行中，我们均匀采样 b，并将对 U 的正向查询与已知可观测量的相干探针控制应用 O_j 按照 b（图2b）交替进行。随后分别对探针和系统执行最终测量，即可得到关于 Q_b的无偏 动力学快照，其中编码了有关底层关联的丰富信息。利用 $\mathcal{O}(k)$ 个此类独立快照，该算法通过经验沃尔什–哈达玛变换同时重构整个 2^k 嵌套关联函数族。可以将其类比于量子态的经典影子；经典影子同样旨在预测多个可观测量 [50]。

建立相匹配的指数下界是我们的主要技术贡献，因为这需要排除所有可能的仅系统协议，包括配备任意自适应电路中操作的协议。为此，我们构造了一个由随机酉演化组成的困难系综，使目标信号隐藏在一个未知的关联函数配置中 $\theta \in \{0,1\}^k$。从物理上看，该信号编码在扩展动力学轨迹之间的相对相位中，而这些轨迹的中间态被 Haar 随机基所遮蔽。单量子比特探针能够相干地干涉这些隐藏路径，但任何试图盲目穿行于随机基之间的仅系统协议，都不可避免地会遭受量子相干性的压缩映射。我们通过将任何仅系统协议归约为一种大幅简化的理想过程 (物理图景见方法部分，完整归约见附录 A–D）。在这一理想过程中，我们证明，无辅助量子比特测量能够提取的关于 θ 的信息随 k呈指数衰减，从而确证额外量子比特不可或缺（附录 F）。

对于 $T = k$，这些结果确立了探测多时刻动力学关联时的指数级单量子比特优势——$\mathcal{O}(k^2)$ 次查询，对比 $\Omega(k2^k)$ 次查询——并凸显出，单个额外量子比特能够重构的动力学性质数量呈指数级增长，超过任何仅系统协议所能重构的数量。

B. 估计单个关联函数的指数级优势

虽然同时学习指数多的性质能带来显著的信息论优势，但对大规模多体系统的研究往往旨在分离特定的目标量。然而，如果我们将关注范围限制在估计单个预先确定的嵌套关联函数 $F_\sigma(U)$，这种指数级差距似乎会消失，因为通过调整无辅助量子比特顺序弱测量协议 $\mathcal{O}(T\varepsilon^{-2})$，便可用 [34, 35, 37] 次查询高效地提取这一特定量（附录 I）。要在实际设备上展现这种优势，一个直接的问题是：当任务只是估计单个动力学性质时，单量子比特探针是否仍能带来指数级优势?

我们对此给出肯定的回答，并证明即使在估计单个多时关联函数时，单量子比特的指数级优势依然存在。与上文分析的嵌套关联函数不同，这个 $(k+1)$ 时关联函数定义为

$$C(U) = \mathrm{Tr}[O_{k+1}(t_{k+1})O_k(t_k)\cdots O_1(t_1)\rho] = Q_{\mathbf{1}}, \tag{4}$$

其中 $\mathbf{1}=(1、.....、1)$。此类关联函数对于诊断量子动力学 [7–10, 14, 32, 37, 51]以及展示实用的量子优势 [52–54]也至关重要。

从物理上看，$C(U) = Q_{\mathbf{1}}$ 表示完全扰动轨迹 $W_{\mathbf{1}}$（其中包含所有中间算符插入）与未扰动轨迹 $W_{\mathbf{0}} = U^T$之间的干涉振幅；后者由最终可观测量O_{k+1} 在时刻 $T = t_{k+1}$ (式 (2))中的探针测得。因此，基于探针的估计可通过算法1的干涉原语实现。^具体而言，可将路径配置固定为 $C(U)$，并对快照 $b = \mathbf{1}$ 取平均来估计 Q。此过程还原了文献 [32](附录 J)中的单量子比特干涉方案。

尽管这种干涉测量方法已知具有很高的效率，并且优于现有的无辅助量子比特算法，但它是否能相对于<样式 id='1'>所有</样式>可能的仅系统策略取得严格的指数级优势，仍然是一个悬而未决的问题。这需要给出仅系统策略的一般下界。下面的定理通过确立指数级分离解决了这一问题。

定理 2（估计单个关联函数时的指数级单量子比特优势，非正式表述）。考虑在总演化时间 T 内、跨越 $k+1$ 个连续时刻，对未知的 n 量子比特幺正演化 U 的 $k+1$ 时刻关联函数 C 进行估计，使其误差不超过加性误差 ε，并以高概率成功。

1. 基于探针：借助一个辅助量子比特，可以使用 $q = \mathcal{O}\big(T\varepsilon^{-2}\big)$ 次总查询来估计 C（U）。

2. 仅系统：对于 $T = k \le n/5$ 以及恒定误差 ε，任何无辅助量子比特协议都需要 $q = \Omega(2^k)$ 次查询 .

证明这一指数下界极具挑战性，因为这需要排除所有仅系统策略，即使目标只是单个关联函数。为此，我们将上文构建的归约框架应用于任意无辅助量子比特协议，将其映射到一个简化的理想过程。在此框架中，我们构造了两个关联函数值相反的幺正动力学系综，C（U）$= \pm 1$，其信息仅编码在两条长度为k的动力学轨迹之间的相对相位中，而轨迹的中间态始终处于隐藏状态。我们证明，除非耗费指数级数量的查询，否则任何仅系统协议对这两个系综产生的测量记录都几乎无法区分（形式化推导见附录E ）。

对于 $T = k$，这种 $\mathcal{O}(k)$ 与 $\Omega(2^k)$ 的查询分离，源于仅提取单个干涉振幅，这表明量子干涉本身就是辅助探针所提供的基础资源。

C. 时间最优性：量子记忆时间带来的指数级优势

上述指数级优势可以通过保留两条动力学轨迹之间的相干性，并在读出时使它们发生干涉来理解。现在，我们将通过探讨基于探针的方法在时间方面的最优性，补上最后一块拼图。换句话说，与相干时间较短的机器相比，延长量子机器的记忆时间是否也能指数级增强其观测能力?

我们对这个问题给出了肯定的回答：将相干时间延长到足以涵盖与演化过程的额外一次交互 U，即可获得指数级优势。为使这一点形式化，我们将相干查询次数 定义为单次实验运行中，在必须测量或重置所有量子寄存器之前，允许对 U 进行的最大查询次数。以此为指标，我们证明了一个精确的复杂度阈值，展示了我们协议在时间上的最优性：如果实验人员每次运行的相干查询次数上限为 $L < k$，那么无论可用量子存储器的大小如何，估计嵌套关联函数 $F_\sigma(U)$ 或单个多时间关联函数 $C(U)$，都不可避免地需要多出指数级数量的实验。值得注意的是，当辅助寄存器仅包含少数量子比特（如我们的协议所示）时，所需的记忆时间直接由相干查询次数决定。

定理 3（最优性：受限相干下的指数下界，非正式表述）。考虑在未知的 n 量子比特酉演化 U 的 $k+1$ 个连续时刻上，以常数加性误差和高概率估计单个多时间关联函数 $C(U)$ 或指定的嵌套关联函数 $F_\sigma(U)$。

对于 $k \le n/5$，任何每次运行最多只能进行 $L < k$ 次相干查询的协议，都需要总查询复杂度达到 $q = 2^{\Omega(n)}$。即使辅助量子存储器不受限制，且允许任意自适应电路中操作，这种指数级开销依然存在。

形式化表述见定理S4。对于连续观测时刻 $t_j = j-1$，我们的基于探针的算法（算法1）每次运行仅需 k 次正向查询，即可探测跨越 $k+1$ 个时间步的相关性。因此，该算法在量子存储器大小和相干时间两方面同时达到最优性，相较于所有低于这一相干阈值运行的协议，具有指数级优势。

从实践角度看，即使可用相干时间较短（例如 $k=2$），这种指数级差距依然存在，为在近期量子设备上展示量子观测优势提供了一条途径 [6, 52–54]，，而相干时间仍是主要瓶颈 [55, 56]。

D. 数值实验：预测探针信号

量子传感的一项关键任务，是理解外部扰动如何影响耦合探针的信号，从而深入了解环境噪声及其对量子相干性的影响 [57]，并为量子控制提供指导 [46]。具体而言，解析这些信号的高阶分量，可用于区分量子核自旋与经典场 [12]，并揭示量子比特中的非高斯噪声 [10]。

受这些能力的启发，我们通过数值实验表明，我们的学习算法能够预测不同扰动下的高阶探针信号，其表现优于仅系统基线 [34, 35, 37]（附录 I）。我们考虑将多体环境视为一个 n自旋系统（其中 $n=10$），并设其未知演化 $U = e^{-iH\Delta}$ 由广泛研究的非可积混合场伊辛哈密顿量生成，

$$H = \sum_{i=1}^{n-1} Z_i Z_{i+1} + 1.05 \sum_{i=1}^{n} X_i + 0.5 \sum_{i=1}^{n} Z_i,$$

时间步长为 $\Delta = 0.4$。环境初始处于非平衡态 $\rho = (I + X_1)/2^{10}$，并使用制备于 $|+\rangle$ 的辅助量子比特 Q 进行探测。探针在时刻（t_1，...，t_9）=（0、1、3、4、5、7、9、10、12）与边界自旋相互作用。这些相互作用由控制角 $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_8)$ 以及独立、均匀采样的脉冲符号 $\boldsymbol{s} = (s_1, \ldots, s_9) \in \{\pm 1\}^9$ 参数化。在前八个步数（$j = 1, \ldots, 8$）中的每一步，我们施加边界旋转 $e^{-is_j \alpha_j Z_1/2}$ 和探针–系统耦合 $e^{-is_j(\pi/2-\alpha_j)Z_Q \otimes Z_1/2}$。最后一步，我们施加耦合 $e^{-is_9 \pi Z_Q \otimes Z_1/4}$（图 3a）。

我们的任务是预测所得探针信号如何随控制参数变化。具体而言，我们考察探针的相干项，$L(\mathbf{s};\boldsymbol{\alpha}) = \langle X_Q \rangle - i\langle Y_Q \rangle$，并关注其按符号加权的分量，该分量可表示为（附录 K）

$$S(\boldsymbol{\alpha}) := \mathbb{E}_{\boldsymbol{s}} \left[\left(\prod_{j=1}^{9} s_j \right) L(\boldsymbol{s};\boldsymbol{\alpha}) \right] = 2 \sum_{\sigma \in \{0,1\}^8} w_\sigma(\boldsymbol{\alpha}) F_\sigma(U). \tag{5}$$

在物理上，与多体环境耦合的单量子比特探针的这一高阶相干分量 $S(\boldsymbol{\alpha})$ 能够揭示无法从低阶环境谱中分辨出的噪声。重要的是，第二个等式将信号表示为嵌套关联函数的线性组合，其中 $F_\sigma(U)$ 是式（1）中定义的关联函数，且 $O_j = Z_1$。信号对控制参数的依赖性由系数 $w_\sigma(\boldsymbol{\alpha})$刻画，因此，估计这些嵌套关联函数，就能预测探针信号 $S(\boldsymbol{\alpha})$ 对任意未见过的 $\boldsymbol{\alpha}$，而无需进行新的实验。

我们应用算法1，使用 $2^8 = 256$ 实验运行次数来估计所有 N 嵌套关联函数。作为基准，我们采用仅系统协议（算法2，附录I），该协议使用 $N/256$实验运行次数分别估计每个关联函数。两种方法每次运行均使用 $t_9 = 12$ 次查询，U，从而确保总查询预算相同，均为 $q = 12N$。在 $N = 2^{24}$时，我们的算法能够准确重现完整的关联函数谱，而仅系统基准则表现出显著更大的误差（图3b）。图3c 通过对关联函数族和 $D = 1024$ 个独立数据集取平均，量化了这一改进，指标为均方根误差（RMSE）。均方根误差约降低了十倍，这意味着我们的算法只需约百分之一的实验运行次数即可达到相同精度。

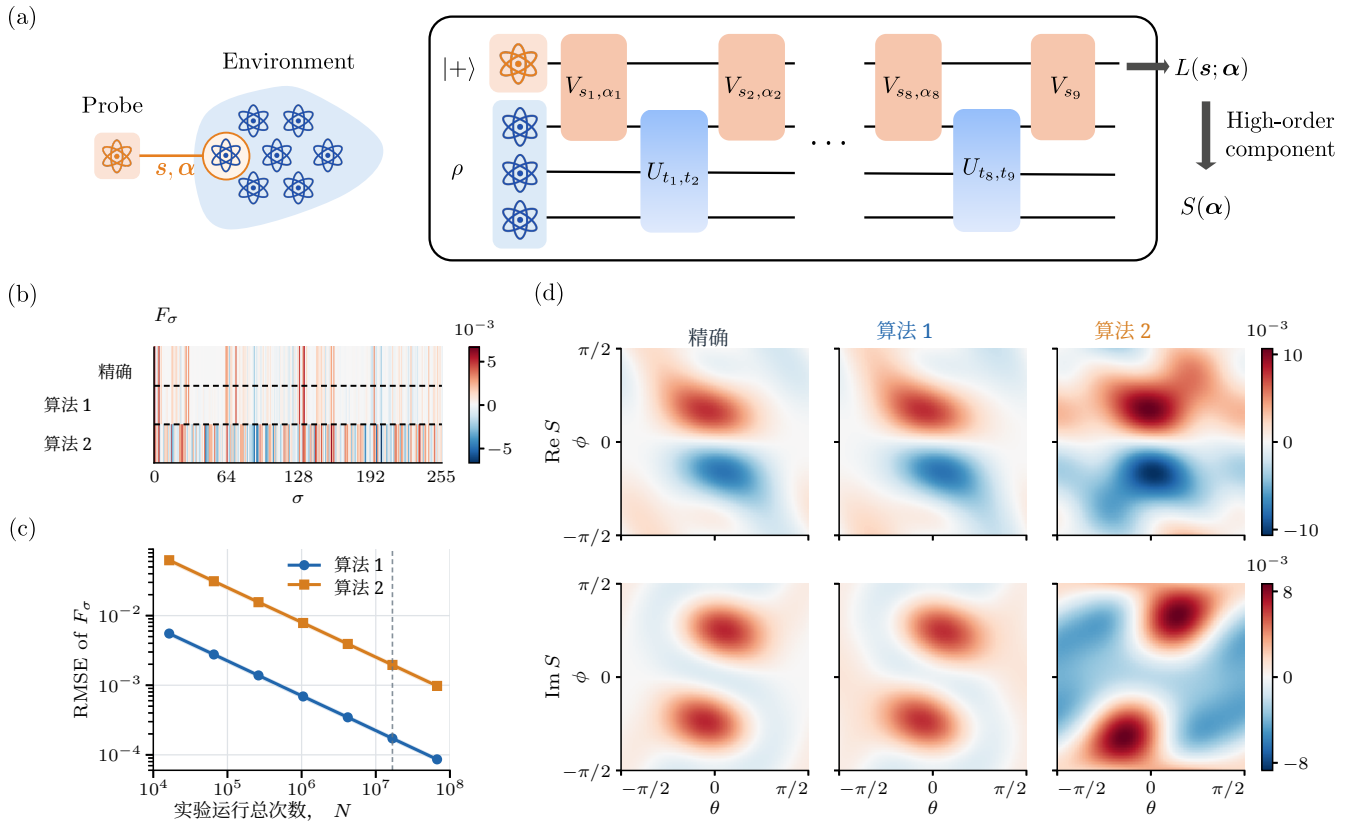

FIG. 3. 基于探针的关联函数估计。(a) 目标多体系统（环境）与单量子比特探针的边界自旋相互作用。控制操作 V_{s_j,α_j} 与参数化脉冲符号 s_j 和角度 α_j 交错进行，目标演化为 $U_{t,\,t'} = e^{-iH\Delta(t'-t)}$。

预测目标是探针相干性 $L(\boldsymbol{s};\,\boldsymbol{\alpha})$ 的带符号权重高阶分量 $S(\boldsymbol{\alpha})$。（b）使用每个算法 $N = 2^{24}$ 次实验运行，给出全部 256 个嵌套关联函数 F_σ 的精确值和估计值。算法 1 使用共享测量记录来估计整个关联函数族，而算法 2 为每个关联函数分配 $N/256$ 次实验运行。（c）在每个预算 N 下，对所有关联函数和 1024 个独立测量数据集计算均方根误差。阴影带表示每个数据集均方根误差的中心 95% 区间。竖直虚线标记 $N = 2^{24}$，即（b）和（d）中使用的预算。（d）给出 $S(\theta, \phi)$ 的精确值与预测值的实部（上）和虚部（下），其中 $\alpha_{1,3,5,7} = \theta$ 以及 $\alpha_{2,4,6,8} = \phi$。预测值由（b）中的关联函数估计值重构而得，未进行额外实验。

随后，我们利用这些学习得到的关联函数，在无需额外实验的情况下预测探针信号。为便于可视化，我们设 $\alpha_j = \theta$，当 j 为奇数时，且 $\alpha_j = \phi$，当 j为偶数时。使用与图3b 中相同的关联函数估计值，我们的算法成功捕捉了 $S(\theta,\ \phi)$实部和虚部的结构与振幅，而仅系统重构则出现了明显失真（图3d）。这表明，在预测此类非线性信号时，我们的基于探针的方法优于传统的仅系统基线方法。上述分析可自然应用于多体系统的非线性光谱学；其响应函数取决于嵌套多时间关联函数的高阶结构，从而揭示出常规线性响应谱中被掩盖的特征 [15–17]。数值实验的详情见附录K。

III. 讨论

我们证明，只需为量子机器增加一个量子比特，就能在观测量子多体动力学方面获得指数级优势。这种优势体现在三个方面。首先，单量子比特探针使对不同动力学性质的测量彼此兼容，从而能够重建数量呈指数级增长的嵌套关联函数。其次，通过对延展的动力学轨迹进行相干干涉，即便只估计单个多时刻关联函数，探针也能大幅降低查询复杂度，且降幅呈指数级。最后，在整条轨迹中维持这种相干性是最优的，这确立了它相较于任何受限于较短记忆时间的协议所具有的指数级优势。

我们的框架具有很强的相关性 关实验前沿架构，例如基于探针的量子技术

术 [19, 21, 47]和混合数字-模拟量子模拟器 [58, 59]。尽管近期实验突破显著延长了量子存储时间 [55, 56, 60], ，实现容错量子计算仍然充满挑战。我们的基于探针的协议利用适度的存储器规模和相干时间，在无需付出高昂资源开销的情况下实现指数级优势。展望未来，一个值得探究的问题是，增加探针能否解锁更多能力 [36], ，例如估算非时序关联函数，从而根据探针规模建立更精细的优势层级 [61]。我们的框架还提供了一条途径，用于刻画量子学习与量子传感中辅助存储器和相干时间之间的基本时空权衡。

数字量子模拟的成熟将赋予实验人员对底层演化过程更加丰富的控制。具体而言，能够获得 U 的显式门分解，可实现高级查询类型，例如时间反演演化 $U^\dagger$ 或相干受控酉算符，从而可能在量子观测中带来进一步优势 [62–64]。此外，由于实际多体系统通常受已知的局域性结构或对称性支配，纳入此类先验物理知识可以进一步降低学习或认证的开销 [44, 65–67]。最终，容错架构将支持把这些观测任务与先进量子算法相结合，从而引出一个颇具吸引力的问题：这种综合能否带来前所未有的加速 [68–70]。

致谢

Z.D.和X.M.获得国家自然科学基金委员会（项目编号：12575023）、量子科学与技术国家科技重大专项（项目编号：2021ZD0300804和2021ZD0300702）、CCF-QuantumCtek超导量子计算专项合作计划（项目编号：CCF-QC2025005）以及南京图灵人工智能研究院的支持。V.V.感谢戈登与贝蒂·摩尔基金会和Conjecture研究所提供的资金支持。

[1] R. P. Feynman，用计算机模拟物理。《国际理论物理学杂志》21，467–488（1982）。[2] S. Lloyd，通用量子模拟器。《科学》273，1073–1078（1996）。[3] Y. Kim 等，故障容错实现前量子计算效用的证据。《自然》618，500–505（2023）。[4] A. D. King 等，量子模拟中的超越经典计算。《科学》388，199–204（2025）。[5] R. Haghshenas 等，在囚禁离子量子计算机上实现数字量子磁性。《自然》，第1–7页（2026）。[6] Google Quantum AI 和合作者，观察到量子遍历性边缘的相长干涉。《自然》646，825–830（2025）。[7] S. A. Crooker、D. G. Rickel、A. V. Balatsky 和 D. L. Smith，将自发自旋噪声光谱学作为探测自旋动力学和磁共振的探针。《自然》431，49–52（2004）。[8] A. Laraoui、F. Dolde、C. Burk、F. Reinhard、J. Wrachtrup 和 C. A. Meriles，金刚石中氮空位中心附近^{13}C自旋的高分辨率关联光谱学。《自然·通讯》4，1651（2013）。[9] L. M. Norris、G. A. Paz-Silva 和 L. Viola，非高斯退相干环境的量子比特噪声谱学。《物理评论快报》116，150503（2016）。[10] Y. Sung 等，利用超导量子比特传感器进行非高斯噪声谱学。《自然·通讯》10，3715（2019）。[11] M. Pfender 等，通过连续弱测量对单个核自旋进行高分辨率光谱学。《自然·通讯》10，594（2019）。[12] J. Meinel、V. Vorobyov、P. Wang、B. Yavkin、M. Pfender、H. Sumiya、S. Onoda、J. Isoya、R.-B. Liu 和 J. Wrachtrup，单个核自旋的量子非线性光谱学。《自然·通讯》13，5318（2022）。[13] Y. Shen、P. Wang、C. T. Cheung、J. Wrachtrup、R.-B. Liu 和 S. Yang，通过量子关联检测不受经典噪声影响的量子信号。《物理评论快报》130，070802（2023）。[14] K. E. Dorfman、F. Schlawin 和 S. Mukamel，量子光的非线性光学信号与光谱学。《现代物理评论》88，045008（2016）。[15] J. Lu、X. Li、H. Y. Hwang、B. K. Ofori-Okai、T. Kurihara、T. Suemoto 和 K. A. Nelson，集体自旋波的相干二维太赫兹磁共振光谱学。《物理评论快报》118，207204（2017）。[16] Y. Wan 和 N. P. Armitage，通过太赫兹二维相干光谱学中的自旋子回波分辨分数量子激发连续谱。《物理评论快报》122，257401（2019）。[17] W. Choi、K. H. Lee 和 Y. B. Kim，Kitaev自旋液体二维非线性光谱学理论。《物理评论快报》124，117205（2020）。[18] C. Zhang 等，利用多体核自旋回波进行分子几何结构的量子计算，arXiv:2510.19550（2025）。[19] M. Cetina 等，耦合到费米海的杂质的超快多体干涉测量。《科学》354，96–99（2016）。

[20] J. M. Boss、K. S. Cujia、J. Zopes 和 C. L. Degen，具有任意频率分辨率的量子传感。《科学》356，837 840 2017–（）。[21] K. Rezai、S. Choi、M. D. Lukin 和 A. O. Sushkov，利用单量子比特传感器探测二维偶极自旋系综的动力学。《物理评论快报》134，050801（2025）。[22] Y. Xia、A. R. Agrawal、C. M. Pluchar、A. J. Brady、Z. Liu、Q. Zhuang、D. J. Wilson 和 Z. Zhang，纠缠增强的光机械传感。《自然·光子学》17，470–477（2023）。[23] E. Knill 和 R. Laflamme，一比特量子信息的力量。《物理评论快报》81，5672–5675（1998）。[24] H.-Y. Huang 等，从实验中学习的量子优势。《科学》376，1182–1186（2022）。[25] I. Kannan、S. Prabhu、S. A. Khan、M. M. Sohoni、X. Song、S. Roy、A. Senanian、V. Fatemi、P. L. McMahon 和 J. Cotler，利用单个量子比特学习信号的指数级量子优势，arXiv:2608.13521（2026）。[26] X. Mi 等，量子电路中的信息扰乱。《科学》374，1479–1483（2021）。[27] K. A. Landsman、C. Figgatt、T. Schuster、N. M. Linke、B. Yoshida、N. Y. Yao 和 C. Monroe，经验证的量子信息扰乱。《自然》567，61–65（2019）。[28] M. Kuffer、A. Zwick 和 G. A. Álvarez，通过诱导量子探针动力学中的时间反演对称性破缺，传感非平衡环境和量子非高斯环境。《PRX Quantum》6，020320（2025）。[29] S. Chen、J. Cotler、H.-Y. Huang 和 J. Li，使用与不使用量子存储器进行学习的指数级差距。2021年IEEE第62届计算机科学基础年度研讨会（FOCS）论文集，574–585（2022）。[30] D. Aharonov、J. Cotler 和 X.-L. Qi，量子算法测量。《自然·通讯》13，887（2022）。[31] Z.-H. Liu 等，可扩展光子平台上的量子学习优势。《科学》389，1332–1335（2025）。[32] J. S. Pedernales、R. Di Candia、I. L. Egusquiza、J. Casanova 和 E. Solano，用于计算n时关联函数的高效量子算法。《物理评论快报》113，020505（2014）。[33] N. Y. Yao、F. Grusdt、B. Swingle、M. D. Lukin、D. M. Stamper-Kurn、J. E. Moore 和 E. A. Demler，探测快速扰乱的干涉测量方法，arXiv:1607.01801（2016）。[34] J. Dressel、J. R. González Alonso、M. Waegell 和 N. Yunger Halpern，增强量子比特非时序关联函数的弱测量。《物理评论A》98，012132（2018）。[35] L. Del Re、B. Rost、M. Foss-Feig、A. F. Kemper 和 J. K. Freericks，在数字量子计算机上稳健测量驱动耗散量子系统的 n点关联函数。《物理评论快报》132，100601（2024）。[36] W. Dong、A. G. Green、V. Vedral 和 J. Sun，量子探针在多体系统学习中的优势，arXiv:2607.11829（2026）。[37] X. Wang、L. Xiong、X. Cai 和 X. Yuan，无需辅助量子比特计算 n时关联函数。《物理评论快报》135，230602（2025）。[38] M. H. Abobeih、J. Randall、C. E. Bradley、H. P. Bartling、M. A. Bakker、M. J. Degen、M. Markham、D. J. Twitchen 和 T. H. Taminiau，利用量子传感器对由27个核自旋组成的簇进行原子尺度成像。《自然》576，411–415（2019）。[39] G. L. Van De Stolpe、D. P. Kwiatkowski、C. E. Bradley、J. Randall、M. H. Abobeih、S. A. Breitweiser、L. C. Bassett、M. Markham、D. J. Twitchen 和 T. H. Taminiau，通过关联传感绘制50自旋量子比特网络。《自然·通讯》15，2006（2024）。[40] C. C. V. de Pradenne、J. Cotler 和 H.-Y. Huang，长时间下学习哈密顿量，arXiv:2606.05690（2026）。[41] A. J. Daley、I. Bloch、C. Kokail、S. Flannigan、N. Pearson、M. Troyer 和 P. Zoller，量子模拟中的实用量子优势。《自然》607，667–676（2022）。[42] A. Browaeys 和 T. Lahaye，利用单独控制的里德堡原子研究多体物理。《自然·物理》16，132–142（2020）。[43] J. Cotler、D. L. Danielson 和 I. Kannan，传感经典场性质的量子优势。《物理评论X》16，041025 2026（）。[44] Z. Liu、Z. Du、Y. Tang、Z.-W. Liu、J. Eisert 和 I. Roth，时间反演对称性的高效认证需要纠缠，arXiv:2610.01555（2026）。[45] R. J. Lewis-Swan、A. Safavi-Naini、A. M. Kaufman 和 A. M. Rey，量子信息动力学。《自然综述：物理》1，627–634（2019）。[46] Z. Wu、P. Wang、T. Wang、Y. Li、R. Liu、Y. Chen、X. Peng 和 R.-B. Liu，通过量子信道选择性检测动力学完备关联集合。《物理评论快报》132，200802（2024）。[47] F. Xia、S. Li、X.-Y. Pan、P. Wang 和 G.-Q. Liu，通过四阶关联揭示量子自旋浴从高斯到非高斯转变。《物理评论快报》134，253601（2025）。[48] K. T. Geier 和 P. Hauke，量子多体系统中从非厄米线性响应到动力学关联与涨落耗散关系。《PRX Quantum》3，030308（2022）。[49] P. Wang、H. Kwon、C.-Y. Luan、W. Chen、M. Qiao、Z. Zhou、K. Wang、M. S. Kim 和 K. Kim，在多个时间点对量子动力学进行快照。《自然·通讯》15，8900（2024）。[50] H.-Y. Huang、R. Kueng 和 J. Preskill，通过极少量测量预测量子系统的多种性质。《自然·物理》16，1050–1057（2020）。[51] T. Schweigler、V. Kasper、S. Erne、I. Mazets、B. Rauer、F. Cataldini、T. Langen、T. Gasenzer、J. Berges 和 J. Schmiedmayer，通过高阶关联对量子多体系统进行实验表征。《自然》545，323–326（2017）。[52] C. Neill 等，精确计算量子环的电子性质。《自然》594，508–512（2021）。[53] E. Kökcü、H. A. Labib、J. K. Freericks 和 A. F. Kemper，用于量子模拟玻色和费米关联函数的线性响应框架。《自然·通讯》15，3881（2024）。[54] J. Sun、L. Vilchez-Estevez、V. Vedral、A. T. Boothroyd 和 M. S. Kim，利用量子模拟器探测量子多体系统的谱特征。《自然·通讯》16，1403（2025）。

[55] B. L. Brock、S. Singh、A. Eickbusch、V. V. Sivak、A. Z. Ding、L. Frunzio、S. M. Girvin 和 M. H. Devoret，突破盈亏平衡点的量子多能级系统量子纠错。《自然》641，612–618（2025年）。[56] Google Quantum AI 和合作者等，低于表面码阈值的量子纠错。《自然》638，920–926（2025年）。[57] Y.-X. Wang 和 A. A. Clerk，用于增强基于量子比特的量子噪声谱学的内禀与诱导量子淬火。《自然·通讯》12，6528（2021年）。[58] D. Bluvstein 等，基于纠缠原子阵列相干输运的量子处理器。《自然》604，451–456（2022年）。[59] T. I. Andersen 等，模拟-数字量子模拟器上的热化与临界性。《自然》638，79–85（2025年）。[60] T. He 等，通过全微波泄漏抑制实现低于表面码阈值的实验量子纠错。《物理评论快报》135，260601（2025年）。[61] M.-H. Hsieh、M. de Oliveira、S. Subramanian 和 X. Zhang，浅层量子电路的最坏情况深度层级，arXiv:2606.16425（2026年）。[62] E. Tang、J. Wright 和 M. Zhandry，共轭查询可以提供帮助，arXiv:2510.07622（2026年）。[63] E. Tang 和 J. Wright，受控酉算子是否有帮助？，arXiv:2508.00055（2026年）。[64] R. King、K. Wan 和 J. R. McClean，借助共轭态和最小量子存储器实现指数级学习优势。《PRX Quantum》5，040301（2024年）。[65] J. Haah、R. Kothari 和 E. Tang，从高温吉布斯态和实时演化过程中学习量子哈密顿量。《自然·物理》20，1027–1031（2024年）。[66] H.-Y. Hu、M. Ma、W. Gong、Q. Ye、Y. Tong、S. T. Flammia 和 S. F. Yelin，无拟设哈密顿量学习与海森堡极限标度。《PRX Quantum》6，040315（2025年）。[67] M. Gao、Z. Ji、Q. Wang、W. Yu 和 Q. Zhao，量子哈密顿量认证。2026年ACM-SIAM离散算法年度研讨会（SODA）论文集，1424–1467。[68] R. R. Allen、F. Machado、I. L. Chuang、H.-Y. Huang 和 S. Choi，量子计算增强传感，arXiv:2501.07625（2025年）。[69] Y.-J. Liu、R. R. Allen、R. Shen、B. Ye、T. T. Chang、J. Choi 和 S. Choi，离散频率谱学的最优量子传感算法，arXiv:2611.21560（2026年）。[70] I. Kannan、A. Venkatesh 和 J. Cotler，算法量子传感，arXiv:2611.25572（2026年）。[71] A. A. Mele，《量子信息中的Haar测度工具简介：初学者教程》。《Quantum》8，1340（2024年）。

方法

A. 操作模型

为刻画仅系统模型中最一般的自适应策略，我们考虑一个本征的 n 量子比特寄存器$\mathcal{H} = \mathbb{C}^d$ $(d = 2^n)$以及一段经典测量历史 h。连续查询之间的操作由依赖历史的量子仪器 $\{K_{z|h}\}$ 表示，满足 $\sum_z K_{z|h}^\dagger K_{z|h} = I$，并将任何初始化和中间操作一并吸收其中。给定一段历史 h 和一个新的测量结果 z，量子寄存器的未归一化分支状态 σ 在第 j 次查询后演化为

$$\sigma_{hz}^{(j+1)}(U) = U K_{z|h}^{(j)} \sigma_h^{(j)}(U) (K_{z|h}^{(j)})^\dagger U^\dagger. \tag{6}$$

经过 q 次查询后，最终操作被吸收到一个依赖历史的正算子值测度 $\{M_{y|h}\}$ 中，从而得到输出分布

$$p(y \mid U) = \sum_h \mathrm{Tr}\big(M_{y|h} \sigma_h^{(q)}(U)\big). \tag{7}$$

相比之下，基于探针的模型引入了一个额外的量子比特，未知演化 U 不会作用于该量子比特，因此它可以在连续查询之间保持相干（图 1b）。值得注意的是，尽管我们的仅系统下界适用于任意自适应仪器 $\{K_{z|h}\}$，我们的基于探针的协议每次运行前只需选定非自适应的探针—系统相互作用，并分别对探针和系统进行最终测量。

在时间受限的情形下（定理 3），我们关注相干查询次数 L。在此，实验者可使用任意数量且不受限制的辅助量子寄存器。然而，每次实验运行最多只能进行L 次对 U的正向查询。各次运行之间，所有量子存储器都必须经过测量或被彻底丢弃，仅保留经典记录，以便自适应地配置后续实验。

B. 估计多个嵌套关联函数的算法

我们基于探针的协议使用单个辅助量子比特，使互补的动力学轨迹发生相干干涉，并获取关联函数族的沃尔什–哈达玛谱，详情见算法 1。

算法 1 使用一个额外量子比特同时估计嵌套关联函数

要求： 初始态 ρ、已知可观测量 O_1、 $\ldots, O_{k+1}$、观测时间 $0 \le t_1 \le \cdots \le t_{k+1}$以及重复次数 N。

对于 $r = 1, \ldots, N$ **do**
  将系统制备为 ρ，并将探针制备为 $|+\rangle$。 ▷初始化并随机化
  均匀抽取 $b \in \{0,1\}^k$，并独立抽取一个公平符号 $u \in \{\pm 1\}$。
  在 U 作用下演化系统 t_1 步。
  对于 $j = 1, \ldots, k$ **执行** ▷ 干涉互补轨迹
    应用 $|0\rangle\langle 0| \otimes O_j^{b_j} + |1\rangle\langle 1| \otimes O_j^{1-b_j}$。
    在 U 下将系统演化 $t_{j+1} - t_j$ 步。
  结束循环
  在探针上测量 $(X + uY)/\sqrt{2}$，得到 $a \in \{\pm 1\}$。
  测量系统上的 O_{k+1}，得到 $x \in \{\pm 1\}$。
  存储 $b_r = b$ 和 $\widehat{Q}_r = \sqrt{2}\, a x\, (1 - iu)$。
结束循环
对 $\sigma \in \{0,1\}^k$ **执行** ▷沃尔什–哈达玛变换
  计算 $\widehat{F}_\sigma = \dfrac{1}{2N} \displaystyle\sum_{r=1}^{N} (-1)^{\sigma \cdot b_r} \, \text{实部}\left[i^{|\sigma|} \widehat{Q}_r \right]$。
结束循环
返回 $\{\widehat{F}_\sigma\}_{\sigma \in \{0,1\}^k}$。

在此算法中，每次实验运行都会测量互补路径重叠的一个单次无偏估计量。具体而言，通过将探针制备为叠加态并执行条件演化，$\widehat{\quad}$ $\widehat{\quad}$对探针和系统进行最终联合测量，即可得到满足 Q 的快照 $\mathbb{E}[Q \mid b] = Q_b$。如附录H所述，这一干涉测量原语确保每个快照的方差都有界。应用标准集中不等式（如霍夫丁不等式），并对所有 $M = 2^k$ 括号模式使用并集界，我们证明，只需进行 $N = \mathcal{O}(\varepsilon^{-2} \log(M/\delta))$ 次实验重复，即可确保以高概率 ε 同时对所有嵌套关联函数达到加性误差。

C. 下界背后的物理直觉

这里，我们概述仅系统协议的指数下界（定理1 和2）背后的核心机制。两种构造都采用相似的困难实例，将目标信号编码在隐藏轨迹之间的干涉中。为便于理解，我们在此聚焦于较简单的单关联函数情形；多个关联函数的同时估计则留待附录F。

1. 在互补轨迹中编码信号

为建立指数下界，我们构造了一组幺正动力学，其中目标关联函数$C(U) = s \in \{\pm 1\}$ 仅编码在两条互补动力学轨迹之间的相对相位中。我们将系统初始化为已知的根态 $|a_0\rangle = |\psi\rangle$，并使用已知的二值可观测量 $O = Z_1$定义其正交对应态 $|b_0\rangle = O|\psi\rangle$。在每个内部层 $1 \le j < k$，酉算子 U 将这些状态进一步传播至系统深处：

$$U|a_{j-1}\rangle = |a_j\rangle, \qquad U|b_{j-1}\rangle = O|b_j\rangle. \tag{8}$$

请注意，第一条轨迹完全在 U 作用下演化，而第二条轨迹则需要在每一步交错插入 O。在最终深度 k 处，两条轨迹分别到达 $|a_k\rangle$ 和 $sO|a_k\rangle$。对 O 进行最终测量，会产生恰好等于 $C(U) = s$ 的干涉振幅。重要的是，改变 s 只会翻转相对相位，而不会改变任一路径各自的密度矩阵。基于探针的协议能够自然地通过将系统相干地沿这两条路径传输，读出这一相对符号。

为了让仅使用系统的机器无法处理这一任务，我们将这些中间轨迹设为不可观测。我们不再使用固定且已知的状态，而是在每个内部层从相互独立的 Haar随机正交归一框架中抽取 $|a_j\rangle$ 和 $|b_j\rangle$ 。因此，状态 $|a_j\rangle$、$O|a_j\rangle$、$|b_j\rangle$、$O|b_j\rangle$ 彼此正交，实验者也完全无法知晓。我们将这些指定跃迁补全为一个随机酉预言机，确保目标符号被深深隐藏（详细构造请参见附录 A 1 和 E1 ）。

2. 量子相干性的不可逆压缩映射

为了界定仅系统协议能够提取的信息，我们将系统的物理演化映射为一种高度简化的理想过程(定理S1)。这一框架表明，任何自适应策略（包括中间测量和反馈控制）都可纳入其中；而试图盲目穿行于随机标架之间，会导致一种严重的有效退相干机制。

在理想过程中，只有成功通过所有 $k-1$ 个内部层的贡献才能抵达最终目标量。在每一步中，一个测量结果 z 通过有效控制 $\alpha_z I+\beta_z O$作用于路径。由于随机基彼此正交，只有 I 分量会推进第一条轨迹（$|a_j\rangle$），而只有 O 分量会推进第二条轨迹（$O|b_j\rangle$）。因此，两条路径之间的任何非对角量子相干性 c 都会在后续层中衰减至 $c_z=\alpha_z\beta_z\,c$。由于物理仪器必须满足完备性关系 $\sum_z(|\alpha_z|^2+|\beta_z|^2)\le 1$，保留下来的相干性至少会收缩一半（引理S10）：

$$\sum_z |c_z| = |c|\sum_z |\alpha_z\beta_z| \le \frac{1}{2}|c|.$$

由于一条轨迹从根出发时，其相干性幅度至多为其概率权重的一半，经过 $k-1$ 次连续压缩映射后，到达端点时可用的相干信号会呈指数级衰减，最多为 2^{-k} 。仅翻转目标符号 s，只会反转这个指数级微小的非对角元素，使最终理想输出分布产生至多 2^{1-k} 的全变差距离扰动。将此误差累加到一个包含 q 次查询的协议中，可得总界 $q\,2^{1-k}$。将此界转移回真实的物理系综，可得

$$\mathrm{TV}(\mathsf{Out}_+,\mathsf{Out}_-)\le q\,2^{1-k}+\mathcal{O}\left(\frac{q^2+q\sqrt{k}}{\sqrt{d}}\right),$$

其中第二项计入了以理想过程替代物理动力学所引入的误差。对 $C(U)$ 进行加性误差为 $1/3$ 且成功概率为 $2/3$ 的精确估计量能够区分这两个符号，因此全变差距离严格来说至少须达到 $1/3$。当 $n\ge 4k$时，这意味着查询复杂度必须为 $q=\Omega(2^k)$（定理S2）。

补充材料

A 分层隐藏预言机及其理想过程.13 植入族 • 理想过程 B 玻色记录与算子估计.16 福克空间作为多项式矩的表示 • 记录空间 • 隐藏编码器与系统操作的压缩 • 补全记录器与隐藏标签的返回 • 具有等距编码器的记录预言机 C 从Haar预言机到记录模型.22 正向查询的正矩比较 • 高斯补全记录 • 将Haar标架耦合到高斯标架 • 累积并平均框架误差 • 复高斯框架场 • 用等距编码器替代高斯场 • 有限粒子域与累积误差 D 从记录模型到理想过程.32 提升理想效应 • 一次反向步骤 • 自适应递归及在真空态上的求值 E 估计多时刻关联函数的无辅助系统下界.38 困难预言机族 • 向理想过程的约化 • 两条路径之间相干性的收缩 • 下界的补全 F 同时估计嵌套关联函数的无辅助系统下界.42 互补路径展开 • 仅有一个非零关联函数的隐藏树 • 归约到理想树 • 遍历过程中的乘积态 • 一次端点访问所获的信息 • 自适应控制下的信息累积 • 下界的补全 G 相干查询次数的下界.49 隐藏树及其首层 • 与一个独立于符号的过程比较 • 构造耦合的Haar补全 H 单辅助量子比特同时估计嵌套关联函数.56 I 单个嵌套关联函数的无辅助比特估计.57 J 单辅助量子比特多时刻关联函数估计.58 K 数值实验详情.60 模型 • 探针信号与关联函数展开 • 学习算法的实现

附录 A：分层隐藏预言机及其理想过程

本附录介绍两个下界所共用的构造。我们首先利用已知可观测量 O的特征子空间构造一族随机酉算子。随后，我们引入一个更简单的理想过程，用以替代预言机查询以及查询之间施加的仪器。最后，模拟定理（定理S1）表明，对随机酉算子取平均后，原协议的经典输出分布与理想过程的经典输出分布十分接近。

全文中，$\|\cdot\|$、$\|\cdot\|_1$和 $\|\cdot\|_{\mathrm{HS}}$ 分别表示算子范数、迹范数和希尔伯特–施密特范数。我们用 $\mathrm{TV}(p,\ p') = \frac{1}{2}\|p - p'\|_1$ 表示全变差距离，用 $\operatorname{col}_z A_z : x \mapsto \bigoplus_z A_z x$ 表示列算子。

1. 隐藏族

设 O 是作用于 $\mathcal{H} = \mathbb{C}^d$ 上的已知二值可观测量，满足 $O^2 = I$ 且 $\operatorname{Tr} O = 0$。在每个特征子空间中选取一个已知单位向量，并称这些向量张成的空间为根子空间。设 $J : \mathbb{C}^2 \to \mathcal{H}$ 是到该子空间上的等距映射，其投影算子为 $R_0 = JJ^\dagger$。对于 $\sigma \in \{+, -\}$，设 $\mathcal{H}_\sigma$ 为相应特征子空间中所选向量的正交补，并设 Π_σ 为其投影算子。则

$$\mathcal{H} = \operatorname{Ran} J \oplus \mathcal{H}_+ \oplus \mathcal{H}_-, \qquad \dim \mathcal{H}_\sigma = N = d/2 - 1.$$

对于 $1 \le r \le N$，独立抽取 Haar分布的 r 标架 $F_\sigma :\ \mathbb{C}^r \to \mathcal{H}_\sigma$。定义

$$\mathcal{L} = \mathcal{L}_+ \oplus \mathcal{L}_-, \qquad \mathcal{L}_\sigma = \mathbb{C}^r, \qquad F = F_+ \oplus F_-.$$

空间 $\mathcal{L}$ 为隐藏态提供固定标签，而等距映射 F 将它们嵌入物理空间 $\mathcal{H}$。令 $Z_{\mathcal{L}}$ 在 $\mathcal{L}_+$ 上作用为 $+I$，在 $\mathcal{L}_-$上作用为 $-I$，使得 $OF = FZ_{\mathcal{L}}$。

将标签空间正交分解为若干层：

$$\mathcal{L} = \bigoplus_{j=1}^{\ell} \mathcal{L}_j, \qquad Z_{\mathcal{L}} \mathcal{L}_j \subseteq \mathcal{L}_j, \qquad \ell \geq 1. \tag{A.1}$$

每一层都在 $Z_{\mathcal{L}}$ 作用下保持不变，因此分解为其 $+$ 扇区和 $-$ 扇区。其像 $F\mathcal{L}_j$ 是相应的隐藏物理层。令根为 $\mathcal{L}_0 = \mathbb{C}^2$。对于每个中间层 $1 \leq j < \ell$，选取一个有限维输入坐标空间 $\mathcal{I}_j$，以及一个等距嵌入 $V_j \colon \mathcal{I}_j \to \mathcal{L}_j$。记

$$\Gamma_j = V_j V_j^{\dagger}$$

表示投影到 $\mathrm{Ran}\, V_j$ 的投影算子。这是我们将指定向层 $j+1$ 的跃迁的子空间，且它不必充满 $\mathcal{L}_j$。在根处，取 $\mathcal{I}_0 = \mathcal{L}_0$、$V_0 = I$ 和 $\Gamma_0 = I$。在端点处，令 $\Gamma_\ell = 0$，因为没有指定跃迁离开最后一层。

令 ϑ 为预言机族的索引。标签空间、它们的层分解以及输入嵌入 V_j，都独立于 ϑ 和随机标架而固定。对 ϑ 的依赖通过指定跃迁引入：对于每个 ϑ，选取部分等距算子 $S_{\vartheta,\,j} \colon \mathcal{L}_j \to \mathcal{L}_{j+1}$，且这些算子独立于标架，并满足

$$S_{\vartheta,j}^{\dagger} S_{\vartheta,j} = \Gamma_j, \qquad 0 \leq j < \ell. \tag{A.2}$$

因此，$S_{\vartheta,\,j}$ 在 $\mathrm{Ran}\, V_j$ 上是等距的，并在其正交补上为零。每个指定变换都前进一层，且没有任何变换返回根。

将输入坐标空间汇集为

$$\mathcal{I} = \bigoplus_{j=0}^{\ell-1} \mathcal{I}_j, \qquad p = \dim \mathcal{I} = 2 + \sum_{j=1}^{\ell-1} \dim \mathcal{I}_j \leq 2 + 2r.$$

组合跃迁映射 $S_\vartheta \colon \mathcal{I} \to \mathcal{L}$，以及物理输入嵌入和输出嵌入 V_F，$W_{F,\,\vartheta} \colon \mathcal{I} \to \mathcal{H}$ 定义如下：

$$\begin{aligned} S_\vartheta|_{\mathcal{I}_j} &= S_{\vartheta,j} V_j \quad (0 \leq j < \ell), \\ V_F|_{\mathcal{I}_0} &= J, \\ V_F|_{\mathcal{I}_j} &= F V_j \qquad (1 \leq j < \ell), \\ W_{F,\vartheta} &= F S_\vartheta. \end{aligned} \tag{A.3}$$

这些映射都是等距映射：它们的分块保持内积，且其值域两两正交。对于 V_F，这也用到了根与隐藏物理层之间的正交性。

现在，我们将指定变换补全为一个酉算子。令 $D = d - p$。选取等距映射 C_F，$B_{F,\,\vartheta} \colon \mathbb{C}^D \to \mathcal{H}$，使其值域分别为 $\mathrm{Ran}\, V_F$ 和 $\mathrm{Ran} W_{F,\,\vartheta}$ 的正交补空间。从与标架独立的分布中抽取 H，并定义

$$U_{F,H,\vartheta} = W_{F,\vartheta} V_F^{\dagger} + B_{F,\vartheta} H C_F^{\dagger}, \qquad H \sim \mathrm{Haar}(\mathrm{U}(D)). \tag{A.4}$$

第一项实现指定变换，第二项则将剩余输入空间酉映射到剩余输出空间。这两项的输入空间和输出空间彼此正交，因此 $U_{F,\,H,\,\vartheta}$ 是酉算子，并满足

$$U_{F,H,\vartheta} V_F = W_{F,\vartheta}.$$

这对 $(F,\ H)$ 只抽样一次，并且每次查询都使用由此得到的酉算子。根据 Haar 不变性，其分布与互补空间的基选择无关。

2. 理想过程

理想过程通过移除对随机标架 F 和补全 H的显式依赖，简化了物理动力学。它追踪标签空间中的跃迁，在每一层内保留量子相干性，但不保留不同层之间的相干性。残余块 $|\perp\rangle\langle\perp|$ 仅记录概率权重。其直观理解是，随机标架和补全会将未追踪的分量扩散到广阔的物理空间中，因此很难利用少量查询来获取其详细结构

。定理 S1 通过比较最终的经典输出分布，对这一简化进行了量化；其中，物理分布是对 $(F,\ H)$ 的单次初始抽样取平均值所得。

具体而言，理想态在以下子空间上呈分块对角形式

$$\mathcal{L}_0 \oplus \mathcal{L}_1 \oplus \cdots \oplus \mathcal{L}_\ell \oplus \mathbb{C}|\perp\rangle, \qquad \omega = \rho_0 \oplus \cdots \oplus \rho_\ell \oplus p_\perp |\perp\rangle\langle\perp|. \tag{A.5}$$

这里，$\rho_j \succeq 0$、$p_\perp \geq 0$ 和 $\sum_{j=0}^{\ell} \operatorname{Tr} \rho_j + p_\perp = 1$。对于已知的物理初始态 ρ，将理想过程初始化为

$$\omega_{\text{in}} = J^\dagger \rho J \ \oplus\ 0_{\mathcal{L}} \oplus \big(1 - \operatorname{Tr}(R_0\rho)\big)|\perp\rangle\langle\perp|. \tag{A.6}$$

因此，根块保留了将 ρ 压缩到已知根子空间的结果，而剩余概率则分配给残余块。

对于第 j 层的输入，理想查询的作用为

$$\mathcal{Q}_\vartheta(\rho_j) = S_{\vartheta,j}\rho_j S_{\vartheta,j}^\dagger + \operatorname{Tr}[(I - \Gamma_j)\rho_j]|\perp\rangle\langle\perp|, \qquad 0 \leq j < \ell. \tag{A.7}$$

支撑在 值域Γ_j 上的分量前进至第 $j+1$ 层，其余权重则成为残余权重。所有端点权重均被送至 $\perp$，已有的残余权重也保留在该处。将这些贡献相加，即定义了查询对一般理想态的作用。根据（A.2），此映射是完全正且保迹的。没有查询输出进入根块，因此每次查询后根块都会立即变为零。

在查询之间，理想过程使用由物理协议的仪器所决定的跃迁规则。它遵循相同的自适应经典策略：对于每段历史，所选的物理仪器决定相应的理想仪器。这些仪器可能会在下一次查询前将权重返回根块。

考虑一个满足 $\sum_z K_z^\dagger K_z = I$ 的物理仪器 $\{K_z\}_z$，并省略其对历史的依赖。定义

$$\begin{aligned} \kappa_{z\sigma} &= \frac{\operatorname{Tr}(\Pi_\sigma K_z)}{N}, & D_z &= \bigoplus_{\sigma=\pm} \kappa_{z\sigma} I_{\mathcal{L}_\sigma}, \\ p_{z\sigma} &= \frac{\operatorname{Tr}(\Pi_\sigma K_z^\dagger K_z)}{N}, & Q_{z\sigma} &= \frac{J^\dagger K_z \Pi_\sigma K_z^\dagger J}{N}, \\ w_{z\sigma} &= p_{z\sigma} - \operatorname{Tr} Q_{z\sigma} - |\kappa_{z\sigma}|^2. \end{aligned} \tag{A.8}$$

这些系数由 K_z 和已知的扇区投影算子决定，其中不包含任何抽样框架。算子 D_z 描述留在当前层中的分量，而 $Q_{z\sigma}$ 和 $w_{z\sigma}$ 描述向根块和残余块的转移。具体而言，设 $P_{j\sigma}$ 为 $\mathcal{L}_j$ 的 σ 扇区上的投影算子。对于隐藏输入块 ρ_j，$1 \leq j \leq \ell$，与测量结果 z 相关的未归一化贡献为

$$\begin{aligned} \text{same layer:}\ & D_z \rho_j D_z^\dagger, \\ \text{root:}\ & \sum_{\sigma=\pm} \operatorname{Tr}(P_{j\sigma}\rho_j) Q_{z\sigma}, \\ \text{residual weight:}\ & \sum_{\sigma=\pm} \operatorname{Tr}(P_{j\sigma}\rho_j) w_{z\sigma}. \end{aligned} \tag{A.9}$$

扇区不变性确保 D_z 保持每一层不变。对于单位残余输入 $|\perp\rangle\langle\perp|$，相应的贡献为

$$\begin{aligned} \text{root:}\ & \frac{J^\dagger K_z K_z^\dagger J}{d}, \\ \text{residual weight:}\ & \frac{\operatorname{Tr}(K_z^\dagger K_z) - \operatorname{Tr}(J^\dagger K_z K_z^\dagger J)}{d}. \end{aligned} \tag{A.10}$$

对于剩余权重 $p_\perp$，将这些表达式乘以 $p_\perp$。不存在残余到隐藏的转移。

我们用 $\Phi_K = \{\Phi_{K,z}\}_z$ 表示这个理想仪器。对所有输入块的贡献求和，即得到测量结果 z对应的未归一化理想态。其迹就是结果概率。将 z 追加到经典历史中，并根据物理协议的策略选择下一个仪器。

每个结果映射都是完全正的，并且它们的和在不含根块的状态上保持迹；查询后立即就会出现这种情况。为验证这一点，首先注意到 $Q_{z\sigma} \succeq 0$ 和

$$\begin{aligned} p_{z\sigma} - \operatorname{Tr} Q_{z\sigma} &= \frac{\|(I - R_0)K_z\Pi_\sigma\|_{\text{HS}}^2}{N} \\ &\geq \frac{\|\Pi_\sigma K_z \Pi_\sigma\|_{\text{HS}}^2}{N} \geq \frac{|\operatorname{Tr}(\Pi_\sigma K_z)|^2}{N^2} = |\kappa_{z\sigma}|^2. \end{aligned} \tag{A.11}$$

因此 $w_{z\sigma} \geq 0$。同层贡献是一个Kraus映射。其他隐藏输入贡献则测量一个扇区，并制备一个正根矩阵或剩余权重。对于支撑在扇区 σ 中的输入，它们的合并输出迹（包括同层贡献）等于输入迹的 $p_{z\sigma}$ 倍。Kraus完备性给出 $\sum_z p_{z\sigma} = 1$。剩余输入贡献也都是正的，其测量结果 z 对应的总迹为 $\mathrm{Tr}(K_z^\dagger K_z)/d$，这些值加起来为一。

还需指定最终测量。对于作用于 $\mathcal{H}$ 上的算子 K，定义其在隐藏标签空间上的扇区平均作用为

$$T(K) = \bigoplus_{\sigma=\pm} \frac{\mathrm{Tr}(\Pi_\sigma K)}{N} I_{\mathcal{L}_\sigma}.$$

由于最后一次查询后根块为零，终端效应只需作用于隐藏块和剩余块。对于物理POVM $\{M_y\}_y$，理想效应为

$$M_y^{\mathrm{id}} = T(M_y) \oplus \frac{\mathrm{Tr}\, M_y}{d} |\perp\rangle\langle\perp|. \tag{A.12}$$

它们均为正算子，且在 $\mathcal{L} \oplus \mathbb{C}|\perp\rangle$ 上的和为恒等算子。对于依赖历史的最终POVM，在每段历史下分别应用此规则。综合这些规则，即可定义一个归一化的理想输出分布。

以下定理说明了为何可以使用这一更简单的过程来证明下界：理想输出的可区分性界可以转移到物理预言机，误差至多为一个较小的量子模拟误差。

定理 S1 (分层隐藏预言机的模拟)。 存在普适常数 c，$C > 0$ 使得以下结论成立。考虑任意预言机族 (A.4)，其具有固定的根嵌入和输入嵌入、扇区不变层，以及 (A.1)–(A.3)中指定的跃迁。假设 $r \leq N = d/2 - 1$ 且 $p \leq 2 + 2r$。对于每个满足以下条件的整数 $q \geq 1$

$$\Delta(q, r, d) = \frac{q^2 + q\sqrt{r+1}}{\sqrt{d}} \leq c, \tag{A.13}$$

每个仅保留原始 d 维量子系统且至多进行 q 次正向查询的自适应协议都满足

$$\mathrm{TV}(\mathsf{Out}_\vartheta, \mathsf{Out}_\vartheta^{\mathrm{id}}) \leq C\Delta(q, r, d) \tag{A.14}$$

对于每个固定的 ϑ。其中，Out_ϑ 是对一次初始抽样 (F, H)取平均后得到的物理输出分布，而 $\mathsf{Out}_\vartheta^{\mathrm{id}}$ 是相应理想过程的输出分布。

证明使用玻色记录模型将物理预言机与理想过程联系起来。我们首先用高斯矩阵替换 Haar 补全和隐藏Haar标架，并界定由此导致的协议平均输出变化。高斯多项式矩具有玻色记录态内积的精确表示，因此对记录进行偏迹即可还原高斯平均输出。在这一记录表示中，我们用等距编码器近似高斯标架算子。最后，我们通过记录演化向后传播测量效应，并证明它们遵循理想过程的更新规则，且仅产生很小的累积误差。

附录 B 构造记录预言机，并建立证明所需的算子估计。附录 C比较物理输出与记录输出，而附录 D 比较记录输出与理想输出。结合这两个界即可证明定理 S1。

附录 B：玻色记录与算子估计

本附录为建立用于连接物理预言机与理想过程的记录模型做准备。玻色记录对高斯变量的多项式依赖进行编码，使得对这些变量取平均值可以表示为对记录空间取偏迹。我们首先说明这种对应关系并明确记录空间。随后，我们为隐藏标签构造一个等距编码器，并为随机补全构造一个记录器，最后将两者组合成一个记录预言机。

这些估计有两个作用。它们控制从高斯框架场到附录C中的等距编码器的近似，并确定附录D的理想过程中出现的扇区平均值和残余动力学。记录空间是仅在证明中使用的辅助空间。

1. 福克空间作为多项式矩的表示

玻色记录使我们能够用偏迹表示高斯平均值。我们首先回顾相关的福克空间算符，然后为多项式振幅确立这种对应关系。

对于单粒子希尔伯特空间 $\mathfrak{h}$，定义玻色福克空间

$$\mathcal{F}(\mathfrak{h}) = \bigoplus_{n=0}^{\infty} \mathrm{Sym}^n \mathfrak{h}.$$

这里，$\mathrm{Sym}^n \mathfrak{h}$ 是 $\mathfrak{h}^{\otimes n}$ 的置换不变子空间，而 $\mathrm{Sym}^0 \mathfrak{h} = \mathbb{C}|\Omega\rangle$ 是真空扇区。选取 $\mathfrak{h}$ 的正交归一模基 $\{|j\rangle\}_j$。归一化占据态 $|\boldsymbol{n}\rangle$ 在模式 j 中有 n_j 个粒子，产生算符与湮灭算符的作用方式如下：

$$a_j^\dagger |\boldsymbol{n}\rangle = \sqrt{n_j+1}\,|\boldsymbol{n}+\boldsymbol{e}_j\rangle, \qquad a_j|\boldsymbol{n}\rangle = \sqrt{n_j}\,|\boldsymbol{n}-\boldsymbol{e}_j\rangle.$$

当 $n_j = 0$ 时，湮灭算符的作用结果为零。

为便于后续进行范数估计，引入湮灭映射与产生映射

$$\begin{aligned} &\mathsf{A}_n : \mathrm{Sym}^n \mathfrak{h} \longrightarrow \mathfrak{h} \otimes \mathrm{Sym}^{n-1} \mathfrak{h}, && \mathsf{A}_n \xi = \sum_j |j\rangle \otimes a_j \xi, \quad \|\mathsf{A}_n\| = \sqrt{n}, \\ &\mathsf{T}_n : \mathfrak{h} \otimes \mathrm{Sym}^n \mathfrak{h} \longrightarrow \mathrm{Sym}^{n+1} \mathfrak{h}, && \mathsf{T}_n(|j\rangle \otimes \xi) = a_j^\dagger \xi, \qquad \|\mathsf{T}_n\| = \sqrt{n+1}. \end{aligned} \tag{B.1}$$

这里，A_n 对 $n \geq 1$ 有定义，而 T_n 对 $n \geq 0$ 有定义。第一个范数恒等式由 n 粒子扇区上的 $\sum_j a_j^\dagger a_j = nI$ 得出。第二个则由 $\mathsf{T}_n = \mathsf{A}_{n+1}^\dagger$ 得出。等价地，T_n 是对称化的 $\sqrt{n+1}$ 倍。——

现在令 g_j 为相互独立的标准复高斯变量。对应关系

$$\prod_j g_j^{n_j} \longmapsto \prod_j (a_j^\dagger)^{n_j} |\Omega\rangle = \sqrt{\prod_j n_j!}\,|\boldsymbol{n}\rangle$$

保持内积：不同的单项式在高斯测度下彼此正交，且每个单项式的平方范数为 $\prod_j n_j!$，与其记录向量相符。将此映射线性扩展到全纯多项式，也就是不含变量 g_j 的共轭变量的多项式。用 $|p\rangle_{\mathrm{rec}}$ 表示 p 的记录向量，则有

$$\langle p_j \mid p_i \rangle_{\mathrm{rec}} = \mathbb{E}[p_i(g)\overline{p_j(g)}]$$

对于振幅为多项式的系统向量，对所有振幅使用同一个记录空间：

$$|v(g)\rangle = \sum_i p_i(g)|i\rangle \quad \longmapsto \quad |\widehat{v}\rangle = \sum_i |i\rangle \otimes |p_i\rangle_{\mathrm{rec}}.$$

内积恒等式给出

$$\mathrm{Tr}_{\mathrm{rec}} |\widehat{v}\rangle\langle\widehat{v}| = \sum_{i,j} \mathbb{E}\left[p_i(g)\overline{p_j(g)}\right] |i\rangle\langle j| = \mathbb{E}_g[|v(g)\rangle\langle v(g)|]\,.$$

因此，对 记录求偏迹即可重现完整的平均输出算符，包括其非对角元素 .

为处理同时包含高斯变量及其共轭变量的框架振幅，我们引入第二组模式。相应的表示在附录 C中建立。

2. 记录空间

回顾附录 A中的扇区标签空间：

$$\mathcal{L} = \mathcal{L}_+ \oplus \mathcal{L}_-, \qquad Z_{\mathcal{L}}|\alpha,\sigma\rangle = \sigma|\alpha,\sigma\rangle.$$

选取 $\mathcal{H}_\sigma$ 的一组标准正交基 $\{|i,\sigma\rangle\}_i$，以及 $\mathcal{L}_\sigma$的一组标准正交基 $\{|\alpha,\sigma\rangle\}_\alpha$。每个框架条目由物理行 i、标签列 α和公共扇区 σ索引。对应的单粒子记录空间为

$$\mathfrak{h}_f = (\mathcal{H}_+ \otimes \mathcal{L}_+) \oplus (\mathcal{H}_- \otimes \mathcal{L}_-). \tag{B.2}$$

直和体现了标架的扇区结构：连接相反扇区的条目为零，因此不需要记录模式。

完整的记录空间由三个玻色模式族组成：

$$\mathcal{F} = \mathcal{F}(\mathfrak{h}_f)_a \otimes \mathcal{F}(\mathfrak{h}_f)_b \otimes \mathcal{F}(\mathbb{C}_X^d \otimes \mathbb{C}_Y^d)_c. \tag{B.3}$$

这 a 和 b 两个模式族共同表示高斯标架条目及其共轭变量。 c 模式族表示一个完整的$d \times d$ 高斯矩阵 Γ，其条目 Γ_{yx} 的方差为 $1/D$。这里， x 为输入坐标的索引， y 为输出坐标的索引。尽管补全作用于 D维子空间之间，使用完整的 $d \times d$ 矩阵可以让我们在固定的物理坐标中定义其记录，而不依赖于标架。对于固定的标架，压缩 $B_{F,\,\vartheta}^{\dagger}\Gamma C_F$ 的独立条目服从分布 $\mathcal{N}_{\mathbb{C}}(0, 1/D)$。因此，它给出了原始 D维 Haar 补全的高斯替代。此表示在附录 C中确立。

令 n_a、 n_b、 n_c 表示三个模式族的总占据数。记 $\Pi_{\le R}^{\mathrm{rec}}$ 为投影到 $n_a + n_b + n_c \le R$上的投影算子。仅限制一个模式族时，记为 $\Pi_{n_a \le R}$ 或 $\Pi_{n_c \le q}$。在诸如 $A\Pi_{\le R}^{\mathrm{rec}}$这样的表达式中，投影算子只限制 A的输入，而输出可能占据更高的粒子数扇区。所有涉及无界玻色算子的恒等式，均视为定义在有限粒子向量上。下文的范数估计采用所标明的受限输入定义域，在这些定义域上，相关算子均有界。

3. 隐藏编码器与系统操作的压缩

现在，我们构造一种等距编码，将隐藏标签编码到物理系统和框架记录中。其关键性质是，通过这种编码压缩已知的系统操作，可得到理想过程中所用的扇区平均作用的近似结果。

从定义在有限粒子输入上的产生算子矩阵开始，

$$E_0 = \frac{1}{\sqrt{N}} \sum_{\sigma,i,\alpha} |i,\sigma\rangle\langle\alpha,\sigma| \otimes a_{i\alpha\sigma}^{\dagger}. \tag{B.4}$$

它将 $\mathcal{L} \otimes \quad \mathcal{F}$映射到 $\mathcal{H} \otimes \mathcal{F}$，并产生一个 a粒子。特别地，对于记录为真空态的标签， s,

$$E_0(|\alpha,\sigma\rangle \otimes |\Omega\rangle) = \frac{1}{\sqrt{N}} \sum_i |i,\sigma\rangle \otimes |i,\alpha,\sigma\rangle_a, \tag{B.5}$$

其中 $|i,\ \alpha,\ \sigma\rangle_a$ 表示相应的单粒子记录态。

对于系统算子 K，回顾其对标签的扇区平均作用：

$$T(K) = \bigoplus_{\sigma=\pm} \kappa_\sigma I_{\mathcal{L}_\sigma}, \qquad \kappa_\sigma = \frac{\mathrm{Tr}(\Pi_\sigma K)}{N}. \tag{B.6}$$

与记录恒等算子的张量积是隐式的。下一条引理将 E_0 归一化为精确等距映射，并给出用 $T(K)$ 替换压缩算子 $E^{\dagger}KE$ 时的误差界。

引理 S1（具有扇区平均压缩的等距编码器）。 假设 $r \le N$。存在一个全局定义的等距映射 E： $\mathcal{L} \otimes \mathcal{F} \to \mathcal{H} \otimes \mathcal{F}$，它将 n_a 提高一，保持 b、 c 记录不变，并且满足

$$E^{\dagger}E = I, \qquad (O \otimes I)E = E(Z_{\mathcal{L}} \otimes I). \tag{B.7}$$

对于每个系统算子 K 和 $0 \le R \le N/2$,

$$\|(E_0^{\dagger}KE_0 - T(K))\Pi_{n_a \le R}\| \le \frac{R}{N}\|K\|, \tag{B.8}$$

$$\|(E - E_0)\Pi_{n_a \le R}\| \le \frac{2R}{N}, \tag{B.9}$$

$$\|(E^{\dagger}KE - T(K))\Pi_{n_a \le R}\| \le \frac{8R}{N}\|K\|. \tag{B.10}$$

这些估计允许任意的 b、 c 记录，包括与它们的纠缠。

证明。产生映射的压缩。正规序给出

$$a_{i\alpha\sigma}a^{\dagger}_{j\beta\tau} = \delta_{ij}\delta_{\alpha\beta}\delta_{\sigma\tau} + a^{\dagger}_{j\beta\tau}a_{i\alpha\sigma}.$$

因此， $E_0^{\dagger}KE_0$ 从标签（β， τ）到标签（α， σ）的块为

$$(E_0^{\dagger}KE_0)_{\alpha\sigma,\beta\tau} = \delta_{\sigma\tau}\delta_{\alpha\beta}\frac{\mathrm{Tr}(\Pi_\sigma K)}{N}I + \frac{1}{N}\sum_{i,j}K_{i\sigma,j\tau}a^{\dagger}_{j\beta\tau}a_{i\alpha\sigma}.$$

第一项是 T（K）。在 n_a-粒子扇区上，其余算子可以写成

$$\frac{1}{N}\sum_{\ell=1}^{n_a}R_K^{(\ell)}, \qquad \|R_K^{(\ell)}\| \le \|K\|.$$

为了得到这个不依赖标签数量的界，将 $\mathfrak{h}_f$ 嵌入到（$\mathcal{H}_+ \oplus \mathcal{H}_-$）$\otimes\,\mathcal{L}$中。每个记录粒子因此都有一个物理坐标和一个标签坐标。算子 $R_K^{(\ell)}$ 将外部标签与粒子 ℓ的标签互换，对该粒子的物理坐标应用 K 的隐藏空间压缩的转置，并投影回允许的扇区对。这些操作重现了上面的矩阵元素，其范数分别不超过 1、 $\|K\|$ 和 1。

每个 $R_K^{(\ell)}$ 都作用于带编号粒子的环境张量积。虽然单个求和项不一定保持对称子空间，但它们的和会保持该子空间。因此，该算子在该子空间上的限制的范数至多为 $n_a\|K\|$。这就证明了（B.8）。取 $K = I$ 也可得

$$(1 - R/N)I \preceq E_0^{\dagger}E_0 \preceq (1 + R/N)I \qquad \text{on } n_a \le R. \tag{B.11}$$

等距编码器的构造。 我们在每个粒子数扇区上分别定义极分解归一化。为此，我们首先证明 E_0 在每个扇区上都是单射。

通过 $|\boldsymbol{n}\rangle \mapsto z^{\boldsymbol{n}}/\sqrt{\boldsymbol{n}!}$ 将占据向量与多项式对应。在这种对应下，产生算符等于乘以相应的变量。对于每个标签扇区 σ，方程 $E_0 f = 0$ 变为 $Z_\sigma f_\sigma = 0$，其中 Z_σ 是坐标不定元的 $N \times r$ 矩阵。由于 $N \ge r$，其前 r 行构成一个方阵，且其行列式是一个非零多项式。将前 r 个方程乘以伴随矩阵可知，该行列式乘以 f_σ 的每个坐标都等于零。多项式环没有零因子，因此 $f_\sigma = 0$。在两个标签扇区中应用这一论证，即可证明单射性。

现在固定 n_a，并省略不变的 b， c因子。在有限维空间 $\mathcal{L}\otimes\mathrm{Sym}^{n_a}(\mathfrak{h}_f)_a$上，格拉姆矩阵$E_0^{\dagger}E_0$ 正定且可逆。定义

$$E = E_0(E_0^{\dagger}E_0)^{-1/2} \tag{B.12}$$

在此扇区上。对 n_a 取直和，并与 b上的恒等算子张量积， c 记录给出了一个有界的全局等距映射。映射 E 使 n_a 增加一。さらに， $OE_0 = E_0Z_{\mathcal{L}}$ 意味着 $E_0^{\dagger}E_0$ 与 $Z_{\mathcal{L}}$对易。因此，其逆平方根也与 $Z_{\mathcal{L}}$对易，从而证明了（B.7）。

低占据数估计。 限制在 $n_a \le R$ 上，并令 $s = R/N \le 1/2$。根据（B.11）， $G = E_0^{\dagger}E_0$ 的谱位于 $[1 - s, 1 + s] \subseteq [1/2, 3/2]$内。因此，

$$\|G^{-1/2}\| \le \sqrt{2}, \qquad \|G^{-1/2} - I\| \le 2s, \qquad \|G^{1/2} - I\| \le 2s.$$

由于 $E_0 = EG^{1/2}$ 和 E 是等距映射，最后一个界证明了（B.9）。

对于压缩作用，写成

$$E^{\dagger}KE - T(K) = G^{-1/2}(E_0^{\dagger}KE_0 - T(K))G^{-1/2} + [G^{-1/2}T(K)G^{-1/2} - T(K)].$$

第一项没有 至多为 $2s\|K\|$，由（B.8）可得。利用 $\|T$（K）$\| \le \|K\|$，第二项的范数至多为

$$\|G^{-1/2} - I\|\,\|T(K)\|\big(\|G^{-1/2}\| + 1\big) \le 2(1 + \sqrt{2})s\|K\|.$$

它们的和至多为 $8s\|K\|$，由此证明了（B.10）。 □

对于自适应协议，估计必须联合控制所有仪器测量结果。以下列界给出的误差与测量结果的数量无关。

引理 S2 (整个量子仪器的压缩)。 设 $\{K_z\}_z$满足 $\sum_z K_z^\dagger K_z \preceq I$，并令 $D_z = T(K_z)$。对于$0 \le R \le N/2$,

$$\|\mathrm{col}_z(E^\dagger K_z E - D_z)\Pi_{n_a \le R}\| \le \frac{8R\sqrt{d}}{N} \le C\frac{R}{\sqrt{N}}, \tag{B.13}$$

其中 C 是通用的。此外，$\mathrm{col}_z\, E^\dagger K_z E$ 和$\mathrm{col}_z\, D_z$ 都是压缩算子。特别地，

$$\sum_z |\kappa_{z,\sigma}|^2 \le 1 \qquad (\sigma = \pm). \tag{B.14}$$

证明。 对每个 B.10应用（ K_z。算子列的平方范数不超过其各元素平方范数之和，并且

$$\sum_z \|K_z\|^2 \le \sum_z \|K_z\|_{\mathrm{HS}}^2 = \mathrm{Tr}\sum_z K_z^\dagger K_z \le d.$$

这就得到（B.13）中的第一个不等式。第二个不等式由 $d = 2N + 2 \le 4N$ 得出。

压缩后的 Kraus 列可分解为

$$\mathrm{col}_z(E^\dagger K_z E) = \left(\bigoplus_z E^\dagger\right)(\mathrm{col}_z\, K_z)E.$$

每个因子都是压缩算子，因此该列也一样n。最后，由希尔伯特–施密特柯西–施瓦茨不等式可得

$$|\kappa_{z,\sigma}|^2 \le \frac{1}{N}\,\mathrm{Tr}(\Pi_\sigma K_z^\dagger K_z).$$

对 z 求和即可证明（B.14）。由于每个 D_z 在扇区 σ 上都等于标量 $\kappa_{z,\,\sigma}$，这也表明 $\mathrm{col}_z\, D_z$ 是一个压缩映射。 □

4. 补全记录器与返回隐藏标签

补全记录器表示用于随机补全的完整高斯矩阵。我们需要控制它对系统算子的作用，以及它与隐藏编码的耦合。

对于 $\mathcal{H} \otimes \mathcal{F}$ 中的有限粒子输入，定义

$$\mathsf{C} = \frac{1}{\sqrt{D}}\sum_{x,y=1}^{d} |y\rangle\langle x| \otimes c_{xy}^\dagger. \tag{B.15}$$

该算子会创建一个补全粒子，并保持框架记录不变。下一个引理表明，$\mathsf{C}^\dagger K \mathsf{C}$ 等于一个迹平均值加上一个由补全粒子数控制的修正项。它还给出了每次使用 C 所导致的放大效应上界。

引理 S3 （迹平均恒等式与范数界）。 对于系统算子 K，在 n_c-粒子扇区上，

$$\mathsf{C}^\dagger K \mathsf{C} = \frac{\mathrm{Tr}\,K}{D} I + \frac{1}{D}\sum_{\ell=1}^{n_c} \mathsf{S}_\ell (K^{\mathsf{T}})_{Y_\ell}. \tag{B.16}$$

此处S_ℓ 将系统坐标与输入坐标互换 X_ℓ 粒子 ℓ，并且 K^{T} 作用于其输出坐标 Y_ℓ。转置是在(B.15)中使用的物理基下进行的。该求和理解为对对称n_c粒子子空间的限制。

因此，

$$\|\mathsf{C}\Pi_{n_c \le q}\| \le c_q := \sqrt{\frac{d+q}{D}}, \tag{B.17}$$

$$\left\|\left(\mathsf{C}^\dagger K \mathsf{C} - \frac{\mathrm{Tr}\,K}{D} I\right)\Pi_{n_c \le q}\right\| \le \frac{q}{D}\|K\|. \tag{B.18}$$

证明。 展开（B.15）并进行正规序排列，得到

$$\mathsf{C}^\dagger K \mathsf{C} = \frac{1}{D} \sum_{x,u,y,v} |x\rangle\langle u|\, K_{yv} \big(\delta_{xu}\delta_{yv} + c^\dagger_{uv} c_{xy}\big).$$

缩并项为 $(\operatorname{Tr} K/D)I$。剩余项会移除坐标为 (x,y) 的一个粒子，创建一个坐标为 (u,v) 的粒子，并将系统坐标从 u 变为 x。在编号粒子表示中，这恰好是$\mathsf{S}_\ell(K^\mathsf{T})Y_\ell$，并对所有粒子求和。这证明了（B.16）。

每个求和项的范数至多为 $\|K\|$：交换的范数为一，而转置保持算子范数不变。尽管各个求和项未必保持对称子空间不变，但它们的和会保持不变。因此，其限制的范数至多为 $n_c\|K\|$，从而证明了（B.18）。

取 $K = I$ 可得

$$\mathsf{C}^\dagger \mathsf{C} = \frac{d}{D} I + \frac{1}{D} \sum_{\ell=1}^{n_c} \mathsf{S}_\ell, \qquad \|\sum_{\ell=1}^{n_c} \mathsf{S}_\ell\| \le n_c.$$

因此 $\mathsf{C}^\dagger\mathsf{C} \preceq (d+q)I/D$ 在 $n_c \le q$上成立，从而证明了（B.17）。 □

接下来，我们将界定从补全项返回隐藏编码的过程。相关算子为 $E^\dagger K\mathsf{C}$：它应用补全记录器，执行系统操作，并将结果压缩回隐藏标签。这一估计将控制记录预言机中植入部分与补全部分之间的交叉项。

引理 S4 （从补全到隐藏标签的小幅回归）。 对于系统算子 K，在满足 $n_a \le R \le N/2$和 $n_c \le q$ 的输入上，

$$\|E^\dagger K \mathsf{C}\| \le \sqrt{\frac{2R(q+1)}{ND}}\|K\|. \tag{B.19}$$

对于满足 $\sum_z K_z^\dagger K_z \preceq I$ 的 *Kraus* 算子族，在相同的输入定义域上，

$$\|\mathrm{col}_z\, E^\dagger K_z \mathsf{C}\| \le \sqrt{\frac{2dR(q+1)}{ND}}. \tag{B.20}$$

对于不含 a 粒子的输入，这两个映射均为零。

证明。 在进行极分解归一化之前，该算子为

$$E_0^\dagger K \mathsf{C} = \frac{1}{\sqrt{ND}} \sum_{\sigma,\alpha,i,x,y} K_{i\sigma,y} |\alpha,\sigma\rangle\langle x| \otimes a_{i\alpha\sigma} c^\dagger_{xy}.$$

该表达式可分解为三个操作。首先，湮灭一个 a 粒子，并提取其物理坐标（i，σ）和标签（α，σ）。接着，对提取出的物理坐标应用 K^T。最后，创建一个 c 粒子，其输入坐标为原系统坐标 x，输出坐标为所得物理坐标 y。提取出的标签（α，σ）成为输出标签。

根据（B.1），这三个操作的范数分别至多为 $\sqrt{R}$，$\|K\|$和 $\sqrt{q+1}$。计入归一化后，得到

$$\|E_0^\dagger K \mathsf{C}\| \le \sqrt{\frac{R(q+1)}{ND}}\|K\|.$$

该表达式在 a-真空态输入上为零，因为其中包含一个 a-湮灭算 r.

对于非零贡献 ，湮灭操作最多留下 $R-1$ a 个粒子。剩余的极分解因子 i n

$$E^\dagger = (E_0^\dagger E_0)^{-1/2} E_0^\dagger$$

因此其范数至多为 $\sqrt{2}$，根据（B.11）。这证明了（B.19）。将单个算子的界平方后求和，并利用$\sum_z \|K_z\|^2 \le d$，即可证明（B.20）。

□

5. 使用等距编码器的记录预言机

现在，我们将隐藏编码器 E 和补全记录器 C 合并为一个记录预言机。定义输入和输出嵌入 V_E, $W_{E,\vartheta}$: $\mathcal{I}\otimes\mathcal{F}\to\mathcal{H}\otimes\mathcal{F}$ 在（A.3）中用 F 替换 E :

$$\begin{aligned} V_E|_{\mathcal{I}_0\otimes\mathcal{F}} &= J\otimes I_{\mathcal{F}},\\ V_E|_{\mathcal{I}_j\otimes\mathcal{F}} &= E(V_j\otimes I_{\mathcal{F}}) \quad (1\le j<\ell),\\ W_{E,\vartheta} &= E(S_\vartheta\otimes I_{\mathcal{F}}). \end{aligned} \tag{B.21}$$

两个映射都是全局等距映射。对于 V_E，这由 $E^\dagger E=I$、输入层子空间的正交性以及 $J^\dagger E=0$ 得出。对于 $W_{E,\vartheta}$，这是因为 S_ϑ 和 E 都是等距映射。

令 $P_V=V_EV_E^\dagger$ 和 $P_{W,\vartheta}=W_{E,\vartheta}W_{E,\vartheta}^\dagger$。将记录查询定义为

$$\mathcal{U}_{E,\vartheta}=W_{E,\vartheta}V_E^\dagger+(I-P_{W,\vartheta})\mathsf{C}(I-P_V). \tag{B.22}$$

第一项通过隐藏编码实现指定跃迁。第二项在互补输入与输出空间之间应用补全记录器。与物理构造中一样，输出投影算子可以依赖于 ϑ。

下一个引理将控制近似误差的放大，以及经过有限次查询后达到的记录占据数。

引理 S5（范数与记录次数）。对于满足 $n_c\le q$,

$$\|\mathcal{U}_{E,\vartheta}\Pi_{n_c\le q}\|\le c_q:=\sqrt{\frac{d+q}{D}}. \tag{B.23}$$

记录查询将总占据数扇区 n 映射到扇区 n 和 $n+1$之和。其伴随算子绝不会增加总占据数。已知系统操作保持所有记录占据数不变。

证明。投影算子 P_V 和 $P_{W,\vartheta}$ 分别保持 n_a、n_b和 n_c。植入项是部分等距算子，而根据引理 S3，补全项在满足 $n_c\le q$的输入上的范数至多为 c_q。这两项具有正交输入支集和正交输出值域，因此它们之和的范数至多为 $\max\{1,c_q\}=c_q$。由此得到式（B.23）。

对于占据数界，从根开始的植入跃迁会产生一个 a 粒子。在隐藏层之间的植入跃迁会先应用 $E^\dagger$，再应用 E，从而保持 n_a。补全项会产生一个 c 粒子，其周围的投影算子则保持全部三个占据数不变。因此，总占据数唯一可能的变化是 0 和 1。取伴随算子会反转这些变化。已知系统操作在记录上作用为恒等算子，因此保持其占据数不变。

□

对于给定的物理协议，将记录初始化为真空态，并把每次查询替换为$\mathcal{U}_{E,\vartheta}$，同时将每个已知的系统操作与记录恒等算子张量积，由此定义其记录演化。全过程使用同一个记录空间，并沿用该协议原有的依赖历史的仪器和最终读出。完成读出并对记录空间取偏迹后，将正输出算子记为 $\rho_{E,\vartheta}$。

尽管编码器 E 是等距的，完整的记录预言机却未必保迹，因此 $\rho_{E,\vartheta}$ 未必归一化。附录 C 给出了它与平均物理输出之间的迹范数距离上界。附录 D 则比较其事件权重与归一化理想过程的概率。

附录 C：从 Haar 预言机到记录模型

本附录比较平均物理输出与附录B中构造的记录预言机的输出。固定 ϑ 并令 $\Delta=\Delta(q,\ r,\ d)$ 如式（A.13）所定义。令 $\rho_{\mathrm{true},\vartheta}$ 表示对 $(F,\ H)$的一次初始抽样取平均所得的物理输出，并在每次查询时重复使用该抽样。令 $\rho_{E,\vartheta}$ 表示附录 B中定义的正的、可能未归一化的记录输出。下面的命题给出二者差异的上界。

命题 S1（物理输出与记录输出的比较）。存在普适常数 c_0、$C>0$，使得定理 *S1* 中考虑的每个满足 $\Delta\le c_0$ 的协议都满足

$$\|\rho_{\mathrm{true},\vartheta}-\rho_{E,\vartheta}\|_1\le C\Delta. \tag{C.1}$$

证明分为三个步骤。首先，我们将 Haar 补全替换为高斯矩阵，并使用 c 记录表示它。接下来，我们将隐藏 Haar标架替换为高斯矩阵，并使用 a、b 记录表示其元素及共轭变量。最后，我们使用等距编码器 E 对所得的高斯标架算子进行近似。两种高斯到记录的表示都精确保持多项式内积，因此近似误差完全来自两次 Haar 到高斯的替换，以及将标架算子替换为 E。

1. 正向查询的正矩比较

我们首先用一个高斯矩阵替代 Haar 补全，并在整个协议中重复使用该矩阵。下面的引理刻画由此引起的平均输出变化。

引理 S6 (Haar 补全与高斯补全的比较)。 设 A 是一个秩为 $d-D$ 、作用于 $\mathcal{H}$上的部分等距算子。设$B_0, C_0 : \mathbb{C}^D \to \mathcal{H}$ 分别是映射到其输出空间和输入空间正交补空间的等距映射。考虑如下预言机

$$U(H) = A + B_0 H C_0^\dagger.$$

对于至多进行 $q < D$ 次正向查询的协议，令 ρ_H 表示其输出对一次抽样 $H \sim \mathrm{Haar}(\mathrm{U}(D))$取平均后的结果。将 H 替换为一个独立条目服从 Z 的单个矩阵 $\mathcal{N}_{\mathbb{C}}(0, 1/D)$，并将由此得到的平均正输出记为 ρ_Z。在两种情况下，采样矩阵都会在每次查询时重复使用。

With

$$a_q = \frac{q(q-1)}{D-q+1},$$

输出满足

$$e^{-a_q}\rho_Z \preceq \rho_H \preceq e^{a_q}\rho_Z, \qquad \|\rho_H - \rho_Z\|_1 \le e^{a_q}(e^{a_q}-1). \tag{C.2}$$

对于保留额外量子寄存器的协议，这一比较同样成立。

证明。 我们先比较 H 和 Z的齐次矩，再将这一比较应用于该协议的多项式振幅。

齐次矩。 使用未归一化的向量化 $|X\rangle\!\rangle = \sum_{i,j=1}^{D} X_{ij}|i\rangle|j\rangle$，并定义

$$M_{H,t} = \mathbb{E}_H\big[(|H\rangle\!\rangle\langle\!\langle H|)^{\otimes t}\big], \qquad M_{Z,t} = \mathbb{E}_Z\big[(|Z\rangle\!\rangle\langle\!\langle Z|)^{\otimes t}\big].$$

两个算子的支撑集均位于 $\mathrm{Sym}^t(\mathbb{C}^D \otimes \mathbb{C}^D)$ 上。在这个子空间上，维克定理给出

$$M_{Z,t} = t! D^{-t} I. \tag{C.3}$$

为计算 Haar 矩，固定 $1 \le t \le q < D$ 并重新排列张量因子，使所有行指标都排在所有列指标之前。在 $\mathcal{V}_t = (\mathbb{C}^D)^{\otimes t}$ 上，定义置换算子如下：

$$T_\pi |i_1, \dots, i_t\rangle = |i_{\pi^{-1}(1)}, \dots, i_{\pi^{-1}(t)}\rangle, \qquad \pi \in S_t.$$

记 $c(\pi)$ 为 π 的循环数，包括不动点。置换格拉姆矩阵为

$$G_{\pi,\sigma} = \mathrm{Tr}(T_\pi^\dagger T_\sigma) = D^{c(\pi^{-1}\sigma)}.$$

对于 $t \le D$，算子 T_π 线性无关：将它们作用于 $|1, \dots, t\rangle$ 会得到互不相同的正交归一向量。因此， G可逆，其逆矩阵定义了 Weingarten 系数：

$$(G^{-1})_{\pi,\sigma} = \mathrm{Wg}_D(\pi^{-1}\sigma).$$

魏因加滕积分公式 [71, 式（35）–（36）] 给出

$$M_{H,t} = \sum_{\pi,\sigma \in S_t} \mathrm{Wg}_D(\pi^{-1}\sigma) T_\pi \otimes T_\sigma.$$

为了了解张量约定，$M_{H,\,t}$ 它是 twirling 映射的未归一化 Choi 算子

$$X \longmapsto \mathbb{E}_H[H^{\otimes t} X (H^\dagger)^{\otimes t}].$$

$X \mapsto \mathrm{Tr}(T_\sigma^\dagger X) T_\pi$的 Choi 算子为 $T_\pi \otimes (T_\sigma^\dagger)^{\mathsf{T}} = T_\pi \otimes T_\sigma$，因为置换矩阵是实矩阵。定义

$$A_t(D) = \sum_{\pi \in S_t} D^{c(\pi)} T_\pi, \qquad \Pi_{\mathrm{sym}} = \frac{1}{t!} \sum_{\sigma \in S_t} T_\sigma \otimes T_\sigma.$$

此处 Π_{sym} 投影到　重新分组后得到原始对称张量空间。恒等算子 $GG^{-1} = I$ 给出　s

$$\sum_{\pi \in S_t} D^{c(\pi)} \,\mathrm{Wg}_D(\pi^{-1}\tau) = \mathbf{1}_{\{\tau = e\}},$$

其中 e 是恒等置换。因此，将相应的置换算子求和后相乘，可得

$$A_t(D)^{-1} = \sum_{\pi \in S_t} \mathrm{Wg}_D(\pi) T_\pi.$$

Weingarten 系数在共轭和求逆下保持不变，因此对$M_{H,\,t}$ 的双重求和重新分组，可得

$$M_{H,t} = t! \big(A_t(D)^{-1} \otimes I\big) \Pi_{\mathrm{sym}}.$$

此外，由于 $A_t(D)$ 的系数仅取决于循环结构，它与每个置换算子都可交换。因此 $A_t(D)^{-1} \otimes I$ 与 Π_{sym}可交换。

界定 *Haar* 矩。 接下来需要界定 $A_t(D)$。对于 $t \geq 2$，令

$$B_t = \sum_{i=1}^{t-1} T_{(i\,t)}.$$

t 个元素的每个置换，要么固定 t，要么唯一地写成 $\sigma(i\,t)$ 的形式，其中 $\sigma(t) = t$ 且 $i < t$。在第一种情况下，t 会额外贡献一个循环。在第二种情况下，将 t 插入一个已有循环不会改变循环数。因此，

$$A_t(D) = \big(A_{t-1}(D) \otimes I\big)(DI + B_t), \qquad A_1(D) = DI.$$

每个换位算子都是厄米算子，且范数为一，因此

$$\|B_t\| \leq t - 1, \qquad (D - t + 1)I \preceq DI + B_t \preceq (D + t - 1)I.$$

对前 $t-1$ 个位置的置换进行共轭，只会重新排列 B_t 的各项。因此，递推关系中的两个因子可交换。由于 $t \leq D$，由 $A_1(D) = DI$ 归纳可得

$$\left[\prod_{j=0}^{t-1}(D - j)\right] I \preceq A_t(D) \preceq \left[\prod_{j=0}^{t-1}(D + j)\right] I.$$

取逆并限制到值域 Π_{sym}，得到

$$\frac{t!}{\prod_{j=0}^{t-1}(D + j)} I \preceq M_{H,t} \preceq \frac{t!}{\prod_{j=0}^{t-1}(D - j)} I.$$

将其与（C.3）结合，可得

$$\left[\prod_{j=0}^{t-1}(1 + j/D)^{-1}\right] M_{Z,t} \preceq M_{H,t} \preceq \left[\prod_{j=0}^{t-1}(1 - j/D)^{-1}\right] M_{Z,t}.$$

利用 $\log(1+x) \le x$ 和 $-\log(1-x) \le x/(1-x)$，任一标量因子的绝对对数至多为

$$\sum_{j=0}^{t-1} \frac{j}{D-j} \le \frac{t(t-1)}{2(D-t+1)} \le a_q.$$

因此

$$e^{-a_q} M_{Z,t} \preceq M_{H,t} \preceq e^{a_q} M_{Z,t}. \tag{C.4}$$

零阶矩相同，因此这一比较对每个 $0 \le t \le q$ 都成立。

从矩到协议输出。 在分析中，将初始态和仪器纯化，并保留其测量结果的正交记录。经过至多 q 次正向查询后，每个右矢振幅都是采样矩阵元素的次数至多为 q 的全纯多项式。事实上，每次查询都会应用 $A + B_0 X C_0^\dagger$，其元素是 X 的仿射函数，而所有已知操作的系数都与 X 无关。自适应性会根据记录的历史改变这些系数，但不会引入 X 的共轭元素。</output>

因此，所得向量可以写为

$$|\Phi(X)\rangle = \sum_{t=0}^{q} L_t |X\rangle\!\rangle^{\otimes t}$$

其中线性映射 L_t 是固定的。出现不同次数，是因为一次查询可能贡献固定项 A，也可能贡献关于 X 的线性项。对于 $X = H$ 和 $X = Z$，在 $X \mapsto e^{i\theta} X$ 下的不变性意味着

$$\mathbb{E}\big[|X\rangle\!\rangle^{\otimes t} \langle\!\langle X|^{\otimes u}\big] = 0 \qquad (t \ne u).$$

因此

$$\mathbb{E}|\Phi(X)\rangle\langle\Phi(X)| = \sum_{t=0}^{q} L_t M_{X,t} L_t^\dagger.$$

将（C.4）应用于每一项，即可证明所需的平均纯化态正序比较。偏迹、对历史记录进行退相干以及最终读出都会保持正序，因此

$$e^{-a_q} \rho_Z \preceq \rho_H \preceq e^{a_q} \rho_Z.$$

最后，$\mathrm{Tr}\ \rho_H = 1$ 和下界推出 $\mathrm{Tr}\ \rho_Z \le e^{a_q}$。两个序界还给出

$$-(e^{a_q} - 1)\rho_Z \preceq \rho_H - \rho_Z \preceq (e^{a_q} - 1)\rho_Z.$$

对于厄米 Y和正的 X，不等式 $-X \preceq Y \preceq X$ 推出 $\|Y\|_1 \le \mathrm{Tr}\, X$。应用这一事实即可证明（C.2）中的迹范数界。 □

现在，我们将引理应用于（A.4）中的补全。由于 $q \ge 1$ 且 $\Delta \le c_0$，

$$p \le 2(r+1) \le 2c_0^2 d, \qquad q^2 \le c_0 \sqrt{d}.$$

当 c_0足够小时，这些不等式给出 $D = d - p \ge d/2$ 和 $q \le D/2$，因此 $a_q = O(q^2/d)$。对标架 F进行条件化，应用引理 S6，然后对 F取平均值。补基可以依赖于 F和 ϑ，因为该引理对每一种固定选择都一致适用。由此得到的迹范数误差为 $O(q^2/d)$。

2. 高斯补全记录

现在，我们使用 c 记录来表示高斯补全。为了使记录坐标独立于标架，首先通过定义在整个物理空间上的高斯矩阵来表示补全。

令 Γ 为一个元素相互独立的 $d \times d$ 矩阵 $\mathcal{N}_{\mathbb{C}}(0,\ 1/D)$，且与 F相互独立。将植入的输入和输出投影定义为

$$P_{\mathrm{in},F} = V_F V_F^\dagger, \qquad P_{\mathrm{out},F,\vartheta} = W_{F,\vartheta} W_{F,\vartheta}^\dagger.$$

对于固定的 F，高斯酉不变性意味着 $B^{\dagger}_{F,\vartheta}\Gamma C_F$ 与 $D\times D$ 高斯矩阵 Z 具有相同的分布。因此，在给定 F 的条件下，

$$B_{F,\vartheta}ZC_F^{\dagger}\overset{\text{law}}{=}(I-P_{\text{out},F,\vartheta})\Gamma(I-P_{\text{in},F}).$$

因此，一个与标架无关的单一全空间矩阵 Γ，即可表示每种固定的 F 选择所对应的高斯补全。其元素方差为 $1/D$。

对于标量 $g\sim\mathcal{N}_{\mathbb{C}}(0,\ 1/D)$,

$$\mathbb{E}[\overline{g}^{m}g^{n}]=\delta_{mn}\frac{n!}{D^{n}}.$$

因此，线性映射

$$g^{n}\longmapsto D^{-n/2}(c^{\dagger})^{n}|\Omega\rangle=\sqrt{\frac{n!}{D^{n}}}|n\rangle \tag{C.5}$$

保持全纯多项式的 L^2 内积。为每个元素 Γ_{yx} 指定一个模式 c_{xy}，即可得到相应的多元映射:

$$\prod_{x,y}\Gamma_{yx}^{n_{xy}}\longmapsto D^{-\frac{1}{2}\sum_{x,y}n_{xy}}\prod_{x,y}(c_{xy}^{\dagger})^{n_{xy}}|\Omega\rangle.$$

在此映射下，乘以 Γ_{yx} 变为 $c_{xy}^{\dagger}/\sqrt{D}$。因此，对系统向量应用 Γ，可由补全记录器表示

$$\mathsf{C}=\frac{1}{\sqrt{D}}\sum_{x,y=1}^{d}|y\rangle\langle x|\otimes c_{xy}^{\dagger}, \tag{C.6}$$

如（B.15）中所定义。

设 T_c d 表示上述多项式到记录的映射。对于具有全纯振幅的向量 ，

$$|v(\Gamma)\rangle=\sum_{i}f_i(\Gamma)|i\rangle,\qquad|\widehat{v}\rangle=\sum_{i}|i\rangle\otimes T_cf_i,$$

内积保持性给出

$$\mathrm{Tr}_c|\widehat{v}\rangle\langle\widehat{v}|=\sum_{i,j}\mathbb{E}_{\Gamma}[f_i(\Gamma)\overline{f_j(\Gamma)}]|i\rangle\langle j|=\mathbb{E}_{\Gamma}|v(\Gamma)\rangle\langle v(\Gamma)|. \tag{C.7}$$

因此，对记录取迹即可还原整个平均矩阵，包括其非对角元素。在整个协议中使用相同的模式，可以保留重复使用同一个高斯矩阵所产生的相关性。

对于每个固定的实数i 因此，对于 F 的每一种实现，高斯补全预言机都有精确的记录表示 on

$$\mathcal{U}_{F,\vartheta}=W_{F,\vartheta}V_F^{\dagger}+(I-W_{F,\vartheta}W_{F,\vartheta}^{\dagger})\mathsf{C}(I-V_FV_F^{\dagger}). \tag{C.8}$$

除 C 之外的所有因子仅作用于物理系统，与记录恒等算子的张量积是隐含的。我们还需要给出此查询的范数上界。根据引理 S3,

$$\|\mathsf{C}\Pi_{n_c\le q}\|\le c_q:=\sqrt{\frac{d+q}{D}}. \tag{C.9}$$

植入项是一个部分等距算子，而（C.8）中的两项具有正交输入支集和正交输出值域。由于 $c_q\ge1$，因此可得

$$\|\mathcal{U}_{F,\vartheta}\Pi_{n_c\le q}\|\le c_q. \tag{C.10}$$

3. 将 Haar 标架耦合到高斯标架

接下来，我们用高斯矩阵替换隐藏Haar标架，同时保留由 c记录表示的补全。我们通过极分解归一化将每个Haar标架与一个高斯矩阵耦合起来，从而可以直接界定它们之间的差异。

在每个 扇区 $\sigma \in \{+,-\}$ 中，独立抽取 G_σ： $\mathcal{L}_\sigma \to \mathcal{H}_\sigma$，其元素服从 $\mathcal{N}_{\mathbb{C}}(0,\ 1/N)$，并且 t

$$\begin{aligned} F_\sigma &= G_\sigma (G_\sigma^\dagger G_\sigma)^{-1/2}, \\ \delta_\sigma &= \|F_\sigma - G_\sigma\| = \|(G_\sigma^\dagger G_\sigma)^{1/2} - I\|. \end{aligned} \tag{C.11}$$

由于 $r \le N$，每个 G_σ 几乎必然都是满列秩的，而 F_σ 是等距映射。极分解归一化与酉算子的左乘可交换：

$$(QG_\sigma)\big((QG_\sigma)^\dagger (QG_\sigma)\big)^{-1/2} = QF_\sigma, \qquad Q \in \mathrm{U}(N).$$

G_σ 的左酉不变性因此意味着， F_σ 在 $\mathcal{H}_\sigma$ 中的 r-标架上服从 Haar 分布。记

$$G = G_+ \oplus G_-, \qquad F = F_+ \oplus F_-, \qquad \delta = \max_{\sigma=\pm} \delta_\sigma = \|F - G\|.$$

在重复查询过程中，替换误差会伴有形如 $e^{Cq\delta}$ 的因子。下一个引理同时控制 δ 的尾部，以及对这些误差取平均值所需的加权矩。

引理 S7 （框架耦合 尾部与加权矩）。 存在通用常数 c、C、$C_0 > 0$，使得 t

$$\Pr(\delta > u) \le C\exp(Cr - cNu^2), \qquad u \ge 0, \tag{C.12}$$

$$\Pr\big(\delta > C_0\sqrt{r/N} + t\big) \le Ce^{-cNt^2}, \qquad t \ge 0. \tag{C.13}$$

此外，对于每个 $h \ge 0$,

$$\mathbb{E}[\delta^2 e^{h\delta}] \le C\frac{r+1}{N}\exp\left(Ch\sqrt{\frac{r+1}{N}} + C\frac{h^2}{N}\right). \tag{C.14}$$

证明。 首先，考虑一个扇区，并省略扇区指标。对于固定的单位向量 $v \in \mathbb{C}^r$， $N\|Gv\|^2$ 是 N 个均值为 1 的独立指数随机变量之和。对于其中任意一个随机变量 X,

$$\mathbb{E}e^{\lambda(X-1)} = \frac{e^{-\lambda}}{1-\lambda}, \qquad \lambda < 1,$$

且当 $|\lambda| \le 1/2$ 时，该表达式的对数至多为 $C\lambda^2$。因此，Chernoff 界给出

$$\Pr\big(|\|Gv\|^2 - 1| > x\big) \le 2e^{-cN\min\{x^2,x\}}, \qquad x \ge 0.$$

取复单位球面上的一个 $1/4$-网，其在 $\mathbb{C}^r$ 中的基数至多为 9^{2r}。对于任意厄米矩阵 A，利用该网进行近似可得

$$\|A\| \le 2 \max_{v \text{ in the net}} |v^\dagger A v|.$$

将此应用于 $G^\dagger G - I$ 并取并集界可得

$$\Pr\big(\|G^\dagger G - I\| > x\big) \le 2\exp\big(Cr - cN\min\{x^2, x\}\big).$$

耦合误差是 G 的某个奇异值偏离 1 的最大程度。如果 $0 < u \le 1$ 且 $|s-1| > u$ 对于奇异值 s，则 $|s^2 - 1| > u$。如果 $u \ge 1$，则只可能向上偏离，且 $s^2 - 1 > u^2$。这些观察结果给出了一个扇区的（C.12）。对两个扇区取并集界，可得到 δ的相同界，但常数有所调整。代入 $u = C_0\sqrt{r/N} + t$ 并选择 C_0 充分大，即可证明（C.13）。

对于加权矩，设

$$a = C_0\sqrt{r/N}, \qquad T = (\delta - a)_+.$$

移位尾界和尾部积分意味着

$$\mathbb{E}T^4 \le \frac{C}{N^2}, \qquad \mathbb{E}e^{hT} = 1 + h\int_0^\infty e^{ht}\Pr(T>t)\,dt \le Ce^{Ch^2/N}.$$

最后一个不等式可通过对 $ht - cNt^2$ 配方得到。由柯西–施瓦茨不等式，

$$\mathbb{E}[T^2 e^{hT}] \le (\mathbb{E}T^4)^{1/2}(\mathbb{E}e^{2hT})^{1/2} \le \frac{C}{N}e^{Ch^2/N}.$$

由于 $\delta \le a + T$，

$$\begin{aligned}\mathbb{E}[\delta^2 e^{h\delta}] &\le 2e^{ha}\left(a^2\mathbb{E}e^{hT} + \mathbb{E}[T^2e^{hT}]\right)\\ &\le C\left(a^2 + \frac{1}{N}\right)e^{ha+Ch^2/N}.\end{aligned}$$

代入 a的值即可证明（C.14）。 □

现在我们来界定单次记录查询所引起的变化。定义 V_G，$W_{G,\,\vartheta}$，其列公式与 V_F，$W_{F,\,\vartheta}$ 相同，只需将每个 F_σ 替换为 G_σ，并保持根列不变。固定标签空间嵌入是压缩映射，因此

$$\|V_G - V_F\| + \|W_{G,\vartheta} - W_{F,\vartheta}\| \le 2\delta. \tag{C.15}$$

按照相同的有序表达式定义高斯框架记录查询：

$$\widetilde{\mathcal{U}}_{G,\vartheta} = W_{G,\vartheta}V_G^\dagger + (I - W_{G,\vartheta}W_{G,\vartheta}^\dagger)\mathsf{C}(I - V_GV_G^\dagger). \tag{C.16}$$

波浪号表示高斯列映射尚未归一化为等距映射。特别是，C 周围的因子不一定是正交投影。

利用（C.15），可得

$$\|V_G\|, \|W_{G,\vartheta}\| \le 1 + \delta.$$

逐个因子相减两个查询表达式，并利用（C.9），可得

$$\|(\widetilde{\mathcal{U}}_{G,\vartheta} - \mathcal{U}_{F,\vartheta})\Pi_{n_c\le q}\| \le Cc_q\delta(1+\delta)^3. \tag{C.17}$$

例如，省略 ϑ 后，

$$W_GW_G^\dagger - W_FW_F^\dagger = (W_G - W_F)W_G^\dagger + W_F(W_G - W_F)^\dagger.$$

补全项通过分别相减其左因子和右因子来处理。每个差异贡献一个数量级为 δ 的因子，而其余因子的乘积至多为 $(1+\delta)^3$,，因为一次查询至多包含四个框架因子。所有这些系统矩阵都保持完备占据数，因此整个过程中都适用 C 的受限范数界。特别地，当 $\delta \le 1$ 时，

$$\|(\widetilde{\mathcal{U}}_{G,\vartheta} - \mathcal{U}_{F,\vartheta})\Pi_{n_c\le q}\| \le Cc_q\delta, \qquad \|\widetilde{\mathcal{U}}_{G,\vartheta}\Pi_{n_c\le q}\| \le c_q(1 + C\delta).$$

4. 累积并平均框架误差

现在，我们将单次查询误差累积到自适应协议中，并对耦合取平均（F，G）。已知仪器不会放大向量误差：完备仪器定义了一个等距列映射，

$$|v\rangle \longmapsto \bigoplus_z (K_z \otimes I)|v\rangle, \qquad \sum_z \|(K_z\otimes I)v\|^2 = \|v\|^2.$$

C根据正交历史标记选择这些仪器，也能得到一个等距映射 .

每次查询至多添加一个 c 粒子，而已知操作保持完备占据数不变。因此，在涉及至多 q 次查询的比较中，每个中间向量都属于定义域 $n_c \le q$。

全局界（C.17）和（C.10）意味着，对每个 $\delta \geq 0$,

$$\|(\widetilde{\mathcal{U}}_{G,\vartheta} - \mathcal{U}_{F,\vartheta})\Pi_{n_c \leq q}\| \leq C c_q \delta e^{C\delta},$$
$$\|\widetilde{\mathcal{U}}_{G,\vartheta}\Pi_{n_c \leq q}\| \leq c_q e^{C\delta}.$$

这里，我们对适当的普适常数 C' 使用了 $(1+\delta)^3 \leq e^{3\delta}$ 和 $1 + C\delta(1+\delta)^3 \leq e^{C'\delta}$。对于两个映射序列，望远镜恒等式

$$B_q \cdots B_1 - A_q \cdots A_1 = \sum_{t=1}^{q} B_q \cdots B_{t+1}(B_t - A_t)A_{t-1} \cdots A_1$$

将总差异表示为单次查询差异之和。将其应用于两个记录演化，包括它们共同的等距仪器。对于每个耦合对 $(F,\ G)$，可得

$$\|\widetilde{\Phi}_G - \Phi_F\| \leq C q\, c_q^q\, \delta e^{Cq\delta},$$

其中，Φ_F 和 Φ_G 是最终联合向量，包括补全记录和历史标记。不假设任一向量已归一化。由于 $D = d - p \geq d/2$,

$$c_q^q = \left(1 + \frac{p+q}{D}\right)^{q/2} \leq \exp\left(C\frac{q(p+q)}{d}\right).$$

因此，

$$\|\widetilde{\Phi}_G - \Phi_F\| \leq Cq\delta \exp\left(Cq\delta + C\frac{q(p+q)}{d}\right). \tag{C.18}$$

接下来使用引理 S7对该界取平均值。假设 $1 \leq r \leq N = d/2 - 1$ 给出 $N \geq d/4$。结合$p \leq 2(r+1)$，可得

$$\frac{q(p+q)}{d} \leq C\Delta, \qquad q\sqrt{\frac{r+1}{N}} \leq C\Delta, \qquad \frac{q^2}{N} \leq C\Delta. \tag{C.19}$$

对于第一个不等式，使用 $(r+1)/d \leq \sqrt{(r+1)/d}$。将 (C.18) 平方，并将 C.14与 $h = Cq$ 结合，可得

$$\begin{aligned}\mathbb{E}\|\widetilde{\Phi}_G - \Phi_F\|^2 &\leq Cq^2 \exp\left(C\frac{q(p+q)}{d}\right)\mathbb{E}[\delta^2 e^{Cq\delta}] \\ &\leq C\frac{q^2(r+1)}{N}\exp\left(C\frac{q(p+q)}{d} + Cq\sqrt{\frac{r+1}{N}} + C\frac{q^2}{N}\right).\end{aligned}$$

By (C.19) 和 $\Delta \leq c_0$，指数因子由一个普适常数界定。因此

$$\mathbb{E}\|\widetilde{\Phi}_G - \Phi_F\|^2 \leq C\frac{q^2(r+1)}{d}. \tag{C.20}$$

要将此向量估计转换为输出估计，请使用

$$|x\rangle\langle x| - |y\rangle\langle y| = |x-y\rangle\langle x| + |y\rangle\langle x-y|.$$

秩一算子的迹范数给出

$$\||x\rangle\langle x| - |y\rangle\langle y|\|_1 \leq (\|x\| + \|y\|)\|x - y\|. \tag{C.21}$$

Haar 标架记录向量满足 $\|\Phi_F\| \leq c_q^q = O(1)$。此外，

$$\mathbb{E}\|\widetilde{\Phi}_G\|^2 \leq 2\mathbb{E}\|\Phi_F\|^2 + 2\mathbb{E}\|\widetilde{\Phi}_G - \Phi_F\|^2 = O(1),$$

因为 $q^2\ (r+1)\ /d \leq \Delta^2$。应用 C.21 式和柯西–施瓦茨不等式可得

$$\mathbb{E}\||\widetilde{\Phi}_G\rangle\langle\widetilde{\Phi}_G| - |\Phi_F\rangle\langle\Phi_F|\|_1 \leq Cq\sqrt{\frac{r+1}{d}}.$$

因此，用高斯矩阵替换 Haar 标架后，平均输出的变化至多为

$$Cq\sqrt{\frac{r+1}{d}} \tag{C.22}$$

在迹范数下。将此估计与 Haar完备化比较相结合，真实输出与全高斯多项式模型的平均输出之间的迹范数距离至多为

$$C\left(\frac{q^2}{d}+q\sqrt{\frac{r+1}{d}}\right). \tag{C.23}$$

5. 复高斯框架场

完备化变量在右矢振幅中仅以全纯形式出现。框架变量也通过其共轭变量出现，因为 (C.16) 同时包含 G 和 $G^\dagger$。因此，我们需要一种记录表示，能够保留关于这两类变量的多项式的内积。

对于每个坐标 $g_\mu \sim \mathcal{N}_{\mathbb{C}}(0,\ 1/N)$，在两个框架记录族中使用对应的模式 a_μ，b_μ，并定义

$$M_\mu = \frac{a_\mu^\dagger + b_\mu}{\sqrt{N}}, \qquad M_\mu^\dagger = \frac{a_\mu + b_\mu^\dagger}{\sqrt{N}}. \tag{C.24}$$

这些场及其伴随算子在有限粒子向量上彼此对易：

$$[M_\mu, M_\nu^\dagger] = \frac{-\delta_{\mu\nu}+\delta_{\mu\nu}}{N} = 0, \qquad [M_\mu, M_\nu] = 0.$$

对于单个坐标，

$$M^n|\Omega\rangle = N^{-n/2}(a^\dagger)^n|\Omega\rangle,$$

因此

$$\langle\Omega|(M^\dagger)^m M^n|\Omega\rangle = \delta_{mn}\frac{n!}{N^n} = \mathbb{E}[\overline{g}^m g^n]. \tag{C.25}$$

交换性使每个多项式矩都能写成这种形式，而不同坐标的矩可以因式分解。因此，线性映射

$$T_{ab}f := f(M, M^\dagger)|\Omega\rangle \qquad \text{satisfies} \qquad \langle T_{ab}f \mid T_{ab}h\rangle = \mathbb{E}_G[\overline{f(G,\overline{G})}\, h(G,\overline{G})] \tag{C.26}$$

对于框架坐标及其共轭变量中的任意多项式 f，h。

产生项记录坐标或其共轭变量出现的位置，而湮灭项则再现它们的高斯缩并。例如，

$$T_{ab}(g\overline{g}) = MM^\dagger|\Omega\rangle = \frac{|\Omega\rangle + a^\dagger b^\dagger|\Omega\rangle}{N}.$$

由 M 的湮灭部分产生的真空项，再现 $\mathbb{E}[gg] = 1/N$。

现在，我们将此替换应用于高斯框架记录查询。将各个场组装成一个算子值矩阵 M，其扇区和指标结构与 G相同。通过在定义 V_M、$W_{M,\vartheta}$和 $\widetilde{U}_{M,\vartheta}$的有序表达式以及（C.16）中，将 G替换为 M，并将 $G^\dagger$替换为 $M^\dagger$来定义这些量。每次出现给定坐标时都使用同一个场，包括在 $I - W_G W_G^\dagger$和 $I - V_G V_G^\dagger$中的出现。

将 T_{ab} 应用于 $\widetilde{\Phi}_G$的每个振幅，并将系统、历史标记和 c 条记录视为系数空间。如果 $\widetilde{\Phi}_M$表示所得的联合向量，那么（C.26）给出

$$\mathrm{Tr}_{ab}|\widetilde{\Phi}_M\rangle\langle\widetilde{\Phi}_M| = \mathbb{E}_G|\widetilde{\Phi}_G\rangle\langle\widetilde{\Phi}_G|.$$

因此，框架场表示能够精确复现高斯平均值，且不会引入近似误差。所有高斯随机性现在都由三个记录族 a、b、c 表示。

6. 用非等距编码器替代高斯场

最终的近似将高斯框架场替换为等距编码器 E。我们首先在记录占据数有界的状态上界定它们之间的差异，然后将这一替换应用于有序查询表达式。在一个物理扇区中，记为

$$M = E_0 + B, \qquad E_0 = \frac{1}{\sqrt{N}} \sum_{i,\alpha} |i\rangle\langle\alpha| \otimes a_{i\alpha}^\dagger, \qquad B = \frac{1}{\sqrt{N}} \sum_{i,\alpha} |i\rangle\langle\alpha| \otimes b_{i\alpha}. \tag{C.27}$$

这些算子将标签寄存器和记录映射到物理寄存器和记录。产生部分 E_0 是引理 S1 中研究的未归一化编码器，而 B 会湮灭一个 b粒子。

令 $\Pi_{\le R}^{\mathrm{rec}}$ 表示总记录占据数不超过 R 的投影算子。我们使用以下界

$$\begin{aligned} \|(E_0^\dagger E_0 - I)\Pi_{\le R}^{\mathrm{rec}}\| &\le \frac{R}{N}, \\ \max\left\{\|B\Pi_{\le R}^{\mathrm{rec}}\|, \|B^\dagger \Pi_{\le R}^{\mathrm{rec}}\|\right\} &\le \sqrt{\frac{r+R}{N}}. \end{aligned} \tag{C.28}$$

The 前者由式（B.11）直接推出。对于后者，在 n_b粒子扇区上进行正规序可得 es

$$BB^\dagger = \frac{1}{N}\left(rI + \sum_{\ell=1}^{n_b} \mathsf{Swap}_{\mathrm{physical},\ell}\right).$$

这里 $\mathsf{Swap}_{\mathrm{physical},\ \ell}$ 将物理寄存器与第 ℓ 个 b粒子的物理坐标互换，同时保持其列标签不变。该求和保持对称子空间，且其范数至多为 n_b。因此，$B^\dagger$ 作用于 n_b 个输入粒子时，其范数至多为 $\sqrt{\ }\left(r+n_b\right)/N$。在相邻粒子扇区之间取伴随算子，可得 B 作用于 $n_b \ge 1$ 个粒子时的范数上界为$\sqrt{\ }\left(r+n_b-1\right)/N$，而 B 在真空态上为零。这就证明了第二个估计，并说明了 r这一项的由来。现在使用引理 S1中的全局等距编码器，

$$E = E_0(E_0^\dagger E_0)^{-1/2}.$$

逆平方根分别在每个固定的 a 粒子扇区上定义，在该扇区中， E_0 对于 $r \le N$是单射。由此得到的极分解因子共同定义了一个全局等距映射，使 n_a 增加一，同时保持其他占据数不变。对于 $R \le N/2$，引理 S1 给出

$$\|(E - E_0)\Pi_{\le R}^{\mathrm{rec}}\| \le C\frac{R}{N}.$$

在相邻的 a 粒子扇区之间取伴随映射，即可得到相应的伴随估计：对于满足$n_a \ge 1$的输入，它使用编码器在 $n_a - 1$ 处的界；而这两个伴随映射作用于 a 真空态输入时均为零。因此

$$\|(E^\dagger - E_0^\dagger)\Pi_{\le R}^{\mathrm{rec}}\| \le C\frac{R}{N}.$$

将这些估计与（C.28）结合，得到

$$\begin{aligned} \max\left\{\|(M-E)\Pi_{\le R}^{\mathrm{rec}}\|, \|(M^\dagger - E^\dagger)\Pi_{\le R}^{\mathrm{rec}}\|\right\} &\le \eta_R, \\ \eta_R &:= C\left(\sqrt{\frac{r+R}{N}} + \frac{R}{N}\right). \end{aligned} \tag{C.29}$$

对两个物理扇区取正交直和，可得完整框架场和编码器满足相同的界。

随后，我们在查询表达式中用 M替换 E，并用 $M^\dagger$替换 $E^\dagger$。利用在（B.21）中定义的列映射 V_E， $W_{E,\ \vartheta}$，得到

$$\mathcal{U}_{E,\vartheta} = W_{E,\vartheta}V_E^\dagger + (I - W_{E,\vartheta}W_{E,\vartheta}^\dagger)\mathsf{C}(I - V_E V_E^\dagger). \tag{C.30}$$

这正是附录B中构造的记录预言机。

7. 有限粒子域与累积误差

高斯场在整个福克空间上是无界的。因此，为了应用前述范数估计，我们跟踪每个中间向量的记录占据数。

每个场 M 或 $M^\dagger$ 最多使总占据数改变一个。植入项$\widetilde{\mathcal{U}}_{M,\,\vartheta}$ 至多包含两个框架因子，而补全项至多包含四个框架因子和一个 c-创建算子。因此，原始查询最多使总占据数增加五。根据引理S5，使用等距编码器的查询最多使总占据数增加一。已知的系统仪器保持所有记录占据数不变。

从真空态出发，任何至多包含 q 次查询的序列（每次查询均可选择为原始查询或归一化查询），因此总占据数最多可达 $5q$。展开单次查询并逐个替换其因子，最多会进一步增加五次占据数。因此，共同上界

$$R_* = 5q + 5 \tag{C.31}$$

涵盖比较中使用的所有中间向量，包括伴随因子的输入。对于充分小的 c_0，条件 $\Delta \le c_0$ 保证 $R_* \le N/2$，正如（C.29）所要求的。

所有截断都限制输入在截断之外以及玻色仅范数估计的部分。我们保持算符乘积不变，保留产生算符子对易关系。

现在，我们可以逐一替换两个查询的框架因子，从而进行比较。固定的标签空间映射是压缩映射；根据 (C.28) 和 $E^\dagger E = I$，所有框架因子在中间定义域上的范数都有界。每次替换至多产生 η_{R_*}的误差，而补全记录器至多产生 c_q的误差。因此，对于每个参与比较的可达输入 v，

$$\begin{aligned} \|(\widetilde{\mathcal{U}}_{M,\vartheta} - \mathcal{U}_{E,\vartheta})v\| &\le C c_q \eta_{R_*} \|v\|, \\ \|\widetilde{\mathcal{U}}_{M,\vartheta} v\| &\le c_q(1 + C\eta_{R_*})\|v\|. \end{aligned} \tag{C.32}$$

第二个不等式由第一个不等式和引理 S5推出。

Let $\widetilde{\Phi}_M$ 以及 Φ_E 分别表示原始场演化过程和等距编码器演化过程的最终联合向量，其中包含所有记录和历史标记。附录 C4 中的望远镜求和论证给出

$$\|\widetilde{\Phi}_M - \Phi_E\| \le C q \eta_{R_*} \exp\left(C q \eta_{R_*} + C \frac{q(p+q)}{d} \right).$$

由于 $R_* = 5q + 5$ 和 $N = \Theta(d)$，

$$q\eta_{R_*} \le C\left(q\sqrt{\frac{r+q}{d}} + \frac{q(q+1)}{d} \right) \le C\Delta. \tag{C.33}$$

最后一个不等式用到了 $q \ge 1$。结合（C.19），可知指数因子被一个普适常数所界定。同样的乘积估计表明，两个最终向量的范数都被普适常数所界定。应用（C.21），再经过共同的输出通道，可得迹范数误差至多为 $C\Delta$。

命题*S1*的证明。两个高斯到记录的表示都是精确的。结合 Haar 到高斯界（C.23）与刚刚证明的场到编码器比较，由三角不等式可得

$$\|\rho_{\mathrm{true},\vartheta} - \rho_{E,\vartheta}\|_1 \le C\left(\frac{q^2}{d} + q\sqrt{\frac{r+1}{d}} + \Delta \right) \le C'\Delta.$$

□

附录 D：从记录模型到理想过程

本附录比较记录模型中任意最终事件的权重与其在理想过程中的概率。我们首先将理想测量效应表示为作用于系统和记录的算子。随后说明，通过记录查询和仪器进行一次反向步骤，大致遵循理想更新规则。最后，我们在自适应协议中累积这一误差，并评估其对初始态产生的影响。结合命题 S1，即可证明定理 S1。

1. 提升理想效应

理想效应将未来事件的概率指定为理想态的一个线性泛函。为了将这一泛函与记录演化进行比较，我们利用根嵌入 J 和隐藏编码器 E，在联合系统–记录空间上表示它。

定义 n S1（提升理想效应）。查询前理想效应是一个三元组 $A = (A_0, A_L, \lambda)$，其 re

$$0 \preceq A_0 \preceq I_2, \qquad 0 \preceq A_L \preceq I_{\mathcal{L}}, \qquad 0 \le \lambda \le 1,$$

且 A_L 在各层上是分块对角的。其提升为

$$\iota(A) = \lambda I + J(A_0 - \lambda I_2)J^\dagger + E(A_L - \lambda I_{\mathcal{L}})E^\dagger. \tag{D.1}$$

与记录恒等算子的张量积为隐含内容。对于查询后效应 (A_L, λ)，省略 J 项。

由于 J 和 E 是值域正交的等距映射，因此 $\iota(A)$在根上作用为 A_0，在编码后的隐藏空间上作用为 A_L，在它们的正交补上作用为 λI。因此 $0 \preceq \iota(A) \preceq I$。提升也保持总记录占据数不变。我们使用理想映射的伴随算子向后传播效应。对于查询，

$$\mathrm{Tr}[B\mathcal{Q}_\vartheta(\omega)] = \mathrm{Tr}[\mathcal{Q}^*_\vartheta(B)\omega].$$

对于一个仪器，未来效应可能取决于其测量结果，因此

$$\mathrm{Tr}[\Phi^*_K(\{A_z\})\omega] = \sum_z \mathrm{Tr}[A_z \Phi_{K,z}(\omega)].$$

这些配对表示层迹之和与剩余标量乘积。由于查询不会留下根块，仪器回拉 $\Phi^*_K(\{A_z\})$ 是作用于隐藏输入和剩余输入的一对 $(H,\ g)$。将这对量通过前一个查询回拉，便得到一个查询前三元组。

2. 一次反向步骤

在本附录中，固定 ϑ，并在以下参数范围内工作：

$$\Delta = \Delta(q, r, d) \le c, \qquad q \ge 1, \qquad R = 5q + 5, \tag{D.2}$$

其中 c 是一个足够小的普适常数。正如附录 C中所证明的，这确保了 $D \ge d/2$ 和 $R \le N/2$。接下来的引理比较一次记录查询后接一个仪器与相应理想操作的差异。其范数上界仅限制输入记录占据数，并控制误差算子的完整输出。这正是迭代此比较所需的形式。

引理 S8 (一次反向步骤重现理想规则)。设 $\{K_z\}_z$ 是一个满足 $\sum_z K_z^\dagger K_z = I$的物理仪器，并为每个测量结果指定一个查询前理想效应 $A_z = (A_{0,\ z},\ A_{L,\ z},\ \lambda_z)$。在参数范围 (D.2)内，存在一个普适常数 C，使得

$$\left\| \left[\mathcal{U}^\dagger_{E,\vartheta} \left(\sum_z K_z^\dagger \iota(A_z) K_z \right) \mathcal{U}_{E,\vartheta} - \iota(\mathcal{Q}^*_\vartheta \Phi^*_K(\{A_z\})) \right] \Pi^{\mathrm{rec}}_{\le R-4} \right\| \le \zeta_R := C \left(\frac{R}{\sqrt{N}} + \frac{R(R+1)}{N} + \frac{p+R}{D} \right). \tag{D.3}$$

证明。在记录嵌入中抑制 ϑ，并写成

$$V = V_E, \qquad W = W_{E,\vartheta}, \qquad P_V = VV^\dagger, \qquad P_W = WW^\dagger.$$

令 $B_z = A_{L,\ z} - \lambda_z I$，使得 $\|B_z\| \le 1$。仪器回拉分解为

$$\begin{aligned} N_0 &= \sum_z K_z^\dagger \left[\lambda_z I + J(A_{0,z} - \lambda_z I) J^\dagger \right] K_z, \\ N_1 &= \sum_z K_z^\dagger E B_z E^\dagger K_z, \qquad \mathsf{N} = N_0 + N_1 = \sum_z K_z^\dagger \iota(A_z) K_z. \end{aligned} \tag{D.4}$$

N_0 和 N 都是正压缩算子。算子 N_0 仅作用于物理系统，而 N_1 也作用于记录。

Let

$$\mathsf{C}_\perp = (I - P_W)\mathsf{C}(I - P_V).$$

展开记录查询的两项可得

$$\begin{aligned}\mathcal{U}_{E,\vartheta}^\dagger \mathsf{N}\mathcal{U}_{E,\vartheta} = VW^\dagger \mathsf{N}WV^\dagger + \mathsf{C}_\perp^\dagger \mathsf{N}\mathsf{C}_\perp \\ + VW^\dagger \mathsf{N}\mathsf{C}_\perp + \mathsf{C}_\perp^\dagger \mathsf{N}WV^\dagger.\end{aligned}$$

W我们分别估计植入项、补全项和两个交叉项 .

就定义域记账而言， N_0， N_1， P_V， P_W 保持总记录占据数不变。 $E^\dagger K_z E$ 和 $E^\dagger K_z \mathsf{C}$也如此：后者将一个 a粒子换成一个 c粒子。其余编码器和记录创建算子使占据数至多偏移一。 $R-4$ 与 R 之间的间隔足以涵盖下文乘积中的中间偏移。

The 植入项。定义两个仪器列和依赖结果的效应如下

$$X = \mathrm{col}_z(E^\dagger K_z E), \qquad Y = \mathrm{col}_z\, D_z, \qquad \mathcal{B} = \bigoplus_z B_z.$$

根据引理S2,

$$\|X\|, \|Y\|, \|\mathcal{B}\| \le 1, \qquad \|(X-Y)\Pi_{\le R}^{\mathrm{rec}}\| \le C\frac{R}{\sqrt{N}}.$$

由于这些映射保持记录占据数不变,

$$\|(X^\dagger \mathcal{B} X - Y^\dagger \mathcal{B} Y)\Pi_{\le R}^{\mathrm{rec}}\| \le 2\|(X-Y)\Pi_{\le R}^{\mathrm{rec}}\|.$$

将其与 N_0 的压缩估计结合，可得

$$\begin{aligned}E^\dagger \mathsf{N} E &= H + \mathcal{E}_H, \\ H &= T(N_0) + \sum_z D_z^\dagger B_z D_z, \\ \|\mathcal{E}_H \Pi_{\le R}^{\mathrm{rec}}\| &\le C\frac{R}{\sqrt{N}}.\end{aligned} \tag{D.5}$$

使用完备仪器列可以避免为每个测量结果分别引入误差。代入 N_0、 B_z 和 $w_{z\sigma}$ 的定义，可得

$$\begin{aligned}H = &\sum_z D_z^\dagger A_{L,z} D_z \\ &+ \bigoplus_{\sigma=\pm}\left(\sum_z \left[\mathrm{Tr}(A_{0,z}Q_{z\sigma}) + \lambda_z w_{z\sigma}\right]\right) I_{\mathcal{L}_\sigma}.\end{aligned} \tag{D.6}$$

第一项将未来效应与同层输出配对。其余两项则将其分别与根输出和残差输出配对。因此，这恰好就是（A.9）中的隐输入伴随规则。特别地， H 是一个层块对角正压缩算子。

补全项。先考虑 $\mathsf{C}^\dagger\mathsf{N}\mathsf{C}$，此时尚未插入输出投影 $I - P_W$。对于仅系统部分，（B.18）给出

$$\left\|\left(\mathsf{C}^\dagger N_0 \mathsf{C} - \frac{\mathrm{Tr}\, N_0}{D} I\right)\Pi_{\le R}^{\mathrm{rec}}\right\| \le \frac{R}{D}.$$

对于编码部分，令

$$Z = \mathrm{col}_z(E^\dagger K_z \mathsf{C}).$$

那么 $\mathsf{C}^\dagger N_1 \mathsf{C} = Z^\dagger \mathcal{B} Z$。引理 S4 中的列返回估计因此给出

$$\|\mathsf{C}^\dagger N_1 \mathsf{C}\Pi_{\le R}^{\mathrm{rec}}\| \le \|Z\Pi_{\le R}^{\mathrm{rec}}\|^2 \le C\frac{R(R+1)}{N}. \tag{D.7}$$

定义

$$g = \frac{\operatorname{Tr} N_0}{d}.$$

由于 $0 \preceq N_0 \preceq I$ 和 $d - D = p$,

$$\left| \frac{\operatorname{Tr} N_0}{D} - g \right| \leq \frac{p}{D}.$$

展开 N_0 可得

$$g = \sum_z \left[\operatorname{Tr}\left(A_{0,z} \frac{J^\dagger K_z K_z^\dagger J}{d} \right) + \lambda_z \frac{\operatorname{Tr}(K_z^\dagger K_z) - \operatorname{Tr}(J^\dagger K_z K_z^\dagger J)}{d} \right]. \tag{D.8}$$

这些恰好是（A.10）中的根项和残差贡献。因此,

$$(H, g) = \Phi_K^*(\{A_z\}).$$

接下来恢复输出投影。由于 值域 $W \subseteq$ 值域 E，引理 S4 给出

$$\|P_W \mathsf{C}\Pi_{\leq R}^{\mathrm{rec}}\| \leq \|E^\dagger \mathsf{C}\Pi_{\leq R}^{\mathrm{rec}}\| \leq C\sqrt{\frac{R(R+1)}{ND}}.$$

此外,

$$\|\mathsf{C}\Pi_{\leq R}^{\mathrm{rec}}\| \leq \sqrt{\frac{d+R}{D}} = O(1).$$

由于 N 且 $I - P_W$是压缩算子，将 $\mathsf{C}^\dagger\mathsf{N}\mathsf{C}$ 替换为 $\mathsf{C}^\dagger(I - P_W)\mathsf{N}(I - P_W)\mathsf{C}$ 至多会产生 st

$$2\|\mathsf{C}\Pi_{\leq R}^{\mathrm{rec}}\|\|P_W \mathsf{C}\Pi_{\leq R}^{\mathrm{rec}}\|.$$

最后，左右夹以 $I - P_V$ 后，主标量 gI 变为 $g(I - P_V)$。

交叉项。 对于仅系统部分，单算子返回估计给出

$$\|E^\dagger N_0 \mathsf{C}\Pi_{\leq R}^{\mathrm{rec}}\| \leq C\sqrt{\frac{R(R+1)}{ND}}.$$

对于编码部分,

$$E^\dagger N_1 \mathsf{C} = X^\dagger \mathcal{B} Z,$$

so

$$\|E^\dagger N_1 \mathsf{C}\Pi_{\leq R}^{\mathrm{rec}}\| \leq \|Z\Pi_{\leq R}^{\mathrm{rec}}\| \leq C\sqrt{\frac{R(R+1)}{N}}.$$

插入 $I - P_W$ 至多会增加 $\|P_W \mathsf{C}\Pi_{\leq R}^{\mathrm{rec}}\|$。由于 $W = E(S_\vartheta \otimes I_{\mathcal{F}})$ 以及其余外部因子都是压缩算子，这些估计控制了查询展开中的两个交叉项。Id

$entific$与理想查询的比较。 综合前述估计，主算子为

$$V S_\vartheta^\dagger H S_\vartheta V^\dagger + g(I - P_V). \tag{D.9}$$

为识别它，写出 $H = \bigoplus_{j=1}^{\ell} H_j$ 并定义

$$\Theta_j = S_{\vartheta,j}^\dagger H_{j+1} S_{\vartheta,j} \qquad (0 \leq j < \ell),$$

$$\Theta_\ell = 0, \qquad \Theta_L = \bigoplus_{j=1}^{\ell} \Theta_j, \qquad \Gamma_L = \bigoplus_{j=1}^{\ell} \Gamma_j.$$

每个 Θ_j 都支撑在 值域Γ_j上。此外，不同的输入层对应不同的后继层，而 H 在这些层之间没有矩阵元。因此，列公式（B.21）给出

$$P_V = JJ^\dagger + E\Gamma_L E^\dagger, \qquad VS_\vartheta^\dagger H S_\vartheta V^\dagger = J\Theta_0 J^\dagger + E\Theta_L E^\dagger.$$

理想查询规则（A.7）给出

$$\mathcal{Q}_\vartheta^*(H,g) = \big(\Theta_0,\, \Theta_L + g(I_\mathcal{L} - \Gamma_L),\, g\big).$$

将这个三元组代入（D.1）恰好得到（D.9）。

总误差有如下界

$$C\left(\frac{R}{\sqrt{N}} + \frac{R(R+1)}{N} + \frac{p+R}{D}\right) = \zeta_R.$$

所有估计都能控制占据数至多为 $R-4$ 的输入上的完整输出，这证明了（D.3）。输出投影估计只用到了 $\operatorname{Ran} W_{E,\,\vartheta} \subseteq \operatorname{Ran} E$，因此允许投影依赖于 ϑ。 □

3. 自适应递归与真空态上的求值

现在，我们将局部比较应用于一个完整的未来事件，沿自适应历史树向后传播其误差，并评估由此得到的效应对初始状态的影响。

定理*S1*的证明。固定一个最终事件。在每个最终经典历史 h处，将最终读出和任何先前的已知操作合并为一个物理效应 $0 \preceq M_h \preceq I$。相应的理想终端效应为

$$\left(T(M_h), \frac{\operatorname{Tr} M_h}{d}\right),$$

如（A.12）中所规定。要将引理S8 应用于终端测量，用二元仪器表示所选事件

$$K_1 = M_h^{1/2}, \qquad K_0 = (I - M_h)^{1/2},$$

其中，测量结果 1 表示事件发生。指定常数理想效应

$$A_1 = (I_2, I_\mathcal{L}, 1), \qquad A_0 = (0,0,0).$$

它们的提升分别为 $\iota(A_1) = I$ 和 $\iota(A_0) = 0$，因此

$$\sum_{z=0}^{1} K_z^\dagger \iota(A_z) K_z = M_h \otimes I_\mathcal{F}.$$

理想仪器规则给出

$$\Phi_K^*(\{A_0, A_1\}) = \left(\bigoplus_{\sigma=\pm} \frac{\operatorname{Tr}(\Pi_\sigma M_h)}{N} I_{\mathcal{L}_\sigma}, \frac{\operatorname{Tr} M_h}{d}\right) = \left(T(M_h), \frac{\operatorname{Tr} M_h}{d}\right).$$

引理S8 因此可直接应用，并得到

$$\left\| \left[\mathcal{U}_{E,\vartheta}^\dagger (M_h \otimes I) \mathcal{U}_{E,\vartheta} - \iota\left(\mathcal{Q}_\vartheta^*\left(T(M_h), \frac{\operatorname{Tr} M_h}{d}\right)\right)\right] \Pi_{\le R-4}^{\mathrm{rec}} \right\| \le \zeta_R.$$

该界限对所选事件和最终历史均匀成立。

未来事件算子。 在一段还剩 t 次查询的历史 h 中，令 $B_{t,h}$ 为记录算子，它与当前状态配对后给出经历剩余演化后所选事件的权重。对于还剩一次查询的情况，

$$B_{1,h} = \mathcal{U}_{E,\vartheta}^\dagger (M_h \otimes I) \mathcal{U}_{E,\vartheta}.$$

对于 $t \geq 2$,

$$B_{t,h} = \mathcal{U}_{E,\vartheta}^{\dagger} \left(\sum_{z} K_{z|h}^{\dagger} B_{t-1,hz} K_{z|h} \right) \mathcal{U}_{E,\vartheta}.$$

这些正算子定义在有限粒子核上。由于记录演化不一定保持迹，它们不一定受恒等算子所界。

令$A_{t,\ h}$ 为相应的理想未来效应:

$$A_{1,h} = \mathcal{Q}_{\vartheta}^{*} \left(T(M_h), \frac{\operatorname{Tr} M_h}{d} \right),$$
$$A_{t,h} = \mathcal{Q}_{\vartheta}^{*} \Phi_{K_{\cdot|h}}^{*} \left(\{A_{t-1,hz}\}_z \right) \qquad (t \geq 2).$$

理想映射保持归一化，因此所有$A_{t,\ h}$ 都是效应。定义一致误差

$$e_t = \sup_h \| (B_{t,h} - \iota(A_{t,h})) \Pi_{\leq q-t}^{\mathrm{rec}} \|.$$

误差的传播。根据引理S5，一次记录查询使总占据数最多增加一，而其伴随算子绝不会使其增加。因此， t查询未来事件算子会将占据数至多为 L 的输入映射为占据数至多为 $L+t$的输出。由于提升的理想效应保持占据数，在 e_t 的定义中出现的每个误差算子，其输出占据数至多为 q。

假设一个节点还剩 $t+1$ 次查询，并令

$$X_z = B_{t,hz} - \iota(A_{t,hz}).$$

传播后的子误差为

$$\mathcal{U}_{E,\vartheta}^{\dagger} \left(\sum_{z} K_{z|h}^{\dagger} X_z K_{z|h} \right) \mathcal{U}_{E,\vartheta}.$$

对于占据数至多为 $q-t-1$ 的输入，右查询产生的占据数至多为 $q-t$。仪器保持占据数不变，其第 $\mathrm{col}_z\, K_{z|h}$ 列是等距映射。因此，分块对角族 $\bigoplus_z X_z$ 的贡献至多为 e_t，且完整输出的支撑集位于占据数至多为 q 的范围内。

左伴随算子查询同样　　在此输出定义域上的范数至多为 c_q 。事实上，其占据数单调性给出

$$\mathcal{U}_{E,\vartheta}^{\dagger} \Pi_{\leq q}^{\mathrm{rec}} = \Pi_{\leq q}^{\mathrm{rec}} \mathcal{U}_{E,\vartheta}^{\dagger} \Pi_{\leq q}^{\mathrm{rec}},$$

从而

$$\| \mathcal{U}_{E,\vartheta}^{\dagger} \Pi_{\leq q}^{\mathrm{rec}} \| = \| \Pi_{\leq q}^{\mathrm{rec}} \mathcal{U}_{E,\vartheta} \Pi_{\leq q}^{\mathrm{rec}} \| \leq c_q.$$

右查询具有相同的界。因此，传播后的子误差至多为 $c_q^2 e_t$。加上引理S8 中的局部误差可得

$$e_1 \leq \zeta_R, \qquad e_{t+1} \leq c_q^2 e_t + \zeta_R. \tag{D.10}$$

根据终端估计，基例成立，因为 $q-1 \leq R-4$。所有后续输入定义域也都处于此截断范围内。

由于

$$c_q^{2q} = \left(1 + \frac{p+q}{D} \right)^q \leq \exp\left(C \frac{q(p+q)}{d} \right) = O(1)$$

由（C.19），对递推式求和可得

$$\begin{aligned} e_q &\leq C q \zeta_R \\ &\leq C \left(\frac{q^2}{\sqrt{d}} + \frac{q^3}{d} + \frac{q(p+q)}{d} \right) \leq C\Delta. \end{aligned} \tag{D.11}$$

这里我们使用了 $R = 5q + 5$、（C.19）以及 $q/\sqrt{d} \le \Delta \le c$。

初始状态评估。记录从真空态开始，且 $E^\dagger$ 会湮灭所有记录处于真空态的输入。因此，对于任意物理初始态 ρ 和理想效应 $A = (A_0,\ A_L,\ \lambda)$，

$$\begin{aligned}\mathrm{Tr}[\iota(A)(\rho \otimes |\Omega\rangle\langle\Omega|)] &= \mathrm{Tr}(A_0 J^\dagger \rho J) + \lambda\big(1 - \mathrm{Tr}(R_0\rho)\big) \\ &= \mathrm{Tr}(A\omega_{\mathrm{in}}).\end{aligned} \tag{D.12}$$

这与（A.6）中的理想初始化完全一致，包括 ρ 在根与其补集之间存在相干性的情况。因此，在该初始态上评估（D.11），可得记录事件权重与理想事件概率之差的上界为 $C\Delta$。对初始经典随机性，可通过对该上界取平均来处理。

最后，命题 S1 将物理事件概率与其记录权重之差限制在另一个$C\Delta$以内。由三角不等式可知，对于所选事件，物理与理想概率之间的误差均匀地具有相同阶数。物理与理想输出分布都已归一化，因此对事件取上确界即可证明（A.14）。 □

附录 E：估计多时间关联函数的无辅助系统下界

我们陈述并证明定理 2 中下界的正式版本，适用于连续时间步$t_j = j - 1$以及单个已知的无迹二值可观测量 $O_j = O$，其中 $C(U) = \langle\psi|(U^k)^\dagger (OU)^k O|\psi\rangle$。

定理 S2（多时间关联函数的仅系统下界，形式化表述）。设 $k \ge 2$，且 $d \ge 4k$ 为偶数。对于每个已知的无迹二值可观测量 O，存在一个已知的单位向量 ψ 和定义在 $\mathrm{U}(d)$ 上的分布 $\mathcal{D}_s$，$s \in \{+1, -1\}$，满足对于 $\mathcal{D}_s$的支撑集上的 $C(U) = s$，任何至多使用 q次正向查询的仅系统协议都满足

$$\mathrm{TV}(\mathsf{Out}_+, \mathsf{Out}_-) \le \min\left\{1,\ q2^{1-k} + C\frac{q^2 + q\sqrt{k}}{\sqrt{d}}\right\}, \tag{E.1}$$

其中，Out_s 是对一次抽样 $U \sim \mathcal{D}_s$取平均后得到的完整经典输出分布，$C > 0$ 是一个普适常数。因此，要以至少 $2/3$ 的成功概率，对这些支撑集中的每个预言机估计 $C(U)$，且加性误差不超过 $1/3$，需要

$$q = \Omega\Big(\min\{2^k, d^{1/4}, \sqrt{d/k}\}\Big). \tag{E.2}$$

特别地，对于 $n \ge 4k$ 个量子比特，任何仅系统协议都需要 $q = \Omega(2^k)$ 次查询。

为证明该定理，我们构造两个随机预言机族，其关联函数值分别为 $+1$ 和 -1，并利用模拟定理，将它们的输出分布与理想过程的输出分布进行比较。在理想过程中，只有通过两条路径之间的相干性才能检测出该符号。我们证明，这种相干性在经过各个内部阶段时会呈指数衰减。将这种压缩映射与混合论证及模拟界结合起来，即可得到所述的查询下界。

1. hardoracle 预言机族

固定 $k \ge 2$ 和一个偶数 $d \ge 4k$。令 O 为定理 S2中的已知二值可观测量。选取已知单位向量 e_σ 满足 $Oe_\sigma = \sigma e_\sigma$ 对于 $\sigma \in \{+1, -1\}$，并令

$$a_0 = \psi = \frac{e_+ + e_-}{\sqrt{2}}, \qquad b_0 = O\psi = \frac{e_+ - e_-}{\sqrt{2}}, \qquad J = (a_0\ \ b_0), \qquad R_0 = JJ^\dagger.$$

向量 a_0、b_0 构成已知根空间的标准正交基。令 $\mathcal{H}_\sigma$ 为 O的 σ-特征空间中 e_σ的正交补，其投影算子为 Π_σ。那么

$$\mathcal{H} = \mathrm{Ran}\, J \oplus \mathcal{H}_+ \oplus \mathcal{H}_-, \qquad \dim \mathcal{H}_\sigma = N = d/2 - 1.$$

设定 $r = 2k - 1 \le N$，并在两个扇区中分别抽取独立的 Haar分布的正交归一 r-框架 F_σ。将每个框架的列标记为

$$A_1, B_1, A_2, B_2, \ldots, A_{k-1}, B_{k-1}, A_k. \tag{E.3}$$

将标记为 A_j 和 B_j 的列分别记为 $x_{j,\sigma}$ 和 $y_{j,\sigma}$，并定义

$$a_j = \frac{x_{j,+} + x_{j,-}}{\sqrt{2}} \quad (1 \le j \le k), \qquad b_j = \frac{y_{j,+} + y_{j,-}}{\sqrt{2}} \quad (1 \le j < k).$$

对于每个内部阶段 $1 \le j < k$，向量 a_j、Oa_j、b_j、Ob_j 均为正交归一向量，端点对 a_k、Oa_k 亦然。它们的张成空间与根空间两两正交。

对于每个符号 $s \in \{+1, -1\}$，规定跃迁

$$\begin{aligned} Ua_{j-1} &= a_j \qquad (1 \le j \le k), \\ Ub_{j-1} &= Ob_j \qquad (1 \le j < k), \\ Ub_{k-1} &= sOa_k. \end{aligned} \tag{E.4}$$

$2k$ 输入向量是正交归一的，其规定的输出也同样如此。令

$$V_F = (a_0, b_0, a_1, b_1, \ldots, a_{k-1}, b_{k-1}),$$

并令 $W_{F,s}$ 包含来自（E.4）的匹配输出列。因此

$$p = 2k, \qquad D = d - 2k \ge d/2. \tag{E.5}$$

利用（A.4）中的补空间嵌入，定义

$$U = W_{F,s} V_F^\dagger + B_{F,s} H C_F^\dagger, \qquad H \sim \mathrm{Haar}(\mathrm{U}(D)), \tag{E.6}$$

其中 H 与标架无关。该构造定义了分布 $\mathcal{D}_s$。

下一个引理证明，要估计目标关联函数，就必须区分这两个预言机族。

L引理 S9（编码关联函数）。支撑集 $\mathcal{D}_s$ 中的每个 U 都满足 $C(U) = s$.

证明。第一个跃迁序列给出 $U^k\psi = a_k$。对于第二个跃迁序列，$O\psi = b_0$ 和

$$OUb_{j-1} = b_j \quad (1 \le j < k), \qquad OUb_{k-1} = sa_k.$$

因此 $(OU)^k O\psi = sa_k$，且 $C(U) = \langle\psi|(U^k)^\dagger (OU)^k O|\psi\rangle = s$。 □

2. 化简为理想过程

现在，我们用附录 A中的记号来表示这一族。取标签层

$$\begin{aligned} \mathcal{L}_j &= \mathrm{span}\{|A_j, +\rangle, |A_j, -\rangle, |B_j, +\rangle, |B_j, -\rangle\} \quad (1 \le j < k), \\ \mathcal{L}_k &= \mathrm{span}\{|A_k, +\rangle, |A_k, -\rangle\}. \end{aligned} \tag{E.7}$$

定义

$$\bar{a}_j = \frac{|A_j, +\rangle + |A_j, -\rangle}{\sqrt{2}} \quad (1 \le j \le k), \qquad \bar{b}_j = \frac{|B_j, +\rangle + |B_j, -\rangle}{\sqrt{2}} \quad (1 \le j < k).$$

令 $\bar{a}_0, \bar{b}_0$ 为经 J 映射到 a_0, b_0 的正交归一根坐标。对于 $0 \le j < k$，选取 $\mathcal{I}_j = \mathbb{C}^2$，并令 V_j 将其基嵌入为 $\bar{a}_j, \bar{b}_j$。相应的输入投影为

$$\Gamma_0 = I, \qquad \Gamma_j = |\bar{a}_j\rangle\langle\bar{a}_j| + |\bar{b}_j\rangle\langle\bar{b}_j| \quad (1 \le j < k), \qquad \Gamma_k = 0.$$

规定的标签空间转移为

$$\begin{aligned} S_{s,j}\bar{a}_j &= \bar{a}_{j+1} \qquad (0 \le j < k), \\ S_{s,j}\bar{b}_j &= Z_{\mathcal{L}}\bar{b}_{j+1} \quad (0 \le j < k-1), \\ S_{s,k-1}\bar{b}_{k-1} &= sZ_{\mathcal{L}}\bar{a}_k. \end{aligned} \tag{E.8}$$

每个映射在其规定输入子空间的正交补上均为零，因此 $S_{s,j}^\dagger S_{s,j} = \Gamma_j$。此外，$Z_{\mathcal{L}}\mathcal{L}_j \subseteq \mathcal{L}_j$，故每一层在 $Z_{\mathcal{L}}$ 下均保持不变。

取 $\ell = k$, $r = 2k - 1$，以及 $p = 2k$，定理 S1 在调整普适常数后给出

$$\mathrm{TV}(\mathsf{Out}_s, \mathsf{Out}_s^{\mathrm{id}}) \le C\Delta_k, \qquad \Delta_k = \frac{q^2 + q\sqrt{k}}{\sqrt{d}}, \qquad \Delta_k \le c. \tag{E.9}$$

理想过程使用附录 A中定义的初始化、仪器和终端效应。只有（E.8）中的最后一次跃迁取决于 s。

3. 两条路径之间相干性的压缩映射

改变最终跃迁的符号不会改变两条路径的布居，只会影响它们的相对相干性。下面的引理将界定这种相干性在每个内部阶段中保留的程度。

引理 S10 （一个内部阶段会压缩双路径相干性）。 固定一个历史及其选定的仪器，并记作

$$\alpha_z = \frac{\kappa_{z+} + \kappa_{z-}}{2}, \qquad \beta_z = \frac{\kappa_{z+} - \kappa_{z-}}{2}, \qquad D_z = \alpha_z I + \beta_z Z_{\mathcal{L}}.$$

Then

$$\sum_z (|\alpha_z|^2 + |\beta_z|^2) \le 1, \qquad \sum_z |\alpha_z \beta_z| \le \frac{1}{2}. \tag{E.10}$$

查询之后立即，一个内部层 $1 \le j < k$ 的支撑集为

$$\mathcal{L}_j^{\text{live}} = \text{span}\{\bar{a}_j, Z_{\mathcal{L}} \bar{b}_j\}.$$

对于该子空间上的未归一化态 ρ ， 定义

$$c = \langle \bar{a}_j | \rho | Z_{\mathcal{L}} \bar{b}_j \rangle, \qquad \rho_{z,\text{acc}} = \Gamma_j D_z \rho D_z^\dagger \Gamma_j.$$

下一次查询所接受的输入中的相干性满足

$$c'_z := \langle \bar{a}_j | \rho_{z,\text{acc}} | \bar{b}_j \rangle = \alpha_z \overline{\beta_z}\, c, \qquad \sum_z |c'_z| \le \frac{1}{2}|c|. \tag{E.11}$$

证明。 方程（B.14）对每个扇区给出 $\sum_z |\kappa_{z\sigma}|^2 \le 1$ 因此

$$\sum_z (|\alpha_z|^2 + |\beta_z|^2) = \frac{1}{2} \sum_z \big(|\kappa_{z+}|^2 + |\kappa_{z-}|^2\big) \le 1.$$

不等式 $2|\alpha_z \beta_z| \le |\alpha_z|^2 + |\beta_z|^2$ 由此证明（E.10）。

这四个向量 $\bar{a}_j$， $Z_{\mathcal{L}} \bar{a}_j$， $\bar{b}_j$, $Z_{\mathcal{L}}\, \bar{b}_j$ 是正交归一的。因此

$$\Gamma_j D_z \bar{a}_j = \alpha_z \bar{a}_j, \qquad \Gamma_j D_z Z_{\mathcal{L}} \bar{b}_j = \beta_z \bar{b}_j.$$

将这些恒等式应用于二维输入态，即可证明 c'_z的公式。对其绝对值求和，并利用（E.10），即可得到收缩界。

□

现在我们来界定其影响 f 在单个查询位置改变符号。然后，我们比较两个完整的协议，每次改变一个位 置。

引理 S11 （在一个查询位置改变符号的影响很小）。 在理想协议中固定一个查询位置 t 。比较两个演化过程：它们在除 t 之外的每个位置都使用相同的自适应控制策略和相同的查询符号。当 $t < k$ 时，它们的输出全变差距离为零；当 $t \ge k$ 时，该距离至多为 2^{1-k} 。其他位置上的共同符号可以任意选择。

证明。两个演化过程在查询 t 之前具有相同的状态。在历史 h 中，令 c_h 表示 ¯接受的最后一层输入 $\bar{a}_{k-1}$， b_{k-1} 之间的相干性。只有这种相干性能够检测出符号变化。在端点基 $\bar{a}_k$， $Z_{\mathcal{L}} \bar{a}_k$ 上，两个查询输出之间的差异为

$$\begin{pmatrix} 0 & 2c_h \\ 2\overline{c_h} & 0 \end{pmatrix},$$

其迹范数为 $4|c_h|$。由于各历史占据彼此正交的经典块，查询后立即得到的迹距离为

$$2 \sum_h |c_h|. \tag{E.12}$$

在查询 t 时到达端点的隐藏贡献，必须在查询 $t-k+1$时已从根离开。每次查询都会使其前进一层；仪器会保留其隐藏层，或将其权重转移到根或残余块。残余输入无法进入隐藏层。由于理想初始化（A.6）没有隐藏权重，因此当 $t<k$ 时，没有任何贡献能够到达端点。

现在假设 $t\geq k$。对于查询 $t-k+1$之前紧邻的每个历史 g，令 ω_g为其根块，并设 $p_g=\mathrm{Tr}\ \omega_g$。归一化给出 $\sum_g p_g\leq 1$。每个根块的正性意味着

$$\left|\langle\bar{a}_0|\omega_g|\bar{b}_0\rangle\right|\leq\sqrt{\langle\bar{a}_0|\omega_g|\bar{a}_0\rangle\langle\bar{b}_0|\omega_g|\bar{b}_0\rangle}\leq\frac{p_g}{2}.$$

离开查询会将这种相干性转移到第一层，而不改变其大小。随后，在端点查询之前有 $k-1$个内部仪器步骤。在每个后代历史处应用引理 S10，并对其测量结果求和，可得

$$\sum_h|c_h|\leq 2^{-(k-1)}\sum_g\frac{p_g}{2}\leq 2^{-k}. \tag{E.13}$$

结合（E.12）和（E.13），可将即时迹距离界定为 2^{1-k}。共同的自适应后缀是作用于联合经典–量子态上的完全正迹保持映射。利用迹距离的压缩性，再经过最终读出，即可证明该断言。

□

Su对单个位置的界求和，可得到整个理想协议的均匀界。

命题 S2（ 理想符号不可区分性）。每个 q-查询理想协议，若由 （A.6）初始化，均满足 es

$$\mathrm{TV}(\mathsf{Out}_+^{\mathrm{id}},\mathsf{Out}_-^{\mathrm{id}})\leq(q-k+1)_+\,2^{1-k}\leq q\,2^{1-k}, \tag{E.14}$$

其中 $(x)_+=$ 最大值$\{x,0\}$。

证明。 采用 $q+1$ 混合演化，将全负查询符号序列逐个位置替换为全正序列。相邻的混合序列具有相同的前缀和共同的自适应后缀，并且恰好只在一个查询位置上不同。引理 S11 给出的输出距离界为：前 $k-1$ 个位置处为零，其余每个位置处为 2^{1-k}。由三角不等式可得（E.14）。

□

4. 下界的补全

定理 *S2* 的证明。 对于 $q\geq 1$ 和 $\Delta_k\leq c$，由三角不等式、两个符号各自对应的（E.9）以及命题 S2 可得

$$\mathrm{TV}(\mathsf{Out}_+,\mathsf{Out}_-)\leq q\,2^{1-k}+C\frac{q^2+q\sqrt{k}}{\sqrt{d}}. \tag{E.15}$$

对于 $q=0$，两个输出分布相同。对于 $\Delta_k>c$，增大通用常数 C，使得 $Cc\geq 1$，即可由 TV ≤ 1推出（E.15）。因此，（E.15）对每个 q 均成立。取其右端与 1 中的较小值，即可证明（E.1）。

为了得到查询下界，回顾引理 S9 可知，这两个预言机族的关联器值分别为 $+1$ 和-1。因此，对于任一预言机族中的每个预言机，若估计量的加性误差至多为 $1/3$且成功概率至少为 $2/3$，那么通过取其估计值实部的符号，就能以相同的成功概率区分这两个预言机族。因此，

$$\mathrm{TV}(\mathsf{Out}_+,\mathsf{Out}_-)\geq\frac{1}{3}.$$

将此结果与（E.15）结合可得

$$q=\Omega\Big(\min\Big\{2^k,d^{1/4},\sqrt{d/k}\Big\}\Big),$$

这证明了（E.2）。

□

附录 F：同时估计嵌套关联函数的无辅助系统下界

本附录对定理 1 中的仅系统下界给出了正式陈述和证明。

定理 S3（同时估计嵌套关联函数的仅系统下界）。 存在普适常数c，$C>0$ 具有以下性质。对于每个 $k\geq 1$、每个偶数维度 $d\geq 4M$ 满足 $M=2^k$，以及每个已知的无迹二值可观测量 O，都存在一个已知的单位向量 ψ 和分布 $\mathcal{D}_{\theta,\,s}$ 其定义在 $\mathrm{U}(d)$上，并由 $\theta\in\{0,1\}^k$ 和 $s\in\{\pm 1\}$索引，使得 （1）中的关联函数在取 $O_j=O$、 $t_j=j-1$ 和 $\rho=|\psi\rangle\langle\psi|$时满足

$$F_\sigma(U)=\frac{3s}{8}\mathbf{1}_{\{\sigma=\theta\}} \tag{F.1}$$

在 $\mathcal{D}_{\theta,\,s}$ 的整个支撑集上。每个满足以下条件的仅系统协议

$$\Pr\left(\max_\sigma|\widehat{F}_\sigma-F_\sigma(U)|\leq\frac{1}{3}\right)\geq\frac{2}{3} \tag{F.2}$$

在这些支撑集中的每个预言机上都需要

$$q\geq c\min\{kM,d^{1/4},\sqrt{d/M}\}. \tag{F.3}$$

特别地， $d\geq Ck^4M^4$ 给出 $q=\Omega(kM)$。

为证明定理 S3，我们首先将嵌套关联函数表示为路径重叠之和，并构造一个恰好只有一个非零关联函数的随机预言机族。随后，我们应用模拟定理来获得一个理想树过程。在此过程中，每次遍历都会以一个乘积态抵达端点，而在一次端点访问期间获得的全部信息都可以由一个有偏比特表示。我们对连续访问过程中累积的信息进行界定，并将所得的估计下界转移到物理预言机上。

1. 互补路径展开

我们使用（1）中的可观测量、时间和输入态，其中 $M=2^k$，并简记 $A_j=U^{-t_j}O_jU^{t_j}$。令 $\mathcal{N}_\sigma$表示（1）中迹内未归一化的嵌套括号算子。下面的下界构造使用特殊情形 $O_j=O$， $t_j=j-1$ 以及 $\rho=|\psi\rangle\langle\psi|$。

对于$b=(b_1,\dots,b_k)\in\{0,1\}^k$，和$\chi_\sigma(b)=(-1)^{\sigma\cdot b}$。式（2）中的路径和重叠在海森堡绘景下的表达式为

$$W_b=U^TA_k^{b_k}\cdots A_1^{b_1}, \tag{F.4}$$

and

$$Q_b=\mathrm{Tr}\left(A_1^{1-b_1}\cdots A_k^{1-b_k}A_{k+1}A_k^{b_k}\cdots A_1^{b_1}\rho\right). \tag{F.5}$$

下面的恒等式将每种括号模式表示为这些重叠的傅里叶系数。

引理 S12（互补路径展开）。 对于均匀的 $b\in\{0,1\}^k$，

$$F_\sigma=\frac{i^{|\sigma|}}{2}\mathbb{E}_b[\chi_\sigma(b)Q_b]. \tag{F.6}$$

此外， $Q_{\bar{b}}=Q_b^*$，并且对于每个模式 σ， F_σ 都是实数。

证明。 在括号 j 中，令 $b_j=1$ 选择对 A_j 右乘，令 $b_j=0$ 选择左乘。相应的系数为 1 和 $(-1)^{\sigma_j}$。展开嵌套括号可得

$$\mathcal{N}_\sigma=\sum_b(-1)^{\sum_j\sigma_j(1-b_j)}A_1^{1-b_1}\cdots A_k^{1-b_k}A_{k+1}A_k^{b_k}\cdots A_1^{b_1}. \tag{F.7}$$

对 ρ 取迹，再乘以式 (1) 中的归一化因子和相位，并利用 $(-1)^{\sum_j\sigma_j(1-b_j)}=(-1)^{|\sigma|}\chi_\sigma(b)$，可得 (F.6)，因为 $(-i)^{|\sigma|}(-1)^{|\sigma|}=i^{|\sigma|}$。对 (F.5) 取复共轭可得 $Q_{\bar{b}}=Q_b^*$。结合$\chi_\sigma(\bar{b})=(-1)^{|\sigma|}\chi_\sigma(b)$，即可证明 F_σ 是实数。

□

2. 含有一个非零关联函数的隐藏树

设 $d \geq 4M$ 为偶数，并设 O 为已知的无迹二值可观测量。选取已知的单位向量 $v_\pm$，使得$Ov_\pm = \pm v_\pm$，并令

$$e_\varnothing = \psi = \frac{v_+ + v_-}{\sqrt{2}}, \qquad f_\varnothing = O\psi = \frac{v_+ - v_-}{\sqrt{2}}, \qquad J = (e_\varnothing \;\; f_\varnothing).$$

这两个向量张成根空间。如附录 A 中所述，令 $\mathcal{H}_\pm$ 为 $v_\pm$ 在 O相应特征空间中的正交补。每个正交补的维数均为 $N = d/2 - 1$。绘制相互独立的 Haar 分布标架，使其

$$r = 2M - 2$$

每个扇区中的列向量。将 $M-2$ 个列向量标记为具有 $1 \leq |w| \leq k-1$ 的二进制字 w，并将其余 M 个列向量标记为长度为 k 的字。对于内部字 w，用 $x_{w,\pm}$ 表示其两个扇区列向量，并定义

$$e_w = \frac{x_{w,+} + x_{w,-}}{\sqrt{2}}, \qquad f_w = \frac{x_{w,+} - x_{w,-}}{\sqrt{2}} = Oe_w.$$

根向量对与所有内部向量对彼此正交归一。当 $k = 1$时，不存在内部字。令$F_{\mathrm{end},\pm} : \mathbb{C}^M \to \mathcal{H}_\pm$ 为由端点列向量构成的子标架。

隐藏　　参数为坐标 $\theta \in \{0,1\}^k$ 和符号 $s \in \{\pm 1\}$。固定 $\lambda = 3/4$，并定义

$$P_\theta = \bigotimes_{j=1}^{k} \begin{cases} X, & \theta_j = 0, \\ -Y, & \theta_j = 1, \end{cases}$$

其中 X，Y 是标准泡利矩阵。通过以下方式在端点处编码参数

$$R_{\theta,s} = F_{\mathrm{end},+}\sqrt{\frac{I + s\lambda P_\theta}{2}} + F_{\mathrm{end},-}\sqrt{\frac{I - s\lambda P_\theta}{2}}.$$

由于 P_θ 是厄米酉算子，且 $\lambda < 1$，两个平方根都有定义。两个扇区的正交性给出

$$R_{\theta,s}^\dagger R_{\theta,s} = I, \qquad R_{\theta,s}^\dagger O R_{\theta,s} = s\lambda P_\theta. \tag{F.8}$$

因此，$R_{\theta,\,s}$ 是一个从 $\mathbb{C}^M$ 映入 $2M$维端点空间的等距映射。指定跃迁

$$\begin{aligned} &Ue_w = e_{w0}, && Uf_w = e_{w1} && (0 \leq |w| \leq k-2), \\ &Ue_w = R_{\theta,s}|w0\rangle, && Uf_w = R_{\theta,s}|w1\rangle && (|w| = k-1). \end{aligned} \tag{F.9}$$

对于 $k = 1$，仅适用第二行，其中 $w = \varnothing$。每次查询都会向路径中追加一位，而第 k次查询到达端点。共有

$$p = 2\sum_{j=0}^{k-1} 2^j = 2M - 2$$

个指定输入向量。它们的输出由 $M-2$ 个内部向量和 M 个端点向量构成，因此两组向量都是正交归一的。设 V_F 和 $W_{F,\,\theta,\,s}$ 分别包含这些输入列和输出列。通过设定以下内容，将指定跃迁补全为一个酉算子

$$U = W_{F,\theta,s}V_F^\dagger + B_{F,\theta,s}H_D C_F^\dagger, \qquad H_D \sim \mathrm{Haar}(\mathrm{U}(D)), \qquad D = d - p. \tag{F.10}$$

这里，C_F 和 $B_{F,\,\theta,\,s}$ 是分别映 onto 输入补空间和输出补空间的等距映射，而 H_D 与标架无关。假设 $d \geq 4M$ 确保 $r \leq N$ 和 $D \geq d/2$。这些标架及补全只抽取一次，并在每次查询中重复使用；它们的联合抽样定义了 $\mathcal{D}_{\theta,\,s}$。

下一个引理验证，这种构造将唯一的非零关联函数置于坐标 θ，其符号为 s。

Lemma S13 （精确关联函数向量）。 支撑集中的每个预言机 $\mathcal{D}_{\theta,\,s}$ 都满足 （F.1）　　.

证明。对于目标时刻， $W_b = (UO^{b_k}) \cdots (UO^{b_1})$ 。从 $\psi = e_\varnothing$开始，门 O^{b_j}选择 e_w或 f_w，接下来的查询将 b_j 追加到路径中。（F.9）因此得到

$$W_b\psi = R_{\theta,s}|b\rangle.$$

由于

$$X|b_j\rangle = |1-b_j\rangle, \qquad (-Y)|b_j\rangle = -i(-1)^{b_j}|1-b_j\rangle,$$

我们有

$$P_\theta|b\rangle = (-i)^{|\theta|}(-1)^{\theta\cdot b}|\bar{b}\rangle.$$

根据（F.8），互补路径重叠为

$$Q_b = \langle\bar{b}|R_{\theta,s}^\dagger O R_{\theta,s}|b\rangle = s\lambda(-i)^{|\theta|}(-1)^{\theta\cdot b}.$$

代入（F.6），并利用 $\mathbb{E}_b(-1)^{(\sigma+\theta)\cdot b} = \mathbf{1}_{\{\sigma=\theta\}}$ 可得

$$F_\sigma = \frac{s\lambda}{2}\mathbf{1}_{\{\sigma=\theta\}}.$$

由 $\lambda = 3/4$ 可得该断言。 □

3. 化简为理想树

现在用附录 A 的记号表示该构造。取 $\vartheta = (\theta, s)$、 $\ell = k$，以及 $r = p = 2M-2$。对于$1 \le j \le k$，定义

$$\mathcal{L}_j = \mathrm{span}\{|w,\nu\rangle : |w| = j,\ \nu = \pm 1\}, \qquad Z_{\mathcal{L}}|w,\nu\rangle = \nu|w,\nu\rangle.$$

因此， $Z_{\mathcal{L}}$ 在每一层内作用。对于 $1 \le |w| < k$，令

$$\bar{e}_w = \frac{|w,+\rangle + |w,-\rangle}{\sqrt{2}}, \qquad \bar{f}_w = \frac{|w,+\rangle - |w,-\rangle}{\sqrt{2}} = Z_{\mathcal{L}}\bar{e}_w.$$

¯在根处，使用基 $\bar{e}_\varnothing$， $f_\varnothing$经 J映射到 $e_\varnothing$， $f_\varnothing$。
对于端点扇区嵌入 $I_\pm : \mathbb{C}^M \to \mathcal{L}_k$，定义

$$\mathcal{R}_{\theta,s} = I_+\sqrt{\frac{I + s\lambda P_\theta}{2}} + I_-\sqrt{\frac{I - s\lambda P_\theta}{2}}.$$

Then

$$\mathcal{R}_{\theta,s}^\dagger\mathcal{R}_{\theta,s} = I, \qquad \mathcal{R}_{\theta,s}^\dagger Z_{\mathcal{L}}\mathcal{R}_{\theta,s} = s\lambda P_\theta. \tag{F.11}$$

¯理想跃迁由（F.9）得到，方法是将 e_w、 f_w、 $R_{\theta、s}$替换为 $\bar{e}_w$、 f_w、 $\mathcal{R}_{\theta、s}$。取 $\mathcal{I}_j = \mathcal{L}_j$和 $V_j = I$作为$0 \le j < k$。因此

$$\Gamma_j = I_{\mathcal{L}_j} \quad (0 \le j < k), \qquad \Gamma_k = 0.$$

每个根或内部输入都会前进到下一层，而端点输入则被送入残余块。Th
这些c hoi这些sat isfy the hypoth这些o f Th定理 S1. C推论 ly, f对于每个a llowed q-查询协议 l and each
固定（θ， s），

$$\mathrm{TV}(\mathsf{Out}_{\theta,s}, \mathsf{Out}_{\theta,s}^{\mathrm{id}}) \le C\Delta, \qquad \Delta = \frac{q^2 + q\sqrt{r+1}}{\sqrt{d}}, \qquad q \ge 1, \quad \Delta \le c_0. \tag{F.12}$$

物理输出对预言机的初始抽取取平均值。

理想仪器规则遵循附录A。具体来说，测量结果 z 中保留在隐藏层内的部分作用于

$$D_z = \bigoplus_{\nu=\pm1} \kappa_{z\nu} I_{\mathcal{L}_\nu}, \qquad \kappa_{z\nu} = \frac{\mathrm{Tr}(\Pi_\nu K_z)}{N}.$$

其他去向是根块和残余块。因此，仪器可以留在当前层，也可以结束当前遍历，但不能直接移动到另一个隐藏层。只有进入端点的最后一次跃迁取决于（θ， s）。

4. 遍历中的乘积态

为了界定理想过程中的可用信息，我们可以向协议提供额外的经典信息。揭示其初始块，并在每次仪器操作后告知状态是留在当前层，还是移至根块或残余块。这些去向是理想仪器的完全正子项，因此忽略额外标记即可还原原始过程。我们允许后续控制依赖这些标记；对于这一扩展类别，成功率的上界同样适用于原始协议。这些标记揭示了占据层，但不揭示任何单独的路径标签。

当一次查询离开根时，遍历便开始；当查询返回根、进入残余块或丢弃端点时，遍历便结束。将根视为一个虚拟量子比特，并将每个内部层表示为

$$\bar{e}_w \longleftrightarrow |w\rangle|0\rangle, \qquad \bar{f}_w \longleftrightarrow |w\rangle|1\rangle, \qquad |w| = j. \tag{F.13}$$

前 j 个量子比特编码路径，最后一个量子比特是标志位。在这些坐标下，

$$Z_{\mathcal{L}} = I_{\text{path}} \otimes X, \qquad D_z = I_{\text{path}} \otimes L_z, \qquad L_z = a_z I + b_z X, \tag{F.14}$$

其中

$$a_z = \frac{\kappa_{z,+} + \kappa_{z,-}}{2}, \qquad b_z = \frac{\kappa_{z,+} - \kappa_{z,-}}{2}.$$

下一个引理表明，它们可达的状态具有乘积结构。

引理 S14 (遍历中的乘积结构)。 在给定完整经典历史 h 的条件下，层 $0 \le j < k$ 中的归一化态具有如下形式

$$\tau_h^{(j)} = \tau_{h,1} \otimes \cdots \otimes \tau_{h,j} \otimes \phi_h, \tag{F.15}$$

其中每个因子都是一个单量子比特密度矩阵，而 ϕ_h 是当前标记态。特别地，端点跃迁的输入是定义在 k 个量子比特上的乘积态：

$$\tau_h = \tau_{h,1} \otimes \cdots \otimes \tau_{h,k-1} \otimes \phi_h, \qquad \tau_h \longmapsto \mathcal{R}_{\theta,s} \tau_h \mathcal{R}_{\theta,s}^\dagger. \tag{F.16}$$

遗忘经典细化后，得到乘积态的凸混合。

证明。 根态是任意一个单量子比特密度矩阵 ϕ_h，由此得到 （F.15），其中 $j = 0$。

假设在某个内部层中，状态具有所述形式。一个存活仪器结果只作用于其最后一个因子。记作 $c_{h,\ z} = \mathrm{Tr}(L_z \phi_h L_z^\dagger)$，当 $c_{h,\ z} > 0$ 时，其归一化输出为

$$\frac{D_z \tau_h^{(j)} D_z^\dagger}{\mathrm{Tr}(D_z \tau_h^{(j)} D_z^\dagger)} = \bigotimes_{a=1}^{j} \tau_{h,a} \otimes \frac{L_z \phi_h L_z^\dagger}{c_{h,z}}. \tag{F.17}$$

对于 $0 \le j < k-1$，下一次查询的作用为

$$\mathcal{T}_j : |w\rangle|b\rangle \longmapsto |wb\rangle|0\rangle.$$

因此得到

$$\mathcal{T}_j \tau_h^{(j)} \mathcal{T}_j^\dagger = \bigotimes_{a=1}^{j} \tau_{h,a} \otimes \phi_h \otimes |0\rangle\langle 0|. \tag{F.18}$$

因此，实时仪器只会改变当前标志，而查询会将该标志存储为下一个路径因子，并重新附加一个标志。

返回根时会丢弃所有路径因子。更明确地说，对于扇区布居为π_ν =Tr($P_{j\nu}\omega$)的归一化隐藏态 ω，测量结果为 z 的根分支具有如下概率和归一化态

$$r_z(\omega) = \sum_\nu \pi_\nu \,\mathrm{Tr}\, Q_{z\nu}, \qquad \rho_{z,\mathrm{root}}(\omega) = \frac{\sum_\nu \pi_\nu Q_{z\nu}}{r_z(\omega)} \quad \text{if } r_z(\omega) > 0. \tag{F.19}$$

这又是一个单独的根量子比特。残余分支只保留一个标量权重，而从残余块后续返回时也会制备一个根量子比特。因此，每次重置后都会重新开始归纳。

最终查询作用于$\mathcal{R}_{\theta,\ s}$得到 k量子比特乘积态，从而证明（F.16）。对被忽略的经典细化取平均，得到乘积态的凸混合。 □

5. 单次端点访问的信息

端点访问在抵达时开始，并在状态移至根或残余块，或执行最终测量时结束。令 Ξ_ν 投影到 $\nu \in \{\pm 1\}$ 的扇区 $\mathcal{L}_k$。对于输入端点跃迁的归一化输入 τ，（F.11）给出各扇区的概率

$$p_{\theta,s}(\nu \mid \tau) = \operatorname{Tr}\left(\Xi_\nu \mathcal{R}_{\theta,s} \tau \mathcal{R}_{\theta,s}^\dagger\right) = \frac{1 + \nu s \lambda \operatorname{Tr}(P_\theta \tau)}{2}. \tag{F.20}$$

下面的引理表明，这两个概率足以模拟一次访问的完整经典记录。

引理 S15 (端点访问的单比特表示)。 固定端点到达之前的历史 h，并令 τ 为端点跃迁的输入。访问期间的测量结果和目的地记录 e 可以通过以下方式生成：首先按照概率 $p_{\theta,\ s}(\nu \mid \tau)$抽取一个比特 $S \in \{\pm 1\}$，然后从条件分布 $K_h(e \mid S)$中抽样得到 e；该条件分布与 θ、s 和 τ 无关。因此，实际访问记录的概率 $\mathbb{P}_{\theta,\ s}(e \mid h, \tau)$ 满足

$$\mathbb{P}_{\theta,s}(e \mid h, \tau) = \sum_{\nu=\pm 1} p_{\theta,s}(\nu \mid \tau) K_h(e \mid \nu). \tag{F.21}$$

证明。 一个停留在端点的仪器结果会施加

$$D_z = \kappa_{z,+}\Xi_+ + \kappa_{z,-}\Xi_-.$$

该算子在每个扇区内都表现为标量。根映射、残余映射和最终测量概率仅取决于扇区权重。因此，在到达时测量扇区不会改变访问统计。其测量结果 $S = \nu$ 的概率为 $p_{\theta,\ s}(\nu \mid \tau)$。给定 $S = \nu$，仪器规则给出

$$\begin{aligned} K(z, \text{live} \mid \nu) &= |\kappa_{z\nu}|^2, \\ K(z, \text{root} \mid \nu) &= \operatorname{Tr} Q_{z\nu}, \\ K(z, \perp \mid \nu) &= w_{z\nu}. \end{aligned} \tag{F.22}$$

这些概率之和为一：

$$\sum_z \left(|\kappa_{z\nu}|^2 + \operatorname{Tr} Q_{z\nu} + w_{z\nu}\right) = \sum_z p_{z\nu} = 1.$$

继续结果保留相同的扇区。根节点结果以非零概率制备 $Q_{z\nu}/\operatorname{Tr} Q_{z\nu}$，而残余结果会结束此次访问。查询也会将状态发送到残余块，从而结束此次访问。对于最终的正算子值测度 $\{M_y\}_y$，条件概率为

$$K(y \mid \nu) = \frac{\operatorname{Tr}(\Pi_\nu M_y)}{N}. \tag{F.23}$$

所有这些规则都与参数无关。按照协议依赖历史的策略应用这些规则，即可定义整个访问记录的条件分布 $K_h(e \mid \nu)$。对 S 取平均即可证明（F.21）。 □

单比特表示将每次访问中的参数依赖性隔离在 S 的偏差中。为了界定协议的性能，我们可以揭示该比特，并允许后续控制依赖于它。这只会为协议提供更多信息；忽略该比特即可恢复原始的理想过程。

给定增强历史，上述重置规则无需知道 (θ, s)即可确定根态。下一个端点到达前的所有跃迁也都与参数无关。因此，下一个端点输入仅由历史决定，并且根据引理 S14，它是一个乘积态。以下界适用于这些状态及其凸混合，并限制每次访问所获得的信息。

引理 S16 （平方偏差界）。对于任意由 τ 个 k 量子比特乘积态构成的凸混合，

$$\sum_{\theta \in \{0,1\}^k} \left[\lambda \operatorname{Tr}(P_\theta \tau)\right]^2 \le \lambda^2. \tag{F.24}$$

证明。对于一个乘积态 $\tau = \bigotimes_j \tau_j$，记 $x_j = \mathrm{Tr}(X\tau_j)$ 和 $y_j = \mathrm{Tr}(Y\tau_j)$。那么

$$\sum_{\theta} \big[\lambda \,\mathrm{Tr}(P_\theta \tau)\big]^2 = \lambda^2 \prod_{j=1}^{k} (x_j^2 + y_j^2) \le \lambda^2,$$

因为每个量子比特态都满足 $x_j^2 + y_j^2 \le 1$。由于每个偏差都是 τ 的实线性函数，(F.24) 左侧关于 τ 是凸的。因此，该界也适用于乘积态的凸混合。 □

虽然存在 $M = 2^k$ 个可能的隐藏坐标，但它们的偏差平方之和有常数λ^2的上界。因此，单个端点输入无法同时在许多参数上产生较大的偏差。在下一小节中，我们将利用这一界来控制自适应选择的端点访问过程中累积的信息。

6. 在自适应控制下累积信息

每次端点到达都需要对 k 个查询进行一次新的从根到端点的遍历。因此，至多使用 q 个查询的协议，在任何一次执行过程中最多有

$$L_{\mathrm{leaf}} := \lfloor q/k \rfloor \tag{F.25}$$

次到达 。为便于分析，必要时在终止后追加独立的公平比特，使得每个分支都有一个精确的 位列表 L_{leaf}。这些额外比特不会影响输出。

令 $\mathbb{P}_{\theta,\, s}$ 表示增强理想过程的完整转录分布，其中包括目的地标志、端点比特、仪器测量结果、经典随机性和最终估计值。定义共同参考概率律 $\mathbb{P}_0$：将每个端点比特替换为公平硬币，同时保持协议策略及所有其他条件规则不变。

在端点到达之前的固定增强历史 h 处，输入 τ_h 是仅由 h 决定的乘积态。事实上，记录的端点比特和测量结果决定了重置态，而内部转移与参数无关。在$\mathbb{P}_{\theta,\, s}$下，下一个端点比特的条件均值为

$$b_{\theta,s}(h) = s\lambda \,\mathrm{Tr}(P_\theta \tau_h), \qquad |b_{\theta,s}(h)| \le \lambda.$$

对于追加的比特，设 $b_{\theta,\, s}(h) = 0$。由于固定历史下的输入对所有参数都相同，我们可以在对历史取平均之前应用平方偏差界。由此得到以下估计成功率界。

命题 S3（理想树中的成功概率）。对于 $\lambda = 3/4$，任何至多使用 q次查询的增强理想协议都满足

$$p_{\mathrm{id}} \le \frac{1}{2} + \frac{3}{2\sqrt{7}} \sqrt{\frac{q}{kM}}, \tag{F.26}$$

其中，p_{id} 是所有关联函数估计值的加性误差至多为 $1/3$ 的概率，取遍 (θ, s) 后的均匀平均值。

证明。我们首先将转录分布与 $\mathbb{P}_0$ 进行比较。记 $D(P\|Q)$ 为采用自然对数的相对熵。对于一个公平比特和一个偏差为 b 的带偏比特，若 $|b| \le \lambda < 1$，

$$d(b) := D(\mathrm{Bern}(1/2) \,\|\, \mathrm{Bern}((1+b)/2)) = -\frac{1}{2}\log(1-b^2) \le \frac{b^2}{2(1-\lambda^2)}.$$

在固定的历史下，只有 t 端点比特分布在 $\mathbb{P}_0$ 和 $\mathbb{P}_{\theta,s}$ 之间不同。因此，链式法则给出 s

$$D(\mathbb{P}_0 \| \mathbb{P}_{\theta,s}) = \sum_{\ell=1}^{L_{\mathrm{leaf}}} \mathbb{E}_{h_\ell \sim \mathbb{P}_0} d\big(b_{\theta,s}(h_\ell)\big),$$

其中，h_ℓ 是第 ℓ 个比特之前的历史。采用这一方向的相对熵，可确保所有期望都在同一个参考分布下计算。

在每次实际端点到达时，引理 S16 给出

$$\frac{1}{2M} \sum_{\theta,s} b_{\theta,s}(h)^2 = \frac{1}{M} \sum_{\theta} \big[\lambda \,\mathrm{Tr}(P_\theta \tau_h)\big]^2 \le \frac{\lambda^2}{M}.$$

同样的界也适用于追加的比特，其偏差为零。对 $(\theta,\ s)$ 的链式法则取平均，得到

$$\frac{1}{2M}\sum_{\theta,s} D(\mathbb{P}_0\|\mathbb{P}_{\theta,s}) \le \frac{L_{\text{leaf}}\lambda^2}{2(1-\lambda^2)M}. \tag{F.27}$$

Pinsker不等式和柯西–施瓦茨不等式随即推出

$$\begin{aligned}\frac{1}{2M}\sum_{\theta,s}\mathrm{TV}(\mathbb{P}_0,\mathbb{P}_{\theta,s}) &\le \sqrt{\frac{1}{4M}\sum_{\theta,s} D(\mathbb{P}_0\|\mathbb{P}_{\theta,s})}\\ &\le \frac{\lambda}{2}\sqrt{\frac{L_{\text{leaf}}}{(1-\lambda^2)M}}.\end{aligned} \tag{F.28}$$

^为将该距离与估计成功率联系起来，我们可以令估计值 F_σ 为实数，因为取实部不会增加其误差。根据（F.1），同时误差至多为 1/3意味着

$$s\widehat{F}_\theta \ge \frac{3}{8}-\frac{1}{3}=\frac{1}{24}.$$

因此，参数（$\theta,\ s$）下的成功意味着事件

$$A_{\theta,s}=\{s\widehat{F}_\theta \ge 1/24\}.$$

对于每个 θ，事件 $A_{\theta,\ +}$ 和 $A_{\theta,\ -}$ 是不相交的。在共同参考概率律下，这给出

$$\frac{1}{2M}\sum_{\theta,s}\mathbb{P}_0(A_{\theta,s}) \le \frac{1}{2}.$$

因此，

$$\begin{aligned}p_{\text{id}} &\le \frac{1}{2M}\sum_{\theta,s}\mathbb{P}_{\theta,s}(A_{\theta,s})\\ &\le \frac{1}{2}+\frac{1}{2M}\sum_{\theta,s}\mathrm{TV}(\mathbb{P}_0,\mathbb{P}_{\theta,s}).\end{aligned}$$

将 $\lambda=3/4$ 代入（F.28），并利用 $L_{\text{leaf}}\le q/k$ 即可证明（F.26）。 □

7. 下界的补全

我们还需要将理想情况下的成功概率上界转移到物理预言机族。

定理 *S3* 的证明。 设 p_{true} 为对均匀抽取的 (θ,s) 以及抽样 $U\sim\mathcal{D}_{\theta,s}$取平均后的成功概率。由引理 S13可知，固定预言机族中的所有预言机 $\mathcal{D}_{\theta,s}$ 都具有相同的关联向量。因此，成功对应于经典输出中的一个固定事件，故可应用（F.12）。将此比较与命题 S3 结合，并利用 $r=2M-2$ 可得

$$p_{\text{true}} \le \frac{1}{2}+\frac{3}{2\sqrt{7}}\sqrt{\frac{q}{kM}}+C\frac{q^2+q\sqrt{M}}{\sqrt{d}} \tag{F.29}$$

对于 $q\ge 1$ 和 $\Delta\le c_0$。对于 $q=0$，输出与参数无关，而上述不相交事件论证给出$p_{\text{true}}\le 1/2$。

假设

$$q < c_*\min\{kM, d^{1/4}, \sqrt{d/M}\}.$$

Then

$$\sqrt{\frac{q}{kM}} < \sqrt{c_*},\qquad \frac{q^2}{\sqrt{d}} < c_*^2,\qquad \frac{q\sqrt{M}}{\sqrt{d}} < c_*.$$

C选择足够小的通用 $c_*>0$ 可确保满足模拟条件，并得到

$$p_{\text{true}} \le \frac{1}{2}+\frac{3}{2\sqrt{7}}\sqrt{c_*}+C(c_*^2+c_*) < \frac{2}{3}.$$

这一矛盾　　的成功概率至少为 2/3，适用于每个支撑集中的每个预言机，从而证明（F.3　　）. □

附录 G：相干查询次数的下界

在本附录中，我们为估计单个多时刻关联函数$C(U)$或嵌套关联函数 $F_\theta(U)$建立指数级查询下界，其中相干查询次数上限为 $L < k$。我们考虑一种通用的自适应模型：每次实验运行都可以使用任意辅助寄存器和电路中途的量子仪器，但对未知酉算子 U至多进行 L 次正向查询。不同实验运行之间，所有量子存储器都会被丢弃或重置，同时保留完整的经典测量记录，以便自适应地配置后续实验。

定理 S4 （相干查询次数的一个阈值，定理 3 的形式化版本）。令 $k \geq 2$、 $M = 2^k$，并令 $d = 2^n \geq 4M$。固定一个已知的无迹二值可观测量 O。存在一个已知的单位向量 ψ 和预言机分布 $\mathcal{D}_{\theta,\, s}$，满足 $\theta \in \{0,1\}^k$和 $s \in \{+1,-1\}$，使得对于 $O_j = O$、 $t_j = j-1$ 和 $\rho = |\psi\rangle\langle\psi|$,

$$C(U) = \frac{3s}{4} i^{|\theta|}, \qquad F_\sigma(U) = \frac{3s}{8} \mathbf{1}_{\{\sigma=\theta\}} \quad on\ \operatorname{supp} \mathcal{D}_{\theta,s}. \tag{G.1}$$

对于任意固定且公开已知的 θ，上述模型中的任何协议若每次运行至多进行 $L < k$ 次正向查询，且总计至多进行 q 次查询，则满足

$$\mathrm{TV}(\mathsf{Out}_{\theta,+}, \mathsf{Out}_{\theta,-}) \leq 32\sqrt{\frac{q^3 \log d}{d}} + 672q\sqrt{\frac{M}{d}}, \tag{G.2}$$

其中，$\mathsf{Out}_{\theta,\, s}$ 是从 $\mathcal{D}_{\theta}$中一次抽取并在整个协议中重复使用的单个预言机上取平均得到的经典输出分布，s 。因此，对于这些支撑集中的每个预言机，以至少 $2/3$ 的成功概率将 $C\ (U)$ 或规定的 $F_\theta\ (U)$ 估计到加性误差 $1/3$ 以内，都需要

$$q \geq \frac{1}{4096} \min\left\{ \left(\frac{d}{\log d}\right)^{1/3}, \sqrt{\frac{d}{2^k}} \right\}. \tag{G.3}$$

特别地， $n \geq 4k$ 给出 $q = \Omega(2^{n/4})$。

具体而言，我们的证明建立在附录 F2中的隐藏树系综之上，其中未知符号 $s \in \{\pm 1\}$ 仅在深度 k处编码。以下小节将详细阐述论证的核心：将每次运行至多进行$L < k$ 次查询的任意协议，与一种将树截断至前 L 层、使其演化完全独立于 s的辅助过程进行比较，并界定所有 q 次查询所导致的总变差误差。

1. 隐藏树及其前几层

我们简要回顾附录 F2 中的隐藏树构造，并提取浅层实验所访问的前缀结构。在整个证明中，目标字符串 $\theta \in \{0,1\}^k$ 固定且公开已知，协议只需区分符号 $s \in \{\pm 1\}$。

C选择已知的单位特征向量 $v_\pm$ ，它们属于 O 且满足 $Ov_\pm = \pm v_\pm$，并定义根基 s

$$e_\varnothing = \psi = \frac{v_+ + v_-}{\sqrt{2}}, \qquad f_\varnothing = \frac{v_+ - v_-}{\sqrt{2}}.$$

每个特征空间内 $v_\pm$ 的正交补 $\mathcal{H}_\pm$ 维数为 $N = d/2 - 1$。在每个扇区中，我们独立抽取一个 Haar 分布标架 $F_\pm$ ，其中每个长度为 $1 \leq |w| \leq k$的二进制字 w 都对应一列 $x_{w,\, \pm}$ ，其中 $|w|$ 表示字长，而 $w0$， $w1$ 表示单比特扩展。因此，每个扇区标架有

$$r = \sum_{j=1}^{k} 2^j = (M-2) + M = 2M - 2$$

列，而已知的根向量不包含在 $F_\pm$ 中。对于每个内部字 $1 \leq |w| < k$，我们设

$$e_w = \frac{x_{w,+} + x_{w,-}}{\sqrt{2}}, \qquad f_w = \frac{x_{w,+} - x_{w,-}}{\sqrt{2}}.$$

记作 $F = F_+ \oplus F_-$，附录 F2 中的预言机族规定了树转换

$$\begin{aligned} Ue_w &= e_{w0}, \qquad Uf_w = e_{w1} \qquad (0 \le |w| \le k-2), \\ Ue_w &= R_{\theta,s}|w0\rangle, \quad Uf_w = R_{\theta,s}|w1\rangle \quad (|w| = k-1), \end{aligned}$$

其中 $R_{\theta,\ s}$ 是附录 F2 （其中 $\lambda = 3/4$）中的端点等距映射，其值域位于长度为 k 的标架列张成的空间中。关键在于，只有 $|w| = k-1$ 处的这次最终跃迁依赖于 （θ，s）。

令 V_F 收集 $|w| < k$ 的输入向量（e_w、f_w），并令 W_F、θ、s 按相同顺序收集它们对应的输出。二者均构成由 $p = 2\sum_{j=0}^{k-1} 2^j = 2M-2$ 列组成的正交归一标架。指定（F、θ、s）即可确定作用 $UV_F = W_F$、θ、s；而在 (Ran V_F)$^\perp$ 上的作用则通过一个独立的 Haar 随机酉算子补全，将其映射到 (Ran W_F、θ、s)$^\perp$，如式（F.10）所示。我们将此称为对指定跃迁的 Haar 补全。

为建立相干查询次数有界的实验模型，对于每个 $1 \le j < k$，我们通过仅保留输入字长度为 $|w| < j$ 的跃迁，来定义其深度为 j 的前缀。其输入与输出标架为

$$V^{[j]} = (e_w, f_w)_{|w|<j}, \qquad W^{[j]} = (e_{w0}, e_{w1})_{|w|<j},$$

排序完全相同。由于深度为 j 的前缀的输出对应的字长至多为 $j < k$，因此该前缀不会访问端点等距映射 $R_{\theta,s}$，并且完全独立于 (θ, s)。

最后，对于 $0 \le t < k$，令 Z_t 收集标架列 $x_{w,\pm}$，其中 $1 \le |w| \le t$ （Z_0 为空），每个扇区包含 $a_t = \sum_{j=1}^{t} 2^j = 2^{t+1} - 2$ 列。我们用以下符号表示投影到其余更深层标架列上的正交投影算子

$$P_t = \sum_{\sigma=\pm} \sum_{t<|w|\le k} |x_{w,\sigma}\rangle\langle x_{w,\sigma}|.$$

注意，Z_t 和 P_t 是为后续分析引入的，协议并不知道它们。下面的引理总结了该系综的精确关联函数值，并表明将树截断在深度 $t+1$ 处，只会改变支撑集位于 Ran P_t 上的跃迁。

引理 S17 (树的信号与几何)。预言机系综 $\mathcal{D}_{\theta,s}$ 满足式 (G.1)。对于每个 $1 \le j < k$，深度为 j 的前缀有 $2^{j+1}-2$ 个输入列和输出列，且完全由 Z_j 确定，与 (θ, s) 无关。此外，对于 $0 \le t \le k-2$，深度为 $(t+1)$ 前缀中省略的跃迁对应于长度为 $t+1 \le |w| \le k-1$ 的输入字，且其中所有输入和输出都位于 值域 P_t:

$$e_w,\ f_w,\ Ue_w,\ Uf_w \in \mathrm{Ran}\, P_t \qquad (t+1 \le |w| \le k-1).$$

此外，在 $F_\pm$ 的初始 *Haar* 分布下，条件于固定前 a_t 列 Z_t 后，每个扇区中的其余列构成环境子空间中秩为 $r - a_t$、维数为

$$N - a_t \ge D_* := d/2 - M/2 + 1 \ge d/4. \tag{G.4}$$

证明。根据引理 S13，互补路径重叠满足 $Q_b = (3s/4)(-i)^{|\theta|}(-1)^{\theta\cdot b}$。将其取值为 $b = \mathbf{1}$ 后，可得到公式 (G.1) 中的 $C(U) = Q_{\mathbf{1}}$，而 $F_\sigma(U)$ 的表达式可直接由公式 (F.1) 得出。接下来，深度为 j 的前缀对于每个长度为 $0 \le |w| \le j-1$ 的字包含两列，因此总共有 $2\sum_{a=0}^{j-1} 2^a = 2^{j+1} - 2$ 列。给定的树转换立即意味着 $(V^{[j]}, W^{[j]})$ 仅取决于 Z_j，并且 $t+1 \le |w| \le k-1$ 的所有输入和输出都支撑在满足 $|w| > t$ 的列上，即位于 Ran P_t 中。最后，在每个扇区内，条件于一个 Haar分布的框架的 a_t 列后，剩余的 $r - a_t$ 列在 $(N - a_t)$ 维正交补中仍服从 Haar分布。由于 $t \le k-2$ 蕴含 $a_t \le 2^{k-1} - 2 = M/2 - 2$，代入 $N = d/2 - 1$ 和 $d \ge 4M$ 即得到公式 (G.4)。

□

2. 与独立于符号的过程进行比较

现在，我们在一个共同概率空间上对完整酉算子和前缀酉算子进行耦合，并利用前缀酉算子定义一个符号无关的辅助过程。随后，将物理协议与该辅助过程进行比较，就归结为界定每个查询输入态在未访问的树子空间 Ran P_t 上的权重。

a. 耦合 *Haar* 补全

由于完整树及其前缀只指定了部分等距算子，我们使用一个独立于 F 抽取的 Haar 酉矩阵 $G \sim \mathrm{Haar}(\mathrm{U}(d))$，将它们的随机补全耦合起来。这个联合构造确保每个预言机都保留其精确的边缘补全分布，同时允许我们直接比较它们对同一输入态的作用。

引理 S18 （完整预言机与前缀预言机的耦合构造）。 设 $G \sim \mathrm{Haar}(\mathrm{U}(d))$ 独立于 F。存在一个联合构造

$$U_{\theta,s} = U_{\theta,s}(F, G), \qquad U^{[j]} = U^{[j]}(Z_j, G), \quad 1 \le j < k,$$

使得给定 F 的条件下，酉算子 $U_{\theta,\,s}$ 满足 $U_{\theta,\,s}V_F = W_{F,\,\theta,\,s}$，并且作为一个从(值域 $V_F)^{\perp}$ 到 （值域 $W_{F,\,\theta,\,s}$）$^{\perp}$ 的 *Haar* 随机酉算子发挥作用。同样，给定 Z_j 的条件下，每个前缀预言机 $U^{[j]}$ 都满足 $U^{[j]}V^{[j]} = W^{[j]}$，并且在相应的正交补空间之间作为 *Haar* 随机酉算子发挥作用。

定义标架重叠

$$\delta_{\theta,s} := \|V_F^{\dagger} G^{\dagger} W_{F,\theta,s}\|.$$

对于每个 $0 \le t \le k-2$ 和每个系统–辅助系统向量 ϕ,

$$\|(U_{\theta,s} - U^{[t+1]})\phi\| \le 2\big(\|P_t\phi\| + \|P_t G\phi\|\big) + 32\delta_{\theta,s}\|\phi\|, \tag{G.5}$$

其中系统算子在辅助系统上作用为恒等算子。此外，

$$\mathbb{E}_G[\delta_{\theta,s} \mid F] \le 10\sqrt{M/d}. \tag{G.6}$$

因此，单次查询的替换误差由以下向量在更深的树子空间上的投影所控制： ϕ 和 $G\phi$ 投影到更深的树子空间值域 P_t，另有一个较小的重叠修正项$\delta_{\theta,\,s}$。引理S18 的证明推迟到第G 3节。

b. 定义辅助过程

辅助过程与物理协议完全相同，唯一区别在于预言机调用：在每次实验运行中，对U_{θ}的 j次查询由 $U^{[j]}$替代。每次完整的量子重置后，步数计数器 j 都会重置为 1；而共享随机对 $\Xi = (F,\ G)$从其先验分布 μ_{Ξ}中抽取一次，并在所有运行中重复使用。由于每次运行至多进行 $L < k$次查询，辅助过程只会调用 $U^{[1]}$、……、$U^{[L]}$，因此完全独立于 s。

我们将所有实验中的查询时隙统一编号为 $i = 1$、……、q。在某个固定时隙之前，令 H 表示经典历史， h 表示一次实现， $t(h)$表示当前实验中已进行的查询次数。对于活跃历史， $t(h) \le L - 1 \le k - 2$。

下一个引理对 H 中累积的经典信息进行界定，并表明量子态仅取决于上次重置后访问过的树列。

引理 S19 (重置后的信息与状态依赖性)。 在辅助过程的每个全局查询时隙之前， Ξ 的边缘分布为 μ_{Ξ}，并且

$$I(\Xi; \mathsf{H}) \le 2q \log d. \tag{G.7}$$

查询寄存器的约化态有一个归一化版本

$$\sigma(\Xi, h) = \sigma(h, G, Z_{t(h)}), \tag{G.8}$$

对每个参数 –历史对均有定义。特别地，辅助输出分布与 s 无关。

证明。对所有历史求和后， Ξ 在 μ_{Ξ} 处的边缘分布保持不变。为证明信息界，令 $A \cong \mathbb{C}^d$ 为查询寄存器， R 为所有其他量子存储器。查询仅作用于 A，并保持 $\mathrm{H}R$ 上的边缘分布不变。根据链式法则和 $0 \le I(\Xi;\ A \,|\, \mathrm{H}R) \le 2$log d，每次查询使 $I(\Xi;\ \mathrm{H}RA)$ 至多增加 2 log d，而已知操作不会增加此信息。由于初始态与 Ξ 独立，至多经过 q 次查询后即可得到式 (G.7)。

对于式（G.8），固定当前实验开始时的历史 h_0。重置后，给定 h_0，其初始态便是已知的。前 $t = t(h)$次查询使用 $U^{[1]}$、……、$U^{[t]}$，它们仅取决于 (G, Z_t)，而已知操作则由记录的结果决定。因此，本次实验中生成的未归一化态仅取决于 h, G, Z_t。到达 h_0的似然可能取决于所有 Ξ，但它只贡献一个标量因子，并会在归一化时抵消。由此可得所断言的依赖关系。 □

c. 界定与剩余标架列的重叠

我们将比较这样的混合协议：前 i 次查询使用辅助规则，此后使用物理预言机。由于相邻的两个混合协议在发生差异的查询位置之前具有相同的辅助演化，它们的共同输入具有约化态 σ，因此式（G.5）中的单步误差由 $\mathrm{Tr}(P_t\sigma)$和 $\mathrm{Tr}(P_tG\sigma G^\dagger)$决定。尽管 σ在前 t 个树层级 Z_t上可能有较大的支撑集，投影算子 P_t 与 Z_t 正交，并且只投影到更深处、尚未访问的列上。接下来我们将证明， σ 与这些剩余 Haar 随机列的预期重叠，受经典历史中累积的互信息所界定。

引理 S20 (信息界定了与剩余列的重叠)。 假设(Ξ,H) 具有边缘分布 $\Xi\sim\mu_\Xi$，且满足 $I(\Xi;\ \mathsf{H})\le\mathcal{I}$。令 $t=t(h)\in\{0,\dots,k-2\}$，并令 $\tau(h,G,Z_t)$ 为查询寄存器上的密度矩阵。那么

$$\mathbb{E}\,\mathrm{Tr}(P_t\tau)\le\frac{2(\mathcal{I}+r)}{D_*}. \tag{G.9}$$

特别地，引理 σ 中的辅助状态 *S19* 满足

$$\mathbb{E}\,\mathrm{Tr}(P_t\sigma),\quad \mathbb{E}\,\mathrm{Tr}(P_tG\sigma G^\dagger)\le B_q:=\frac{4(q\log d+M)}{D_*}. \tag{G.10}$$

证明。令 P 表示 (Ξ,H) 的真实联合分布，并引入解耦参考分布 $Q=\mu_\Xi\otimes P_{\mathsf{H}}$，在该分布下，历史 H 与预言机参数 Ξ 相互独立。在 P 下，给定历史 h 通常会使剩余标架列的分布发生偏斜。然而，在 Q 下，给定 (h,G,Z_t) 会固定状态$\tau(h,G,Z_t)$，同时剩余的 $F_\pm$ 列仍按照引理 S17 中的条件 Haar 测度分布。

对于维度为 D 的空间中的秩为 r' 的 Haar 随机投影算子 P'，以及任意固定的单位向量 v，

$$\mathbb{E}\langle v|P'|v\rangle^j=\frac{(r')_j}{(D)_j},\qquad (a)_j=a(a+1)\cdots(a+j-1),\quad (a)_0=1.$$

对于 $D\ge D_*$ 和 $r'\le r$，我们有 $(r')_j/(D)_j\le(r')_j/D_*^j$，因此展开指数级数可得

$$\mathbb{E}e^{(D_*/2)\langle v|P'|v\rangle}\le\sum_{j\ge0}\frac{(r')_j}{2^jj!}=(1-1/2)^{-r'}=2^{r'}\le2^r.$$

由指数函数的凸性可知，将 $|v\rangle\langle v|$ 替换为任意密度矩阵时，同一上界仍然成立；该结论也可推广至两个扇区 $\mathcal{H}_\pm$ 的直和以及根空间（其中 P_t 为零）。因此，在 Q 下对 $(h,\ G,\ Z_t)$ 进行条件化并取平均，可得

$$\mathbb{E}_Q\left[e^{(D_*/2)\,\mathrm{Tr}(P_t\tau)}\right]\le2^r.$$

Next，我们运用相对熵的 Donsker–Varadhan 变分公式，得到

$$\lambda\mathbb{E}_P[X]\le D(P\|Q)+\log\mathbb{E}_Q\left[e^{\lambda X}\right],$$

令 $X=\mathrm{Tr}(P_t\tau)$，且 $\lambda=D_*/2$。由于 $D(P\|Q)=I(\Xi;\mathsf{H})\le\mathcal{I}$，重新排列即可得到式 (G.9)。最后，将式 (G.7) 中的 $\mathcal{I}=2q\log d$ 和 $r=2M-2<2M$ 代入式 (G.9)，分别取 $\tau=\sigma(h,G,Z_t)$ 和 $\tau=G\sigma(h,G,Z_t)G^\dagger$，即可得到式 (G.10)。 □

d. 累积查询误差

现在，我们对所有 q 全局查询时隙中的单次查询替换误差求和，以界定物理输出分布与辅助输出分布之间的全变差距离。

引理 S21 （与辅助过程的比较）。 令 $\mathsf{Out}_{\mathrm{aux}}$ 表示辅助过程的经典输出分布。对于任一符号 $s\in\{\pm1\}$,

$$\mathrm{TV}(\mathsf{Out}_{\theta,s},\mathsf{Out}_{\mathrm{aux}})\le4q\sqrt{B_q}+320q\sqrt{M/d}. \tag{G.11}$$

因此,

$$\mathrm{TV}(\mathsf{Out}_{\theta,+},\mathsf{Out}_{\theta,-})\le8q\sqrt{B_q}+640q\sqrt{M/d}. \tag{G.12}$$

证明。 对于 $i = 0, \ldots, q$，定义第 i 个混合过程：在前 i 个全局查询时隙中遵循辅助规则，并在所有后续时隙中查询物理预言机 $U_{\theta,s}$(Ξ)。因此，第 0 个混合过程是物理协议，而第q个混合过程是辅助过程。

考虑第 $(i-1)$ 个和第 i 个混合过程。在槽位 i 之前，它们的演化完全相同，此时它们的共同状态就是辅助过程的状态；在槽位 i 之后，它们执行完全相同的条件操作。将 Ξ 和经典历史保留为经典寄存器后，槽位 i之后的演化是一个与参数无关的量子信道，因此会收缩迹距离。

为界定槽位 i引入的迹距离，固定一个活动历史 h （其中 $t = t(h) \le L - 1 \le k - 2$），并将联合系统—辅助系统输入态 $|\phi(\Xi,\ h)\rangle$ 纯化，使其在查询寄存器上的约化态为 $\sigma(h,\ G,\ Z_t)$。根据 Fuchs–van de Graaf，两个混合过程在查询后的状态之间的迹距离有上界，即欧几里得范数$\|(U_{\theta,\ s} - U^{[t+1]})\phi\|$。根据引理 S18，有

$$\|(U_{\theta,s} - U^{[t+1]})\phi\| \le 2\sqrt{\mathrm{Tr}(P_t\sigma)} + 2\sqrt{\mathrm{Tr}(P_t G\sigma G^\dagger)} + 32\delta_{\theta,s}.$$

对 (Ξ, H) 取期望，并结合 Jensen 不等式与式（G.10），两个投影算子项的总贡献至多为 $4\sqrt{B_q}$。对于重叠项，由于 Ξ 的约化态为 μ_Ξ，式（G.6）给出

$$32\,\mathbb{E}_{\mu_\Xi}[\delta_{\theta,s}] \le 320\sqrt{M/d}.$$

因此，替换 i次查询，最终输出分布的全变差距离至多改变 $4\sqrt{B_q} + 320\sqrt{M/d}$ 。通过三角不等式，对 $i = 1$、……、q 求和，即可得到公式 (G.11)。由于$\mathsf{Out}_{\mathrm{aux}}$ 与 s无关，三角不等式给出公式 (G.12)。 □

定理*S4*的证明。 公式 (G.1中的精确关联器值由引理S17证明。为了界定 $s = +1$ 与 $s = -1$对应的输出分布之间的全变差距离，我们将公式 (G.10) 中 B_q 的表达式代入公式 (G.12)：

$$\begin{aligned}
\mathrm{TV}(\mathsf{Out}_{\theta,+}, \mathsf{Out}_{\theta,-}) &\le 8q\sqrt{B_q} + 640q\sqrt{\frac{M}{d}} \\
&\le 16q\sqrt{\frac{q\log d + M}{D_*}} + 640q\sqrt{\frac{M}{d}} \\
&\le 32\sqrt{\frac{q^3\log d}{d}} + 672q\sqrt{\frac{M}{d}},
\end{aligned} \tag{G.13}$$

其中，最后的不等 式利用了公式 ($D_* \ge d/4$ G.4) 中的$\sqrt{a+b} \le \sqrt{a} + \sqrt{b}$。这就证明了公式 (G.2).

要将公式 (G.2) 转化为查询下界，注意到由公式 (G.1) 可知， $|C(U)| = 3/4$和 $|F_\theta(U)| = 3/8$。因此，对 $C(U)$ 的估计值 $\widehat{C}$若加性误差至多为 $1/3 < 3/4$，便可通过符号 $\mathrm{Re}(i^{-|\theta|}\widehat{C})$ 唯一确定 s。同样，对 $F_\theta(U)$ 的估计值 F_θ若加性误差不超过 $1/3 < 3/8$，便可通过符号 Re F_θ 确定 s。任何在 $\mathrm{supp}\,\mathcal{D}_{\theta,+} \cup \mathrm{supp}\,\mathcal{D}_{\theta,-}$ 中的每个预言机上均以至少 $2/3$ 的概率成功的协议，因此都能以至少 $2/3$ 的成功概率区分 $\mathcal{D}_{\theta,+}$ 与 $\mathcal{D}_{\theta,-}$，这要求 $\mathrm{TV}(\mathsf{Out}_{\theta,+}, \mathsf{Out}_{\theta,-}) \ge \frac{1}{3}$。另一方面，如果 q 严格小于公式 (G.3) 右侧的值，那么公式 (G.2) 将给出 $\mathrm{TV}(\mathsf{Out}_{\theta,+}, \mathsf{Out}_{\theta,-}) < 32(4096)$ ——— – $^{-3/2} + \frac{672}{4096} = \frac{672.125}{4096} < \frac{1}{3}$，这就产生了矛盾。由此得到公式 (G.3)。 □

3. 构造耦合的 Haar 补全

本小节证明引理 S18。我们的目标是在共同概率空间上耦合完整预言机 $U_{\theta,s}$ 和前缀预言机 $U^{[j]}$，使得 $U_{\theta,s}$ 和 $U^{[t+1]}$ 对任何支撑集位于较深树层级 Ran P_t 之外的状态，其作用几乎完全相同。由于 $U_{\theta,s}$ 和 $U^{[t+1]}$ 规定的树转换数量不同，它们的随机补全作用于维数不同的子空间，因此无法仅通过共用一个分块矩阵来进行耦合。我们改为从单个 Haar 酉矩阵 $G \sim \mathrm{Haar}(\mathrm{U}(d))$ 生成两个酉算子：对于任何给定的输入与输出标架 (V, W)，我们将 G 右乘一个校正酉矩阵 R，以确保满足 $GRV = W$。在高维（$d \gg M$）下，子空间 Ran V 和 Ran$(G^\dagger W)$ 几乎正交，因此 $R - I$ 近似为由 V 和 W 的各列构成的秩一项之和。因此，计算差值 $U_{\theta,s} - U^{[t+1]}$时，共同的前 $t+1$ 个树层级所对应的贡献会相互抵消，只留下支撑集位于较深层级 Ran P_t 的误差，正如公式 (G.5) 中所述。

引理的证明 *S18*。步骤 *1*：从共享的 *Haar* 酉矩阵进行精确酉补全。 设 V， W： $\mathbb{C}^m \to \mathbb{C}^d$ 为等距映射（ $V^\dagger V = W^\dagger W = I_m$），且满足 $2m \le d$。完整树框架（$2p = 4M - 4 \le d$）以及所有前缀子框架均满足此条件。给定一个酉算子 $G \sim \mathrm{Haar}(\mathrm{U}(d))$，我们要寻找一个形如 $\mathcal{U} = GR$ 的酉算子，使其满足 $\mathcal{U}V = W$。将 G 移至等式右侧后，该条件等价于要求 R 将框架 V 映射到拉回的框架 $B := G^\dagger W$：

$$RV = B.$$

为了构造这样的酉算子 ary R 显式地，定义差分框架 X： $\mathbb{C}^m \to \mathbb{C}^d$ 以及 $m \times m$ 矩阵 A 为

$$X = V - B, \qquad A = I_m - B^\dagger V = X^\dagger V.$$

由于 G 服从 Haar 分布且 $2m \le d$，子空间 $\mathrm{Ran}\, V$ 与 $\mathrm{Ran}\, B$ 几乎必然没有非零交集，因此 $\|V^\dagger B\| < 1$ 和 A 几乎必然可逆。在这个测度为一事件上，定义

$$R(V,B) = I_d - X A^{-1} X^\dagger.$$

让我们验证 $R = R(V,\ B)$ 将 V映射到 B 且为酉算子。首先，利用 $X^\dagger V = A$，我们有

$$RV = V - X A^{-1}(X^\dagger V) = V - X = B.$$

其次，由于 $V^\dagger V = B^\dagger B = I_m$，展开 $X^\dagger X = (V-B)^\dagger (V-B)$ 得到

$$X^\dagger X = 2I_m - V^\dagger B - B^\dagger V = A + A^\dagger.$$

利用这一恒等式，我们计算

$$R^\dagger R = (I_d - X(A^\dagger)^{-1}X^\dagger)(I_d - X A^{-1}X^\dagger) = I_d + X(A^\dagger)^{-1}(X^\dagger X - A - A^\dagger)A^{-1}X^\dagger = I_d,$$

从而确认 R是酉算子。因此，令 $\mathcal{U}(V,\ W;\ G) := GR(V,\ G^\dagger W)$，即可得到一个实现指定跃迁 $V \mapsto W$的酉算子。

现在我们验证，在给定 $(V,\ W)$ 的条件下， $\mathcal{U}(V,\ W;\ G)$ 从 $(\mathrm{Ran}\ V)^\perp$ 到 $(\mathrm{Ran}\ W)^\perp$ 的作用服从 Haar 分布。设 $K \in \mathrm{U}(d)$ 是任意一个在 $\mathrm{Ran}\ W$ 上作用为恒等算子（因此 $KW = W$）、并在 $(\mathrm{Ran}\ W)^\perp$ 上作用为任意酉算子的酉算子。在左平移 $G \mapsto KG$ 下， $G \sim \mathrm{Haar}(\mathrm{U}(d))$ 的分布保持不变。此外，由于 $G^\dagger K^\dagger W = G^\dagger W = B$，校正酉矩阵 $R(V,\ G^\dagger W)$ 不变，因此 $\mathcal{U}$变换为

$$\mathcal{U}(V,W;KG) = KG\, R(V, G^\dagger K^\dagger W) = K\,\mathcal{U}(V,W;G).$$

因此， $\mathcal{U}(V,\ W;\ G)$ 的条件分布在所有作用于 $(\mathrm{Ran}\ W)^\perp$ 的酉算子 K 下均保持左不变，这意味着它从 $(\mathrm{Ran}\ V)^\perp$ 到 $(\mathrm{Ran}\ W)^\perp$ 的限制服从 Haar 分布。将这一构造应用于完整标架以及每个前缀，并使用同一个随机矩阵 G，即可定义耦合预言机：

$$U_{\theta,s} = \mathcal{U}(V_F, W_{F,\theta,s}; G), \qquad U^{[j]} = \mathcal{U}(V^{[j]}, W^{[j]}; G), \quad 1 \le j < k.$$

由于前缀框架（$V^{[j]}$、 $W^{[j]}$）仅取决于前 j个树层级 Z_j，因此前缀预言机 $U^{[j]}$完全由（Z_j、 G）确定。

步骤 *2*：校正旋转的线性化。 在公式 $R(V$、 $B) = I_d - X A^{-1} X^\dagger$ 中， $m \times m$ 逆矩阵 $A^{-1} = (I_m - B^\dagger V)^{-1}$ 将 X 的不同列耦合起来。然而，当 V和 B近似正交时， A接近 I_m。将 A^{-1} 替换为 I_m 可得到简化的算子

$$R_0(V,B) := I_d - XX^\dagger = I_d - VV^\dagger - BB^\dagger + VB^\dagger + BV^\dagger.$$

我们根据标架重叠 δ 对这一近似的误差进行了界定：$= \|V^\dagger B\| = \|I_m - A\|$:

$$\|R(V,B) - R_0(V,B)\| \le 16\|V^\dagger B\|. \tag{G.14}$$

为证明式（G.14），首先注意到 $\|X\| \le \|V\| + \|B\| = 2$。如果 $\delta \le 1/2$，那么 $A^{-1} =$ （$I_m - B^\dagger V$）$^{-1} = \sum_{t\ge 0}$ （$B^\dagger V$）^{t}给出 $\|A^{-1} - I_m\| \le \delta/$（$1-\delta$） $\le 2\delta$，因此

$$\|R(V,B) - R_0(V,B)\| = \|X(A^{-1} - I_m)X^\dagger\| \le \|X\|^2 \|A^{-1} - I_m\| \le 8\delta.$$

如果改为 $\delta > 1/2$，则由三角不等式可得平凡的界

$$\|R(V,B) - R_0(V,B)\| \le \|R(V,B)\| + \|I_d\| + \|X\|^2 \le 1 + 1 + 4 = 6 < 16\delta.$$

因此，式（G.14）对所有 $\delta \ge 0$ 均成立。

步骤 *3*：消去共享前缀列。现在，对于固定的 $0 \le t \le k-2$，我们比较 $U_{\theta,s}$ 和 $U^{[t+1]}$。令 $j = t+1$，并将完整标架划分为深度为 j 的前缀列（对应长度为 $|w| \le t$ 的输入字）和其余更深层的列（对应长度为 $t+1 \le |w| \le k-1$ 的输入字）：

$$V_F = \begin{pmatrix} V^{[j]} & V_{\mathrm{rem}} \end{pmatrix}, \qquad W_{F,\theta,s} = \begin{pmatrix} W^{[j]} & W_{\mathrm{rem}} \end{pmatrix}.$$

相应地，差分框架 $X_F := V_F - G^\dagger W_{F,\theta,s}$ 分成两个列块：

$$X_F = \begin{pmatrix} X^{[j]} & X_{\mathrm{rem}} \end{pmatrix}, \qquad X^{[j]} := V^{[j]} - G^\dagger W^{[j]}, \qquad X_{\mathrm{rem}} := V_{\mathrm{rem}} - G^\dagger W_{\mathrm{rem}}.$$

由于 $X_F X_F^\dagger = X^{[j]}(X^{[j]})^\dagger + X_{\mathrm{rem}} X_{\mathrm{rem}}^\dagger$，在计算两个线性化旋转之差时，共享前缀列会相互抵消：

$$R_0(V_F, G^\dagger W_{F,\theta,s}) - R_0(V^{[j]}, G^\dagger W^{[j]}) = -X_{\mathrm{rem}} X_{\mathrm{rem}}^\dagger. \tag{G.15}$$

让我们界定 $X_{\mathrm{rem}} X_{\mathrm{rem}}^\dagger$ 对任意向量 ϕ 的作用。由于 V_{rem} 和 W_{rem} 是等距映射，我们有 $\|X_{\mathrm{rem}}\| \le \|V_{\mathrm{rem}}\| + \|G^\dagger W_{\mathrm{rem}}\| = 2$，从而得到

$$\|X_{\mathrm{rem}} X_{\mathrm{rem}}^\dagger \phi\| \le \|X_{\mathrm{rem}}\| \|X_{\mathrm{rem}}^\dagger \phi\| \le 2\big(\|V_{\mathrm{rem}}^\dagger \phi\| + \|W_{\mathrm{rem}}^\dagger G \phi\|\big).$$

根据引理 S17，V_{rem} 和 W_{rem} 的列都是正交归一向量，且完全位于 值域 P_t 内。因此 $V_{\mathrm{rem}} V^\dagger{}_{\text{余}} \preceq P_t$ 和 $W_{\mathrm{rem}} W^\dagger{}_{\text{余}} \preceq P_t$，这意味着 $\|V^\dagger{}_{\text{余}} \phi\| = \|V_{\mathrm{rem}} V^\dagger{}_{\text{余}} \phi\| \le \|P_t \phi\|$，同理 $\|W_{\mathrm{rem}}^\dagger G \phi\| \le \|P_t G \phi\|$。将这些界与公式 (G.15) 结合，得到

$$\|\big(R_0(V_F, G^\dagger W_{F,\theta,s}) - R_0(V^{[j]}, G^\dagger W^{[j]})\big)\phi\| \le 2\big(\|P_t \phi\| + \|P_t G \phi\|\big).$$

要从线性化旋转 R_0 回到精确的酉算子 $U_{\theta,s} = GR(V_F, G^\dagger W_{F,\theta,s})$ 和 $U^{[j]} = GR(V^{[j]}, G^\dagger W^{[j]})$，注意到 $(V^{[j]})^\dagger G^\dagger W^{[j]}$ 是 $V_F^\dagger G^\dagger W_{F,\theta,s}$ 的子矩阵，因此其算子范数也不超过 $\delta_{\theta,s} = \|V_F^\dagger G^\dagger W_{F,\theta,s}\|$。对 $R(V_F, G^\dagger W_{F,\theta,s})$ 和 $R(V^{[j]}, G^\dagger W^{[j]})$ 分别应用公式 (G.14)，最多会增加 $2 \times 16\delta_{\theta,s}\|\phi\| = 32\delta_{\theta,s}\|\phi\|$ 的误差。左乘酉算子 G 不会改变范数，由此得到公式 (G.5)。当 ϕ 是系统–辅助系统联合向量时，将所有算子与辅助系统恒等算子作张量积，推导过程不变。

步骤 *4*：界定期望框架重叠。接下来只需通过界定 $\mathbb{E}_G[\delta_{\theta,s} \mid F]$ 来证明式（G.6）。固定框架 F，因此 V_F、$W_{F,\theta,s}$ 均为固定的等距映射。选取单位球面 $\mathbb{C}^p$ 上一个基数为 $|\mathcal{N}| \le 9^{2p}$ 的 $(1/4)$-网 $\mathcal{N}$。对于任意单位向量 a、$b \in \mathbb{C}^p$，选取 a_0、$b_0 \in \mathcal{N}$，使得 $\|a - a_0\| \le 1/4$ 且 $\|b - b_0\| \le 1/4$，可得

$$|a^\dagger V_F^\dagger G^\dagger W_{F,\theta,s} b| \le |a_0^\dagger V_F^\dagger G^\dagger W_{F,\theta,s} b_0| + \big(\|a - a_0\| + \|b - b_0\|\big)\delta_{\theta,s} \le \max_{a_0,b_0 \in \mathcal{N}} |a_0^\dagger V_F^\dagger G^\dagger W_{F,\theta,s} b_0| + \frac{1}{2}\delta_{\theta,s}.$$

对单位向量 a、b 取上确界并重新整理，得到

$$\delta_{\theta,s} \le 2 \max_{a,b \in \mathcal{N}} |a^\dagger V_F^\dagger G^\dagger W_{F,\theta,s} b|.$$

对于每一对固定的 a、$b \in \mathcal{N}$，$V_F a$ 和 $W_{F,\theta,s} b$ 都是 $\mathbb{C}^d$ 中的固定单位向量。在 $G \sim \mathrm{Haar}(\mathrm{U}(d))$ 下，随机向量 $G^\dagger(W_{F,\theta,s} b)$ 在 $\mathbb{C}^d$ 的单位球面上均匀分布，因此重叠平方 $|(V_F a)^\dagger G^\dagger (W_{F,\theta,s} b)|^2$ 服从 $\mathrm{Beta}(1, d-1)$ 分布，其尾概率为

$$\Pr_G\big(|a^\dagger V_F^\dagger G^\dagger W_{F,\theta,s} b| \ge u \;\big|\; F\big) = (1-u^2)^{d-1} \le e^{-(d-1)u^2}, \qquad 0 \le u \le 1.$$

对所有 $|\mathcal{N}|^2 \le 9^{4p}$ 对取并集界，得到

$$\Pr_G(\delta_{\theta,s} \ge 2u \mid F) \le \min\big\{1,\, e^{4p \log 9 - (d-1)u^2}\big\}, \qquad 0 \le u \le 1.$$

最后，我们对该尾界进行积分，以控制 $\delta_{\theta,s}$ 的二阶矩：

$$\begin{aligned} \mathbb{E}_G[\delta_{\theta,s}^2 \mid F] &= 4 \int_0^4 \Pr_G(\delta_{\theta,s} \ge 2\sqrt{v} \mid F)\, dv \\ &\le 4 \int_0^\infty \min\{1, e^{4p \log 9 - (d-1)v}\}\, dv \\ &\le 4u_0^2 + 4 \int_{u_0^2}^\infty e^{4p \log 9 - (d-1)s}\, ds \le \frac{4(4p \log 9 + 1)}{d-1} \le \frac{100M}{d}, \end{aligned}$$

其中 $u_0^2 := 4p \log 9/(d-1)$，最后一个不等式用到了 $p = 2M - 2$ 和 $d \ge 4M \ge 16$。根据柯西–施瓦茨不等式，$\mathbb{E}_G[\delta_{\theta,s} \mid F] \le \big(\mathbb{E}_G[\delta_{\theta,s}^2 \mid F]\big)^{1/2} \le 10\sqrt{M/d}$，证明完毕。 □

附录 H：单辅助量子比特同时估计嵌套关联函数

在本附录中，我们陈述算法1 的正式性能保证，并给出定理1中上界的完整证明。

定理 S5 （算法 1的性能保证）。 设 $k \geq 1$ 和 $M = 2^k$。对于任意酉算子 U、任意一系列已知的二值可观测量 O_1、. . .、 O_{k+1}、任意一系列整数观测时间 $0 \leq t_1 \leq \cdots \leq t_{k+1} = T$ 、 $\widehat{\ }$ 以及任意可重复制备的量子态 ρ，算法 *1* 会生成估计值 $\{F_\sigma\}_{\sigma\in\{0,1\}^k}$ ，用于估计式 （1）中的嵌套关联函数，并满足

$$\Pr\left(\max_{\sigma\in\{0,1\}^k} |\widehat{F}_\sigma - F_\sigma(U)| \leq \varepsilon\right) \geq 1-\delta$$

对于任意 $\varepsilon > 0$ 和 $0 < \delta < 1$，使用一个辅助量子比特和一个包含

$$N = \left\lceil \varepsilon^{-2} \log \frac{2M}{\delta} \right\rceil = \left\lceil \varepsilon^{-2}\big(k + 1 + \log(1/\delta)\big) \right\rceil \tag{H.1}$$

次实验重复的共享数据集，总共对应于对 U 进行 $q = TN$ 次正向查询。

证明。 在算法 1的每次重复中，给定固定路径字符串 $b \in \{0,1\}^k$时，探针量子比特的 $|0\rangle$ 和 $|1\rangle$ 分支会经历式 W_b 和 $W_{\bar{b}}$ 中定义的有效演化过程（式（2）和式（F.4））。在时间 $T = t_{k+1}$进行最终测量之前，探针—系统联合态为

$$\Omega_b = \frac{1}{2}\begin{pmatrix} W_b\rho W_b^\dagger & W_b\rho W_{\bar{b}}^\dagger \\ W_{\bar{b}}\rho W_b^\dagger & W_{\bar{b}}\rho W_{\bar{b}}^\dagger \end{pmatrix}. \tag{H.2}$$

在探针上测量（结果为 $a \in \{\pm 1\}$）$/\sqrt{2}$，并在系统上测量（结果为 $x \in \{\pm 1\}$） O_{k+1}，得到乘积 $ax \in \{\pm 1\}$，其条件期望值为

$$\mathbb{E}[ax \mid b, u] = \mathrm{Tr}\left[\left(\frac{X + uY}{\sqrt{2}} \otimes O_{k+1}\right)\Omega_b\right] = \frac{\mathrm{Re}\, Q_b - u\,\mathrm{Im}\, Q_b}{\sqrt{2}}, \tag{H.3}$$

其中 $Q_b = \mathrm{Tr}(O_{k+1}W_b\rho W_{\bar{b}}^\dagger)$。对独立的公平符号 $u \in \{\pm 1\}$ 取平均，得到 es

$$\mathbb{E}[ax \mid b] = \frac{\mathrm{Re}\, Q_b}{\sqrt{2}}, \qquad \mathbb{E}[uax \mid b] = -\frac{\mathrm{Im}\, Q_b}{\sqrt{2}}.$$

因此，单次快照 $\widehat{Q} = \sqrt{2}\, ax(1 - iu)$ 是在给定 $\bar{b}$ 的条件下对 Q_b 的无偏估计量，即 $\frown\mathbb{E}[Q \mid b] = Q_b$。

对于每个目标模式 $\sigma \in \{0,1\}^k$，令

$$T_\sigma = \frac{(-1)^{\sigma\cdot b}}{2}\,\mathrm{Re}\Big(i^{|\sigma|}\widehat{Q}\Big) \tag{H.4}$$

表示估计量中的单次贡献 $\widehat{F}_\sigma = \frac{1}{N}\sum_{r=1}^N T_\sigma^{(r)}$，它出现在算法1中。对于固定的 b，对 u、a、x 取条件期望，得到

$$\mathbb{E}[T_\sigma \mid b] = \frac{(-1)^{\sigma\cdot b}}{2}\,\mathrm{Re}\Big(i^{|\sigma|}Q_b\Big).$$

对均匀抽取的路径求平均 $b \sim \{0,1\}^k$，并应用引理 S12中的互补路径对偶性，得到

$$\mathbb{E}T_\sigma = \frac{1}{2}\,\mathrm{Re}\Big(i^{|\sigma|}\mathbb{E}_b\big[(-1)^{\sigma\cdot b}Q_b\big]\Big) = F_\sigma(U),$$

这里用到了 $F_\sigma(U)$ 为实数这一事实。

最后，为了界定样本复杂度，注意对于 (b,u,a,x) 的每一种可能取值以及每个 $\sigma\in\{0,1\}^k$，$\mathrm{Re}(i^{|\sigma|}\widehat{Q})=\sqrt{2}\,ax$ 在 $|\sigma|$ 为偶数时成立，而在 $|\sigma|$ 为奇数时 $\pm\sqrt{2}\,uax$ 成立。因此，每个单次测量变量 T_σ 的取值都在 $\{-1/\sqrt{2},+1/\sqrt{2}\}$ 内，这是一个宽度为 $\sqrt{2}$ 的有界区间。根据霍夫丁不等式，对于每个固定的 σ，

$$\Pr\Big(|\widehat{F}_\sigma - F_\sigma(U)|>\varepsilon\Big)\le 2\exp(-N\varepsilon^2).$$

对所有 $M=2^k$ 括号模式 $\sigma\in\{0,1\}^k$ 应用并集界，可得

$$\Pr\Big(\max_{\sigma\in\{0,1\}^k}|\widehat{F}_\sigma - F_\sigma(U)|>\varepsilon\Big)\le 2Me^{-N\varepsilon^2}. \tag{H.5}$$

令右侧不超过 δ，取 $N=\lceil\varepsilon^{-2}\log(2M/\delta)\rceil$即可满足条件。由于算法 1的每次运行都会对 T执行 U次正向查询，因此总查询复杂度为 $q=TN$。 □

附录 I：单个嵌套关联函数的无辅助比特估计

这里我们介绍一种无需辅助系统的实现方案，用于实现参考文献 [34, 35, 37], 中的序贯测量方案，从而高效估计任意一个 $F_\sigma(U)$，该关联函数在数据收集前已确定。利用已知的二值可观测量 $O_1,\dots,O_{k+1}$、整数观测时间 $0\le t_1\le\cdots\le t_{k+1}=T$以及可重复制备的量子态 ρ（在式 (1) 中指定），针对给定括号模式 $\sigma\in\{0,1\}^k$ 的具体过程详见算法 2。每次实验运行需要对 T 执行 U 次正向查询，且不需要辅助量子存储器，由此产生一个有界的单次随机变量

$$Z_\sigma=\frac{x}{2}\prod_{j=1}^{k}a_j\in\left\{-\frac{1}{2},+\frac{1}{2}\right\}. \tag{I.1}$$

算法 2 无辅助量子比特估计单个嵌套关联函数

需要：初始态 ρ、已知可观测量 O_1、...、O_{k+1}、观测时间 $0\le t_1\le\cdots\le t_{k+1}$、目标括号模式$\sigma\in\{0,1\}^k$和重复次数 N。1：对于 $r=1$、...、N，执行 2：将系统制备为 ρ，并在 U 作用下演化 t_1 步。▷初始化 3：对于 $j=1$、...、k，执行▷应用特定于模式的干预 4：如果 $\sigma_j=0$，则 5：对系统上的 O_j 进行投影测量，得到测量结果 $a_j\in\{\pm1\}$。6：否则，如果 $\sigma_j=1$，则 7：抽取一个公平符号 $a_j\in\{\pm1\}$，并施加酉旋转 $e^{-ia_j\pi O_j/4}$。8：结束如果 9：在 U 作用下将系统演化 $t_{j+1}-t_j$ 步。10：结束循环 11：测量系统上的 O_{k+1}，得到测量结果 $x\in\{\pm1\}$。12：存储 $Z_\sigma^{(r)}=\frac{x}{2}\prod_{j=1}^{k}a_j$。13：结束循环 14：返回 $\widehat{F}_\sigma=\frac{1}{N}\sum_{r=1}^{N}Z_\sigma^{(r)}$。

定理 S6（无辅助比特估计单个嵌套关联函数）。对于每个固定的 $\sigma\in\{0,1\}^k$、每个 $\varepsilon>0$以及每个 $0<\delta<1$，算法 2 实现

$$\Pr\Big(|\widehat{F}_\sigma - F_\sigma(U)|\le\varepsilon\Big)\ge 1-\delta$$

对于每个酉算子 U、上述指定的每个已知二值可观测量序列和整数观测时间，以及每个可重复制备的输入态 ρ，在不使用辅助量子存储器的情况下，并

$$q=T\left\lceil\frac{\log(2/\delta)}{2\varepsilon^2}\right\rceil \tag{I.2}$$

对 U 进行正向查询。

证明。对于二值可观测量 O，在 $\sigma_j = b \in \{0,1\}$ 和测量结果/符号 $a \in \{\pm 1\}$ 条件下的中间干预由以下 Kraus 算子描述：

$$K_a^{(0)}(O) = \frac{I + aO}{2}, \qquad K_a^{(1)}(O) = \frac{I - iaO}{2} = \frac{1}{\sqrt{2}} e^{-ia\pi O/4}. \tag{I.3}$$

对于任意可观测量 B，直接展开可知，按 a 对测量结果加权会在海森堡绘景中生成相应的括号：

$$\mathcal{B}_O^{(b)}(B) := \sum_{a=\pm 1} a K_a^{(b)}(O)^\dagger B K_a^{(b)}(O) = \frac{[B, O]_b}{2i^b}. \tag{I.4}$$

记作 $A_j = (U^{t_j})^\dagger O_j U^{t_j}$，时刻 t_j 的干预在海森堡绘景中作用 Kraus 算子 $K^{(\sigma_j)a_j}(A_j)$。将带符号的期望值从 A_{k+1} 的最终测量向后传播，得到

$$\mathbb{E} Z_\sigma = \frac{1}{2} \operatorname{Tr}\Big[\big(\mathcal{B}_{A_1}^{(\sigma_1)} \circ \cdots \circ \mathcal{B}_{A_k}^{(\sigma_k)}\big)(A_{k+1})\, \rho \Big]. \tag{I.5}$$

每个超算子 $\mathcal{B}^{(\sigma_j)\, A_j}$ 贡献括号 $[\cdot, A_j]_{\sigma_j}$，并带有因子 $1/(2i^{\sigma_j})$。再结合总前因子 $1/2$，即可还原式（ $2^{-(k+1)}(-i)^{|\sigma|}$ ）中的精确嵌套括号和归一化 1），从而确认

$$\mathbb{E} Z_\sigma = F_\sigma(U). \tag{I.6}$$

由于每个样本 $Z_\sigma^{(r)}$ 的取值都在 $\{-1/2, +1/2\}$ 中，霍夫丁不等式给出

$$\Pr\Big(|\widehat{F}_\sigma - F_\sigma(U)| > \varepsilon \Big) \le 2 \exp(-2N\varepsilon^2). \tag{I.7}$$

令 $N = \lceil \log(2/\delta)/(2\varepsilon^2) \rceil$ 即可保证失败概率至多为 δ，再乘以每次运行的 T 次正向查询，便得到式（I.2）。

□

附录 J：单辅助量子比特多时刻关联函数估计

为完整起见，我们用自己的记号重新表述 Pedernales 等人提出的单辅助量子比特干涉协议 [32]，并确定其前向查询复杂度。设 U 为一个未知酉算子，ρ 为一个可重复制备的初始态，且O_1、……、O_{k+1}为满足 $O_j = O_j^\dagger$和 $O_j^2 = I$的已知二值可观测量，其中 $k \ge 1$。对于整数观测时间$0 \le t_1 \le \cdots \le t_{k+1} = T$，记 $O_j(t_j) = (U^{t_j})^\dagger O_j U^{t_j}$。目标量为

$$C(U) = \operatorname{Tr}[O_{k+1}(t_{k+1}) \cdots O_1(t_1) \rho] = Q_{\mathbf{1}}, \tag{J.1}$$

其中 $\mathbf{1} = (1、\ldots\ldots、1)$。在方程（2）的轨迹表示法中，

$$\begin{aligned} W_{\mathbf{0}} &= U^T, \\ W_{\mathbf{1}} &= U^{T - t_k} O_k \cdots U^{t_2 - t_1} O_1 U^{t_1}, \end{aligned} \tag{J.2}$$

因此 $C(U) = \operatorname{Tr}(O_{k+1} W_{\mathbf{1}} \rho W_{\mathbf{0}}^\dagger)$。每次运行都会对这两条轨迹进行干涉，并与探针自旋分量联合测量最终可观测量 O_{k+1}。算法 3 通过每次重复使用 T 次对 U 的正向查询来实现这一过程。

定理 S7 (单辅助量子比特对一般多时刻关联函数的估计**)。** 对于任意酉算子 U、可重复制备的量子态 ρ、已知二分观测量序列 O_1，……，O_{k+1}以及整数观测时间 $0 \le t_1 \le \cdots \le t_{k+1} = T$，算法 3 会生成对式 (J.1)中复数关联函数的无偏估计 C。对于任意 $\varepsilon > 0$ 和 $0 < \delta < 1$，选择

$$N = \left\lceil 8 \varepsilon^{-2} \log \frac{4}{\delta} \right\rceil \tag{J.3}$$

确保

$$\Pr\Big(|\widehat{C} - C(U)| \le \varepsilon \Big) \ge 1 - \delta.$$

算法 3 使用一个额外量子比特估计一般多时刻关联函数

要求：初始态 ρ、已知可观测量 O_1、…、O_{k+1}、观测时间 $0 \le t_1 \le \cdots \le t_{k+1}$，以及重复次数 N。**1**：对于 $r = 1$、…、N，执行 **2**：将系统制备为 ρ，并将探针制备为 $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$。**3**：随机选取一个独立的公平符号 $u_r \in \{\pm 1\}$。**4**：在 U 作用下演化系统 t_1 步。**5**：对于 $j = 1$、…、k，执行 **6**：应用 $|0\rangle\langle 0| \otimes O_j + |1\rangle\langle 1| \otimes I$。**7**：在 U 作用下演化系统 $t_{j+1} - t_j$ 步。**8**：结束循环 **9**：在探针上测量 $(X + u_r Y)/\sqrt{2}$，得到 $a_r \in \{\pm 1\}$。**10**：在系统上测量 O_{k+1}，得到 $x_r \in \{\pm 1\}$。**11**：存储 $\widehat{Q}_r = \sqrt{2}\, a_r x_r (1 - i u_r)$。**12**：结束循环 **13**：返回 $\widehat{C} = \dfrac{1}{N} \sum_{r=1}^{N} \widehat{Q}_r$。 ▷ Fix $b = \mathbf{1}$

该协议使用一个辅助量子比特，总共进行

$$q = TN = T \left\lceil 8\varepsilon^{-2} \log \frac{4}{\delta} \right\rceil \tag{J.4}$$

次正向查询，查询对象为 U。

证明。首先，对海森堡演化进行望远镜求和可得

$$W_{\mathbf{0}}^{\dagger} O_{k+1} W_{\mathbf{1}} = O_{k+1}(t_{k+1}) \cdots O_1(t_1),$$

这验证了恒等算子 $C(U) = Q_{\mathbf{1}}$。算法 3 中的受控插入 $W_{\mathbf{1}}$ 作用于 $|0\rangle$ 分支，并$W_{\mathbf{0}}$ 作用于 $|1\rangle$ 分支。因此，对于任意输入密度算符 ρ，最终测量之前的探针—系统联合态为

$$\Omega_{\mathbf{1}} = \frac{1}{2} \begin{pmatrix} W_{\mathbf{1}} \rho W_{\mathbf{1}}^{\dagger} & W_{\mathbf{1}} \rho W_{\mathbf{0}}^{\dagger} \\ W_{\mathbf{0}} \rho W_{\mathbf{1}}^{\dagger} & W_{\mathbf{0}} \rho W_{\mathbf{0}}^{\dagger} \end{pmatrix}. \tag{J.5}$$

因此，两个测量结果的乘积满足

$$\begin{aligned} \mathbb{E}[ax \mid u] &= \operatorname{Tr}\left[\left(\frac{X + uY}{\sqrt{2}} \otimes O_{k+1} \right) \Omega_{\mathbf{1}} \right] \\ &= \frac{\operatorname{Re} C(U) - u \operatorname{Im} C(U)}{\sqrt{2}}. \end{aligned} \tag{J.6}$$

对公平符号 u 取平均可得

$$\mathbb{E}[ax] = \frac{\operatorname{Re} C(U)}{\sqrt{2}}, \qquad \mathbb{E}[uax] = -\frac{\operatorname{Im} C(U)}{\sqrt{2}}.$$

因此，每个快照 $\widehat{Q} = \sqrt{2}\, ax(1 - iu)$ 都满足 $\mathbb{E}\widehat{Q} = C(U)$，这证明了 $\widehat{C}$ 的无偏性。

实部和虚部分量 $\widehat{Q}$ 的取值均在 $\{-\sqrt{2}, +\sqrt{2}\}$ 中。对它们的样本均值应用霍夫丁不等式，将每个误差设为 $\varepsilon/\sqrt{2}$，再利用并集界可得

$$\Pr\left(|\widehat{C} - C(U)| > \varepsilon \right) \le 4 \exp(-N\varepsilon^2/8). \tag{J.7}$$

式 (J.3中的选择使该概率至多为 δ。每次重复使用

$$t_1 + \sum_{j=1}^{k} (t_{j+1} - t_j) = T$$

正向查询，从而建立方程（J.4）。 □

附录 K：数值实验的详细信息

本附录进一步介绍图 3 所示数值实验的细节。我们首先明确模型，并推导探针信号关于嵌套关联函数的展开。随后，我们详细说明算法 1 和 2 的实现，以及数据分析流程。

1. 模型

我们考虑 一个由 $n = 10$ 量子比特组成的链（$d = 2^{10}$），其哈密顿量和初始态由下式给出

$$H = \sum_{i=1}^{9} Z_i Z_{i+1} + 1.05 \sum_{i=1}^{10} X_i + 0.5 \sum_{i=1}^{10} Z_i, \qquad \rho = \frac{I + X_1}{d}. \tag{K.1}$$

因此，量子比特 1 的初始极化方向为 x，而其余量子比特处于最大混合态。幺正演化为$U = e^{-iH\Delta}$，其中 $\Delta = 0.4$。观测时间为

$$(t_1, \ldots, t_9) = (0, 1, 3, 4, 5, 7, 9, 10, 12). \tag{K.2}$$

因此，连续两次探针–系统接触之间的演化为 $U_{t_j,\ t_{j+1}} \coloneqq e^{-iH\Delta(t_{j+1}-t_j)}$。

嵌套关联函数 $\{F_\sigma\}_\sigma$ 在式（1中使用边界可观测量 $O_j = Z_1$定义。这些选择给出$k = 8$ 个区间和 $M = 2^k = 256$ 个关联函数。每次运行任一学习算法都使用

$$t_1 + \sum_{j=1}^{8} (t_{j+1} - t_j) = 12 \tag{K.3}$$

次正向查询，查询对象均为同一个 U。因此， N 次实验运行对应的总查询预算为 $q = 12N$，适用于任一算法。

2. 探针信号与关联函数展开

目标实验使用一个初始状态为 $|+\rangle$ 的探针。在前八次接触中，边界旋转和探针–系统耦合采用相同的随机符号：

$$V_{s_j,\alpha_j} = e^{-is_j\alpha_j I_Q \otimes Z_1/2} e^{-is_j\beta_j Z_Q \otimes Z_1/2}, \qquad \beta_j = \frac{\pi}{2} - \alpha_j. \tag{K.4}$$

最后一次接触为 $V_{s_9,\ 0} = e^{-is_9\pi Z_Q \otimes B/4}$。全部九个符号 $\boldsymbol{s} = (s_1, \ldots, s_9) \in \{\pm 1\}^9$ 彼此独立，且在$\{\pm 1\}$上均匀分布。

令 Ω 表示探针—系统联合态，并定义其重缩放的非对角块

$$\chi = 2\, {}_Q\langle 0|\Omega|1\rangle_Q, \qquad L = \langle X_Q \rangle - i\langle Y_Q \rangle = \operatorname{Tr} \chi. \tag{K.5}$$

起初， $\chi = \rho$。预测目标是

$$S(\boldsymbol{\alpha}) = 2^{-9} \sum_{\boldsymbol{s} \in \{\pm 1\}^9} \left(\prod_{j=1}^{9} s_j \right) L(\boldsymbol{s}; \boldsymbol{\alpha}). \tag{K.6}$$

从操作上看，其实部是 $(\prod_j s_j) x_Q$ 在 X_Q 次读出中的平均值，而其虚部是 $(\prod_j s_j) y_Q$ 在另一组 Y_Q 次读出中的负平均值，其中 $x_Q,\ y_Q \in \{\pm 1\}$。将 L 展开为关于二元符号的多项式可见，方程（K.6）恰好选出了 $s_1 \cdots s_9$的系数。与任意一个符号无关的贡献会相互抵消。因此，这一符号加权操作能够分离出信号的最高阶分量。

为推导关联函数表示，我们在相互作用绘景中进行计算，并写出

$$B_j = (U^{t_j})^\dagger Z_1 U^{t_j}, \qquad B_j^2 = I. \tag{K.7}$$

在符号 s的条件下，接触 j 将非对角块变换为

$$\Phi_{j,s}(X) = e^{-is(\alpha_j+\beta_j)B_j/2} X e^{is(\alpha_j-\beta_j)B_j/2}. \tag{K.8}$$

引入线性映射

$$\mathcal{A}_j(X) = \frac{\{B_j, X\}}{2}, \qquad \mathcal{C}_j(X) = \frac{[B_j, X]}{2i}, \tag{K.9}$$

并利用恒等算子 $e^{-i\gamma B_j} = \cos\gamma\, I - i \sin\, \gamma\, B_j$，我们计算带符号平均：

$$\begin{aligned} \mathcal{M}_j(X) &\coloneqq \frac{1}{2}\sum_{s=\pm1} s\,\Phi_{j,s}(X) \\ &= -\frac{i}{2}\left[(\sin\alpha_j + \sin\beta_j)B_j X + (\sin\beta_j - \sin\alpha_j) X B_j\right] \\ &= -i\sin\beta_j\,\mathcal{A}_j(X) + \sin\alpha_j\,\mathcal{C}_j(X). \end{aligned} \tag{K.10}$$

代入 $\beta_j = \pi/2 - \alpha_j$，得到

$$\mathcal{M}_j = -i\cos\alpha_j\,\mathcal{A}_j + \sin\alpha_j\,\mathcal{C}_j \quad (j \le 8), \qquad \mathcal{M}_9 = -i\mathcal{A}_9. \tag{K.11}$$

因此，完整的符号加权信号由这些线性映射的复合生成：

$$S(\boldsymbol{\alpha}) = \mathrm{Tr}[\mathcal{M}_9 \circ \cdots \circ \mathcal{M}_1(\rho)] = -i\ \mathrm{Tr}[B_9\,\mathcal{M}_8 \circ \cdots \circ \mathcal{M}_1(\rho)]\,, \tag{K.12}$$

其中，第二个等式由 $\mathrm{Tr}[\mathcal{A}_9(X)] = \mathrm{Tr}(B_9 X)$ 得出。

为将其与嵌套关联函数联系起来，令 $\mathcal{D}_j^{(0)} = \mathcal{A}_j$ 和 $\mathcal{D}_j^{(1)} = \mathcal{C}_j$。迹的循环性给出对偶关系

$$\mathrm{Tr}\left[Y\mathcal{D}_j^{(b)}(X)\right] = \frac{1}{2i^b}\,\mathrm{Tr}([Y, B_j]_b X)\,, \qquad b \in \{0,1\}. \tag{K.13}$$

将式（K.13）依次应用于式（K.12）可得

$$\mathrm{Tr}\left[B_9\,\mathcal{D}_8^{(\sigma_8)} \circ \cdots \circ \mathcal{D}_1^{(\sigma_1)}(\rho)\right] = \frac{(-i)^{|\sigma|}}{2^8}\,\mathrm{Tr}\left[\rho\left[\cdots[B_9, B_8]_{\sigma_8}\cdots, B_1\right]_{\sigma_1}\right] = 2F_\sigma(U). \tag{K.14}$$

因此，将式（ $\mathcal{M}_j$ 中前八个映射展开K.12，即可得到精确表示：

$$S(\boldsymbol{\alpha}) = 2\sum_{\sigma\in\{0,1\}^8} w_\sigma(\boldsymbol{\alpha}) F_\sigma(U), \qquad w_\sigma(\boldsymbol{\alpha}) = (-i)^{9-|\sigma|}\prod_{j=1}^{8}(\cos\alpha_j)^{1-\sigma_j}(\sin\alpha_j)^{\sigma_j}. \tag{K.15}$$

关键在于，权重 $w_\sigma(\boldsymbol{\alpha})$ 是控制角的显式函数，且不依赖于系统动力学 U。此外，由于 F_σ 为实数，具有奇数汉明重量 $|\sigma|$ 的关联函数仅对 $\mathrm{Re}\,S$ 有贡献，而具有偶数 $|\sigma|$ 的关联函数则对 $\mathrm{Im}\,S$ 有贡献。

用于构造256 个关联函数 F_σ 的学习数据通过以下任一方式获取：算法1或算法2，具体如下。估算后，这些关联函数还可重复用于预测 $S(\boldsymbol{\alpha})$ 在任意控制角选择下的探针信号。

3. 学习算法的实现

我们首先通过直接矩阵乘法计算精确的关联器值 $\{F_\sigma\}$，如图3b 所示。计算时对方程（K.14）进行求值。这些精确值构成我们的参考基准。它们还决定了用于模拟两种学习算法测量记录的玻恩概率，详情如下。

a. 算法1：共享记录

对于路径字符串 $b \in \{0,1\}^8$，令 $\chi_\sigma(b) = (-1)^{\sigma \cdot b}$，并令 Q_b 为方程（F.5）中定义的互补路径重叠。对方程（F.6）求逆可得

$$Q_b = 2 \sum_\sigma \chi_\sigma(b)(-i)^{|\sigma|} F_\sigma. \tag{K.16}$$

算法均匀地抽取一条路径 b 和一个公平符号 u，然后测量$(X_Q + uY_Q)/\sqrt{2}$ 和 Z_1，得到测量结果a，$x \in \{\pm 1\}$。只有它们的乘积 $z = ax$ 会参与估计量的计算。根据公式（H.3），这些变量的联合分布为

$$p(b,u,z) = \frac{1}{4M}\left[1 + \frac{z}{\sqrt{2}}\left(\operatorname{Re} Q_b - u \operatorname{Im} Q_b\right)\right]. \tag{K.17}$$

回顾公式（H.4，每个目标量的单条记录贡献为

$$T_\sigma(b,u,z) = \frac{\chi_\sigma(b)}{2} \operatorname{Re}\left[i^{|\sigma|}\sqrt{2}\, z(1-iu)\right] \in \{-1/\sqrt{2}, +1/\sqrt{2}\}, \tag{K.18}$$

它满足 $\mathbb{E}T_\sigma = F_\sigma$，证明见附录H。

生成每个数据集时，我们从 $4M = 1024$ 个可能的记录中抽取一个计数向量，并计算共享估计量：

$$\{C_{buz}\} \sim \text{Multinomial}(N, \{p(b,u,z)\}), \qquad \widehat{F}_\sigma^{(1)} = \frac{1}{N} \sum_{b,u,z} C_{buz} T_\sigma(b,u,z). \tag{K.19}$$

同一个计数向量用于估计每个 σ。

b. 算法2：分别估计

我们为每个目标量分配 $m = N/M$ 次运行。在接触点 j，若比特 $\sigma_j = 0$ 为 0，则执行对B的投影测量；若比特 $\sigma_j = 1$ 为 1，则执行随机旋转 $e^{-ia_j \pi B/4}$，详见附录 I。保留的输出为

$$Z_\sigma = \frac{x}{2} \prod_{j=1}^{8} a_j \in \{-1/2, +1/2\}, \qquad \mathbb{E}Z_\sigma = F_\sigma. \tag{K.20}$$

由于 Z_σ 是二进制的，其分布由 $\Pr(Z_\sigma = +1/2) = 1/2 + F_\sigma$ 给出。因此，各个目标量的独立计数满足

$$C_\sigma \sim \text{Binomial}(m, 1/2 + F_\sigma), \qquad \widehat{F}_\sigma^{(2)} = \frac{C_\sigma}{m} - \frac{1}{2}. \tag{K.21}$$

c. 图3的误差统计与构建

对于每种算法 $\ell \in \{1,2\}$ 和每种预算 $N \in \{2^{14}, 2^{16}, \ldots, 2^{26}\}$，我们生成 $D = 1024$ 个独立数据集。定义单个数据集$e_{\ell,\ r}(N)$ 的均方根（RMS）误差 r，以及图3c 中绘制的整体集合平均均方根误差，表示为

$$\begin{aligned} e_{\ell,r}(N) &= \left[\frac{1}{M}\sum_\sigma \left(\widehat{F}_\sigma^{(\ell,r)}(N) - F_\sigma\right)^2\right]^{1/2}, \\ \text{RMSE}_\ell(N) &= \left[\frac{1}{D}\sum_{r=1}^{D} e_{\ell,r}(N)^2\right]^{1/2} = \left[\frac{1}{DM}\sum_{r=1}^{D}\sum_\sigma \left(\widehat{F}_\sigma^{(\ell,r)}(N) - F_\sigma\right)^2\right]^{1/2}. \end{aligned} \tag{K.22}$$

图3c 中的阴影带表示 $e_{\ell,\ r}(N)$ 的经验 2.5% 和 97.5% 分位数，描述了独立数据集间的统计波动。

为解析比较这两种算法的性能，我们定义 $\mu_2 = M^{-1}\sum_\sigma F_\sigma^2$。于是，期望均方误差满足

$$\mathbb{E}[e_{1,r}(N)^2] = \frac{1/2-\mu_2}{N}, \qquad \mathbb{E}[e_{2,r}(N)^2] = \frac{M(1/4-\mu_2)}{N}. \tag{K.23}$$

对于此模型，$\mu_2 = 1.0\ \ 7718\times 10^{-6}$。若要使期望均方根误差相等，这些表达式给出的成本比为 o f

$$\frac{q_2}{q_1} = \frac{N_2}{N_1} = M\frac{1/4-\mu_2}{1/2-\mu_2} \simeq 128. \tag{K.24}$$

相反，在相同预算 N下，相应的均方根误差比约为 $\sqrt{128}\approx 11.31$。在 $N = 2^{24}$ 处的有限数据集均方根误差分别为 1.72×10^{-4} 和 1.96×10^{-3}，对应算法 1 和 2。这证实了总体实验成本降低了约两个数量级。

图 3 的 b 面板和 d 面板展示了每种算法在 $r = 0$处首个生成的数据集（ $N = 2^{24}$）上的结果。在 d 面板中，我们设定 $\alpha_{1,\ 3,\ 5,\ 7} = \theta$ 和 $\alpha_{2,\ 4,\ 6,\ 8} = \phi$ 在均匀 121×121 网格 $\mathcal{G}$ 上，覆盖 $[-\pi/2,\pi/2]^2$。精确的信号映射$S(\theta,\ \phi)$ 通过方程（K.15）计算，而预测映射则根据估计的关联函数重建如下：

$$\widehat{S}_\ell(\theta,\phi) = 2\sum_\sigma w_\sigma(\theta,\ \phi)\,\widehat{F}_\sigma^{(\ell)}. \tag{K.25}$$

为了量化这些重建结果的准确性，我们将 $\mathcal{G}$ 上的相对均方根误差定义为

$$\epsilon_{S,\ell} = \left[\frac{\sum_{(\theta,\phi)\in\mathcal{G}}|\widehat{S}_\ell(\theta,\phi)-S(\theta,\phi)|^2}{\sum_{(\theta,\phi)\in\mathcal{G}}|S(\theta,\phi)|^2}\right]^{1/2}. \tag{K.26}$$

对于所显示的映射，这得到 $\epsilon_{S,\ 1} = 0.136$ 对于算法 1 和 $\epsilon_{S,\ 2} = 1.24$ 对于算法 2。