物理上自然的度量测度 Lindbladian 系综及其学习困难性

Caisheng Cheng[1,2,3,*] 和 Ruicheng Bao[4,†]
[1]合肥微尺度物质科学国家实验室与中国科学技术大学现代物理系，中国安徽合肥
[2]中国科学院卓越创新中心量子信息与量子物理协同创新中心上海分部，中国科学技术大学，中国上海 *201315*
[3]上海量子科学研究中心，中国上海 *201315*
[4]东京大学理学研究科物理系，日本东京都文京区本乡 *113-0033*

arXiv:2601.01806v1 [quant-ph] 5 Jan 2026

在开放量子系统中，量子信息、统计物理和多体动力学交汇处的一个基本问题是：仅凭有限时间测量统计，能够在多大程度上推断噪声和耗散生成元的结构？受此问题启发，我们研究由 Lindblad-Gorini-Kossakowski-Sudarshan（GKSL）主方程生成的随机开放系统动力学的可学习性及其密码学应用。我们在 GKSL 锥的仿射包中，通过围绕参考生成元进行线性参数化，引入具有物理动机的随机局部 Lindblad 算子系综。在这一几何结构之上，我们将统计查询（SQ）和量子过程统计查询（QPStat）框架扩展到开放系统场景，并证明学习随机 Lindblad 动力学所需的查询数量存在关于参数维数 M 的指数下界。具体而言，我们确立了学习全变差距离意义下输出分布的平均情形 SQ 困难性，以及学习菱形范数意义下 Lindblad 通道的平均情形 QPStat 困难性。为从物理上支持这些结果，我们推导出系综平均全变差距离的线性响应表达式，并在随机局域振幅阻尼链中验证所需的非零标度。最后，我们基于随机 Lindblad 算子系综设计了两种 Lindblad 物理不可克隆函数（Lindbladian-PUF）协议，分别采用分布层面的验证和基于层析的验证，从而提供了将学习困难性转化为密码学安全保证的开放系统实例。

目录

I. 引言 2

II. 结果概要 4
A. 从随机酉电路到随机林布拉德算子：系综构造蓝图 4
B. 设置 6
C. 学习困难性与密码学应用 8

III. 讨论与展望 13

IV. 预备知识 15
A. 范数约定与基本不等式 15
B. GKSL 生成元与量子马尔可夫半群 17
C. 统计查询学习模型 18
D. 从学习到判定的归约与平均情形下界 20
E. 随机统计查询算法与确定性算法 20
F. QPStat 模型与一般下界 21
G. 弗雷歇导数与扰动公式 22
H. Haar 测度、集中性与 2-范数 Lipschitz 常数 24

V. 随机林德布拉德系综 25
A. 随机林德布拉德系综的线性参数化与集中性 25
B. $P_{\mathcal{L}}[\varphi]$ 的接口与 Lipschitz 连续性 28

* ccs112202@mail.ustc.edu.cn
† C. Cheng 和 R. Bao 对本工作贡献相同。

C. 参数球面上的 Lipschitz 常数与列维集中30D. 独立局部耦合的乘积测度集中32E. 平均情形下学习随机 Lindblad 通道的 QPStat 困难性35

VI. 物理上自然的 球面随机扰动林德布拉德算子系综 40

VII. 远离-Q 44
A. 关于参数的全变差距离 Lipschitz 连续性 44B. 均值假设与远离Q集中性 47C. 平均情形统计查询复杂度 48D. 从远离Q 到远离任意D 50

VIII. 随机林布拉德算子系综中平均总变差距离的线性响应标度 52
A. 根据扰动公式进行线性响应展开 52B. 球面上线性形式的绝对值期望 54C. 平均总变差距离的线性响应标度 56

第九节. 线性响应 随机局域振幅阻尼林德布拉德模型中的均值缩放与数值模拟 58
A. 平均总变差距离的标度常数 $m_0 > 0$ 58B. 数值模拟：验证开放系统 Porter–Thomas 均值假设 64

X. 随机林德布拉德算子构造的物理不可克隆函数：分布层面与基于层析的验证 67
A. 方案 A：基于输出分布的 Lindbladian-PUF 68B. 扩展 QPStat 模型与层析基 83C. 方案 B：基于层析的 Lindbladian-PUF 86

参考文献 90

I. 引言

理解多体量子系统中混沌与遍历行为如何普遍涌现，是现代量子多体物理的核心目标之一。关于随机矩阵和单粒子量子混沌的早期研究，以及本征态热化假说的提出，已经表明，只需在混沌哈密顿量的参数中引入微小的不确定性，就足以使谱统计和物理可观测量呈现普适的涨落行为 [Wig67, BGS84, MHB+04, Deu91, RDO08]。过去十年间，局域随机量子线路、酉 t-设计和伪随机酉矩阵（PRUs）已发展成为成熟的技术框架 [EWS+03, GAE07, Dan05, DCEL09, BHH16, NHKW16, Haf22, JLS18, BS19, MPSY24, CBB+24, ABGL25, MH25, LL24, SHH25, LDNT25, GHH+25, CSBH25, SML+25, SKYH25]：一方面，它们量化了物理上可实现的电路多快会变得无法与 Haar 随机酉算子区分；另一方面，这类伪随机动力学已广泛应用于随机基准测试和噪声表征、随机线路采样与量子优势的展示，以及量子引力和黑洞信息等基础问题 [EAŻ05, KLR+08, EFH+23, GKKT20, HKP20a, ZRM21, AC16, BIS+18, BFNV19, AAB+19, MVM+23, AAAB+25, HP07, KTP20, AEH+22, ABC+24, YE25]。从信息论和复杂性理论视角来看，这些研究共同表明，封闭系统中的“典型动力学”往往在物理上高度混沌，在计算上也具有很高的复杂度。

与此同时，量子学习理论从访问模型的角度，系统地研究了量子机器学习在经典与量子任务中的优势和局限 [Val84, Kea98, AdW17]。特别是在封闭系统的随机电路情境中，学习复杂度与伪随机性密切相关。在这一框架下，学习器可以是经典、量子或混合算法，通过有限访问来构建对未知对象（布尔函数、概率分布、量子态或量子过程）的假设 [HHJ+15, WPS+17, Aar18a, AdW18a, ACH+18, HKP20b, CW20, CCHL21, HKP21, ACQ22, CCHL23, HTFS23, CCHL21, HBC+22, ACQ22]。经典的随机样本模型和统计查询（SQ）模型已扩展至量子领域，由此产生了量子样本模型和量子统计查询（QSQs） [BJ95, ADW18b, AGY20, AHS24, HIN+23, NIS+23, Nie23]。在这些访问模型中，人们已针对量子态学习

、影子层析、概率分布学习和量子过程学习 [BCD+09，Aar18b，CLL+22，Mon17a，MRL08，CL21，HKOT23]。结合酉设计和伪随机酉的构造，这些结果描绘出封闭系统的如下图景：一方面，在强访问模型下，存在能够高效预测复杂度极高的量子过程局部性质的算法；另一方面，对于随机电路系综，在受限访问模型下，典型的输出分布或量子信道表现出显著的平均情形学习困难性。

与这种封闭系统图景形成鲜明对比的是，现实中的量子器件不可避免地与环境耦合，其动力学用 Lindblad-Gorini-Kossakowski-Sudarshan（GKSL）主方程描述更为自然。一方面，耗散和退相干限制了封闭系统随机电路模型的适用性；另一方面，开放系统催生了各种利用耗散制备稳态和调控量子动力学的方案 [VWIC09、DMK+08、KBD+08、BMS+11]。近期关于随机林德布拉德算子系综及其典型弛豫性质的研究 DLT+19，TCDŻ23、Bao25]，，以及提出从稳态、时间序列或轨迹数据中学习 Lindblad 算子的方案 [BGP+20、WL24、WAG+25]，揭示了许多引人入胜的现象，包括普适谱统计、谱隙结构以及对初态的不敏感性。然而，从学习复杂度和密码学的角度来看，开放系统领域仍存在一个显著空白：迄今为止，GKSL 锥中尚无一类对象能同时具备物理上的自然性，以及“随机 Lindblad 算子设计”意义下良好的度量测度结构；此外，对于典型开放系统动力学在 SQ/QPStat 访问模型中的可学习性，也缺乏定量刻画，更遑论构造基于此类系综的伪随机过程或密码协议原语的开放系统对应物。

本工作的目标是建立一个统一框架来填补这一空白：既与酉设计/伪随机酉以及 SQ/QPStat 学习理论相呼应，又着重阐明开放系统所特有的结构与物理意义。我们的主要贡献概括如下：

1. **随机 Lindblad 算子系综与度量测度结构**。我们在 GKSL 锥的仿射包内开展研究，从局域 Lindblad 算子出发，通过线性参数化 $\mathcal{L}(\theta) = \mathcal{L}_{\mathrm{ref}} + \sum_{j=1}^{M} \theta_j G_j$. 构造两种物理上自然的随机林德布拉德算子系综。一种是“Lindblad Haar 型”球面系综，其参数位于单位球面 S^{M-1} 上，并采用 $1/\sqrt{M}$ 归一化；另一种是乘积测度系综，其中每个局部耦合强度都在一个小区间内独立波动。我们将两者统一视为度量概率空间 (Θ, d, μ)，并证明，对于任意有界的 SQ（类比 QPStat）测试函数 $\varphi : X \to [-1, 1]$，诱导函数 $F_\varphi(\theta) := P_{\mathcal{L}(\theta)}[\varphi]$在参数空间上具有与维数无关的利普希茨常数；此外，它在球面上分别满足列维型集中不等式，在乘积测度下满足 McDiarmid 型有界差分集中不等式。

2. **开放系统中的 SQ 与 QPStat 困难性结果**。在分布层面，我们固定一个单次测量接口（演化时间 t、输入态 ρ_{in}，以及有限输出集合 X上的 POVM $\{M_x\}$），并且只能通过 SQ 查询访问信道输出分布 $P_{\mathcal{L}}$。我们证明，对于上述 Lindblad 生成元系综，无论是判断$\mathcal{L}$ 来自某个子系综还是参考分布的二元假设检验问题，还是在平均情形下学习输出分布 $P_{\mathcal{L}}$ 的任务，都要求任何 SQ 算法（包括由量子过程实现的 SQ 算法）至少使用关于参数维数 M呈指数级数量的查询，即使只要求算法在参数的某个子集上成功也是如此。在通道层面，我们引入一种适用于林德布拉德算子的 QPStat 访问模型，使学习器能够针对信道$\Lambda_t^{(\mathcal{L}(\theta))}$ 的期望值进行过程层面的统计查询。我们证明，对于同样的 Lindblad 生成元系综，任何试图以菱形距离或平均信道距离达到常数精度来学习典型随机 Lindblad 信道的 QPStat 算法，都必须使用指数级数量的过程查询，从而确立了开放系统场景中信道学习的平均情形 QPStat 困难性结果。因此，我们的结果表明，在弱访问模型下，随机过程的“开放系统版本”具有内在的平均情形学习困难性。

3. **开放系统 Porter-Thomas 型平均假设与线性响应分析**。为支持上述平均情形下界，我们提出并分析开放系统中与 Porter-Thomas 型“平均全变差距离假设”相对应的版本：经过适当归一化和缩放后，系综平均全变差距离 $\mathbb{E}_{\mathcal{L}} d_{\mathrm{TV}}(P_{\mathcal{L}}, Q)$ 在高维极限下收敛到一个严格为正的

常数 $m_0 > 0$。我们利用 Kubo 型微扰公式，对随机局域 Lindblad 模型进行线性响应展开，明确计算一阶响应向量的范数及其随参数维数 M、演化时间 t 以及局部跳跃算符结构的标度行为，并通过一个局域随机振幅阻尼链的具体模型，从解析和数值两方面验证 m_0 的常数标度。这使我们对 Lindblad 生成元系综的分析统一于一个具有物理意义的图景之中，并与封闭系统中基于 Porter-Thomas 的分析相呼应。

4. **基于随机林布拉德算子的物理不可克隆函数协议**。最后，我们通过构造两种基于随机林布拉德算子的物理不可克隆函数（PUF）协议，将上述学习困难性结果与密码学原语联系起来。第一种是完全基于输出分布的“分布级验证”方案；其安全性直接源于学习输出分布的 SQ 困难性，并且验证接口经过有意限制，使该方案在对手受到给定资源上限约束时仍然安全。第二种是“基于层析的验证”方案，允许进行有限次数的 QPStat 查询或实验层析；通过在适当的算符基中定义层析指纹，该方案将信道在菱形距离意义下的不可克隆性转化为学习 Lindblad 通道的 QPStat 困难性。在我们的框架内，我们还讨论了如何在开放系统场景中明确权衡验证成本与安全性，从而展示了“SQ/QPStat 困难性蕴含密码学安全性”在开放系统体制中的一个实例。

本文其余部分的组织如下。我们首先总结并讨论主要定理和结果。在第 IV节，我们回顾 GKSL 生成元、SQ 和 QPStat 模型，以及测度集中的相关工具。第 V-VII 节分别建立 Lindblad 生成元系综的几何结构、其 Lipschitz–Lévy 型集中性质，以及关于输出分布和量子信道的 SQ/QPStat 学习复杂度下界。第 VIII-IX 节介绍线性响应分析，以及一个支持 Porter-Thomas 型平均假设的随机振幅阻尼链具体模型。第 X 节随后详细讨论基于随机 Lindblad 生成元的 Lindblad 生成元物理不可克隆函数协议及其安全性分析。

II. 结果总结

A. 从随机酉电路到随机林德布拉德算子：系综构造蓝图

在随机量子电路和典型性的相关文献中，随机酉矩阵的构造通常遵循一个共同的蓝图 [Mel24, BHH16, Haf22, NIS+25]: 首先固定一个电路空间 C（例如，固定深度的砖墙式局域线路 d，其各层由双量子比特门组成），然后在 C 上指定一个物理上自然的随机系综 $\mu_{\mathcal{C}}$。在理想化情形下，这是 $U(d)$ 上的哈尔测度；而在更贴近硬件的砖墙式线路中，每个局域双量子比特门都独立地从 Haar 分布中抽取，从而在 C 上得到乘积测度型分布。对于足够大的深度，此类局域随机电路可近似固定 t [阶的 Haar t-设计 BHH16, Haf22]。给定固定的测量架构，每个电路 $C \in$C 都会诱导出一个经典输出分布 P_C，而测度 $\mu_{\mathcal{C}}$ 随后定义了随机电路输出分布的一个系综。在此基础上，人们研究 (C $d_{\mathrm{circ}}, \mu_{\mathcal{C}}$) 上的集中性质（例如 Lipschitz 函数 $C \mapsto P_C[\varphi]$的集中性），以及相对于 $\mu_{\mathcal{C}}$ [NIS+25] 的平均情形 SQ 困难性。

我们的首要贡献是构造一个随机林德布拉德算子系综，而本工作的一个核心概念出发点，是将这一随机电路蓝图系统地移植到 Lindblad 生成元框架中。我们不直接在抽象的 GKSL 锥上假定一个测度，而是先在有限维超算符空间中构建一个线性坐标系，再在由此得到的参数空间中选取度量和测度；这样便能以可控的方式生成随机林德布拉德算子系综。如图 1 所示，我们的随机林德布拉德系综始终定义在一个度量概率空间 (Θ, d, μ) 上，其中 Haar 球面模型和乘积测度模型对应于参数空间、度量和抽样测度的两种具体选择。具体而言，我们的构造过程如下：

1. **完整线性参数化**。 对于固定的希尔伯特空间维数 d，GKSL 锥的仿射包可以视为有限维实向量空间中的一个仿射子空间。引理 8 表明

存在一组基 $\{G_j\}_{j=1}^M$ 以及一个参考生成元 $\mathcal{L}_{\text{ref}} \in$GKSL，使得

$$\mathcal{L} = \mathcal{L}_{\text{ref}} + \sum_{j=1}^{M} \theta_j(\mathcal{L})\, G_j$$

对于每个 Lindblad 算子 $\mathcal{L} \in$ GKSL，其中可行参数 $\theta(\mathcal{L}) \in \mathbb{R}^M$ 位于凸锥 $\mathcal{C}_{\text{GKSL}} \subset \mathbb{R}^M$中。换言之，在适当的线性坐标下，形式 $\mathcal{L} = \mathcal{L}_{\text{ref}} + \sum_j \theta_j(\mathcal{L})G_j$ 涵盖了所有 GKSL 生成元；从这个意义上说，该参数化甚至比随机酉模型中受群结构约束的参数化更加灵活。

2. **从 (θ, d, μ) 到随机林德布拉德算子系综。** 固定线性坐标系后，我们不会直接在 GKSL 上选取测度，而是先在参数空间 $\Theta \subset \mathbb{R}^M$上选取

$$\text{(i) a parameter domain } \Theta, \quad \text{(ii) a metric } d(\cdot,\cdot), \quad \text{(iii) a probability measure } \mu,$$

从而构成一个度量概率空间 (Θ, d, μ)。随后我们通过 μ

$$\theta \longmapsto \mathcal{L}(\theta) := \mathcal{L}_{\text{ref}} + \sum_{j=1}^{M} \theta_j G_j$$

得到 Lindblad 算子上的先验分布 $\mu_{\mathcal{L}} := \mathcal{L}_{\#}\mu$ 。这与随机电路中的步骤“选择一个电路空间 $\mathcal{C}$ 和一个电路测度 $\mu_{\mathcal{C}}$”相对应，只不过现在我们是在一个线性超算符空间而非酉群中进行操作。

3. **专为集中性和 SQ 困难性设计的两个具体系综。** 为了使后续的学习复杂度分析成立，我们要求 (Θ, d, μ) 满足：

(a) 对于每个 SQ（类比 QPStat）测试函数 $\varphi : X \to [-1, 1]$，映射 $\theta \mapsto F_\varphi(\theta) := P_{\mathcal{L}(\theta)}[\varphi]$关于 d具有一致 Lipschitz 常数，这由推论 1 结合线性参数化得到；

(b) 度量概率空间 (Θ, d, μ) 本身满足强集中不等式（列维型或 McDiarmid 型），因此 F_φ 在 μ 下表现出高维集中性，从而得到 frac$(\mu_{\mathcal{L}}, Q, \tau)$ 的指数级小上界。

基于这些要求，我们引入两个在物理上自然且几何性质受控的系综：

i. 球面随机扰动系综 (定义23 和注释 15)：在 $\mathbb{R}^M$ 中取单位球面S^{M-1} 及其旋转不变测度，并定义

$$\mathcal{L}_{\text{sph}}(\theta) = \mathcal{L}_{\text{ref}} + \frac{\delta}{\sqrt{M}} \sum_{j=1}^{M} \theta_j G_j, \qquad \theta \in S^{M-1},$$

其中 $\delta > 0$ 是一个小参数。通过选择 δ 足够小（或对交集进行归一化$S^{M-1} \cap$GKSL），我们可以确保 $\mathcal{L}_{\text{sph}}(\theta) \in$ 对所有 θ都属于 GKSL。欧几里得／球面几何使我们能够应用列维集中（引理 7），并得到定理 exp$(-\Omega(M))$型界10。

ii. 独立局部耦合参数（乘积测度）系综 （定义 24）：此处 $\Theta_{\text{prod}} = [-\delta/M, \delta/M]^M$，每个坐标 θ_j均独立抽取，度量为 ℓ_1， $d_1(\theta,\ \theta') = \|\theta - \theta'\|_1$。参数化

$$\mathcal{L}_{\text{prod}}(\theta) = \mathcal{L}_{\text{ref}} + \sum_{j=1}^{M} \theta_j G_j$$

刻画了“每个局域耦合常数都是相互独立的小随机数”这一假设。于是F_φ（θ）在 d_1 （引理 13）中具有与维数无关的利普希茨常数，而麦克迪尔米德不等式（引理14）给出了定理 11。

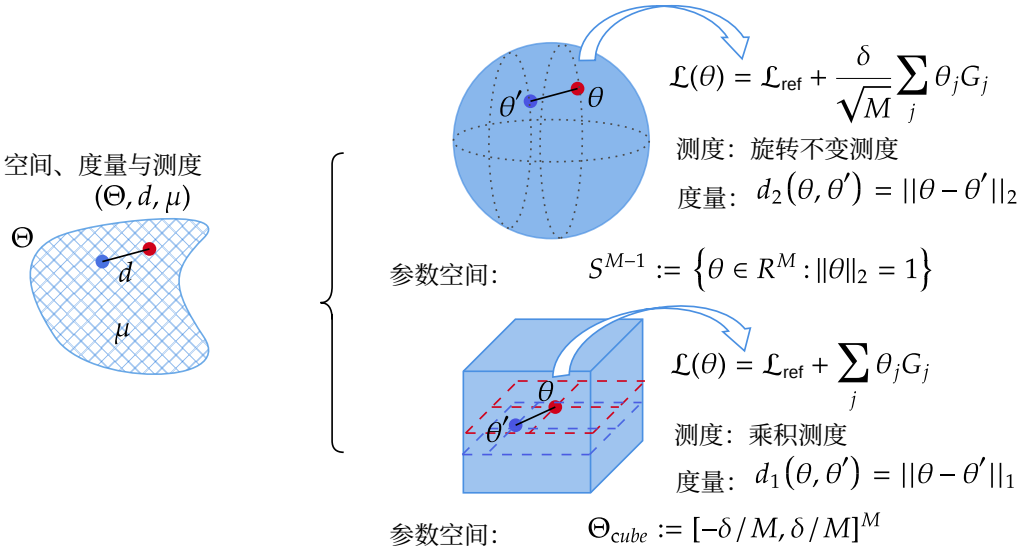

图 1。用于定义随机林德布拉德系综的度量概率空间示意图。左侧：抽象参数空间（Θ、d、μ），其中 Θ 是参数域，d 是定义在 Θ 上的选定度量，μ 是系综（采样）测度。右上：Haar 球面系综，其中参数相对于旋转不变的（由 Haar 测度诱导的）表面测度，从高维球面 S^{M-1} 上一致采样：$=\{\theta \in \mathbb{R}^M : \|\theta\|_2 = 1\}$。度量是欧几里得距离 $d_2(\theta、\theta') = \|\theta - \theta'\|_2$，林德布拉德算子参数化为 $\mathrm{L}(\theta) = \mathrm{L}_{\text{ref}} + \frac{\delta}{\sqrt{M}} \sum_j \theta_j G_j$。右下：乘积测度系综，其中每个耦合参数 θ_j 都是一个独立的随机变量，其支撑集为 $[-\delta/M, \delta/M]$，因此 $\Theta_{\text{cube}} : = [-\delta/M, \delta/M]^M$。此处的度量是 ℓ_1 距离 $d_1(\theta、\theta') = \|\theta - \theta'\|_1$，测度是乘积测度 μ_{prod}，林德布拉德算子参数化为 $\mathrm{L}(\theta) = \mathrm{L}_{\text{ref}} + \sum_j \theta_j G_j$。

在这两种构造中，小参数 δ 具有双重作用，因为它控制 $\mathcal{L}$（θ）偏离参考分布 $\mathcal{L}_{\text{ref}}$ 的程度（保持在局部 GKSL 邻域内），同时使第 VIII节中的线性响应分析得以进行。

从这一视角来看，我们工作的一个结构性贡献是系统地建立了以下路径

“线性参数化 + （参数空间、度量、测度）”

用于生成随机林德布拉德系综：在有限维情形下，我们涵盖所有 GKSL 生成元（引理 8）；通过适当选择 Θ、d、μ，我们可以将列维或 McDiarmid 集中性工具直接代入 SQ/QPStat学习复杂度框架。从概念上看，这类似于传统的随机电路构造（Haar 或局部门集），但在开放系统场景中，它实现了一种线性的、显式参数化且符合物理直觉的构造。

B. 设置

一旦 $(\Theta、d、\mu)$ 的几何结构以及线性参数化 $\theta \mapsto \mathcal{L}(\theta)$ 确立之后，我们将基于两种互补的信息访问模型，研究随机林德布拉德动力学中的学习问题和判定问题。我们模型的整体架构如图 2所示。

（i）分布层面的SQ接口，其中固定时间 $t > 0$、输入态 ρ_{in} 和 POVM $\{M_x\}_{x \in X}$，只能通过容差为 τ 的统计查询 $P_{\mathcal{L}(\theta)}[\varphi]$观测由此诱导的经典输出分布 $P_{\mathcal{L}(\theta)} \in \mathcal{D}_X$；

(ii) 过程层面的QPStat接口，其中对于每个参数 θ，将 CPTP 映射 $E_\theta = e^{t\mathcal{L}(\theta)}$ 视为待学习的对象，而 QPStat 预言机会对任意量子态 $\rho \in \mathrm{S}(\mathcal{H})$ 和算子 $O \in \mathcal{B}(\mathcal{H})$，以指定容差返回近似期望值 $\mathrm{Tr}[O\, E_\theta(\rho)]$ $\|\rho\|_1 \le 1$ 和 $\|O\|_\infty \le 1$。

在分布方面，利用定理 10和 11给出的指数级小上界，以及 Feldman 和 Nietner 等人 [Fel17、NIS+25]的一般 SQ 学习与决策理论引理，

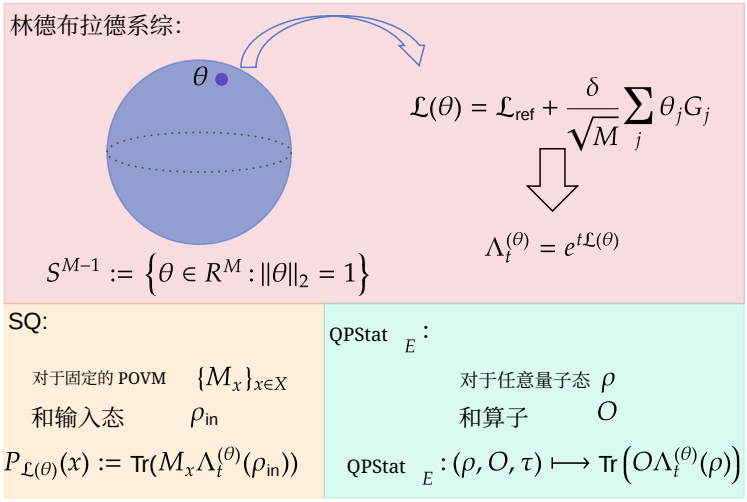

图 2。本文所考虑的随机 Lindblad 算子系综及两种信息访问模型的示意设置。上：Lindblad 算子族通过高维球面上的点 θ，经由线性嵌入 $\mathcal{L}(\theta) = \mathcal{L}_{\text{ref}} + \frac{\delta}{\sqrt{M}} \sum_j \theta_j G_j$ 进行参数化，并生成一个量子马尔可夫半群 $\Lambda_t^{(\theta)} = e^{t\mathcal{L}(\theta)}$。左下：分布层面的SQ接口，其中固定的输入态 ρ_{in} 和POVM $\{M_x\}_{x\in X}$ 定义输出分布$P_{\mathcal{L}(\theta)}(x) = \text{Tr}\left(M_x \Lambda_t^{(\theta)}(\rho_{\text{in}})\right)$，学习器只能访问期望值 $P_{\mathcal{L}(\theta)}[\varphi]$。右下：针对信道 $E_\theta := \Lambda_t^{(\theta)}$ 的过程层面的QPStat接口，其中 QPStat 预言机接收一个量子态 ρ、一个可观测量 O 和一个容差 τ，并返回 $\text{Tr}\left(O\,\Lambda_t^{(\theta)}(\rho)\right)$ 的近似值。

我们在第 VIIC 节针对随机 Lindblad 算子输出分布上的平均情形学习任务，得到了指数级 SQ 下界。为便于与随机电路文献中关于 Haar 设计的研究进行比较，我们主要以球面随机扰动系综（定义 23）为基准来表述 SQ 困难性结果；同时，独立局部耦合系综也表明，该框架同样适用于其他物理上自然的随机 GKSL 模型。

在过程层面，我们在第 VE 节中引入一种适用于开放系统动力学的 QPStat 预言机模型，以及一个通用的菱形范数下界框架。我们证明，对于相同的参数球面系综(Θ, d, μ)，映射 $\theta \mapsto E_\theta = e^{t\mathcal{L}(\theta)}$ 关于适当的算子范数具有一致的 Lipschitz 控制，而 (Θ, d, μ) 上的列维型或 McDiarmid 型集中性再次意味着可区分比例呈指数级小。应用于我们的线性随机林德布拉德嵌入后，这将导出一个指数级的 QPStat 查询下界，用于以菱形距离学习量子信道 $\{E_\theta\}$，如定理 12所述。在第 X节中，我们将把这两种访问模型与我们的统计查询和 QPStat 困难性结果结合起来，构造分布级及基于层析的 Lindbladian-PUF。

现在我们具体说明随机局域林德布拉德系综，它将作为统计查询和 QPStat 分析共同的基础。

定义 1 (随机局域林德布拉德系综)。 考虑一个由 N 个量子比特组成的系统，其希尔伯特空间为 $H = (\mathbb{C}^2)^{\otimes N}$，维数为 $d = 2^N$。令 $B(H)$ 表示 H 上的有界算子代数。

1. 固定一个满足 *GKSL* 条件的参考 *Lindblad* 生成元 L_{ref}： $B(H) \to B(H)$。将其对应的量子马尔可夫半群（*QMS*）记为

$$\Lambda_t^{(\text{ref})} := e^{t\mathcal{L}_{\text{ref}}}.$$

2. 构造一族局部 *Lindblad* 耗散子 $\{G_j\}_{j=1}^M$，其中每个 G_j 都是耗散子的线性组合

$$\mathcal{D}_\alpha(\rho) = L_\alpha \rho L_\alpha^\dagger - \frac{1}{2}\{L_\alpha^\dagger L_\alpha, \rho\},$$

与局部跳跃算符 L_α 相关联。假设存在一个常数 $C_G > 0$ （与 M 无关），使得

that

$$\|G_j\|_{1\to 1} \le C_G, \qquad j = 1, \dots, M. \tag{2.1}$$

3. 取参数空间为实球面

$$S^{M-1} := \{\theta \in \mathbb{R}^M : \ \|\theta\|_2 = 1\},$$

并令 μ_{sph} 表示该球面上的一致（*Haar*）测度。给定扰动幅度 $\delta > 0$，定义随机林布拉德算子

$$\mathcal{L}(\theta) := \mathcal{L}_{\mathrm{ref}} + \frac{\delta}{\sqrt{M}} \sum_{j=1}^{M} \theta_j G_j, \qquad \theta \in S^{M-1}. \tag{2.2}$$

当 δ 足够小时，引理 *9*保证所有 $\mathcal{L}(\theta)$ 仍然是有效的 *GKSL* 生成元。将相应的量子马尔可夫半群记为

$$\Lambda_t^{(\theta)} := e^{t\mathcal{L}(\theta)}.$$

4. 固定演化时间 $t > 0$、初态 $\rho_{\mathrm{in}} \in S_d^+$，以及有限结果集合 X 上的 *POVM* $\{M_x\}_{x\in X}$。对每个 θ，定义输出测量分布

$$P_{\mathcal{L}(\theta)}(x) := \mathrm{Tr}\big(M_x\, \Lambda_t^{(\theta)}(\rho_{\mathrm{in}})\big), \qquad x \in X. \tag{2.3}$$

在统计查询模型中，学习器只能通过期望值 $P_{\mathcal{L}(\theta)}[\varphi]$ 访问 $P_{\mathcal{L}(\theta)}$。

5. 同时，对于每个 θ，我们将 *CPTP* 映射视为

$$E_\theta := \Lambda_t^{(\theta)}$$

在 *QPStat* 模型中作为待学习的量子信道。第 *VE*节所研究的 *QPStat* 预言机会针对任意量子态 迹[$O\, E_\theta(\rho)$] S $\rho \in \mathsf{S}(\mathcal{H})$ 和算子 $O \in \mathcal{B}(\mathcal{H})$，在满足 $\|\rho\|_1 \le 1$ 且$\|O\|_\infty \le 1$ 的条件下，提供具有指定容差的近似值。

C. 学习困难性与密码学应用

我们的第二组结果关注随机 Lindblad 算子系综的学习复杂度及其密码学应用。在分布方面，我们证明，由一种具有物理自然性的随机 Lindblad 算子系综诱导的经典输出统计，在平均情形下，在统计查询模型中具有指数级学习困难性。在过程方面，我们为针对量子信道的期望值查询引入了 QPStat 预言机模型，并证明了一个类似的指数级困难性结果：在菱形范数下学习随机 Lindblad 通道具有指数级困难性。最后，我们结合这两种查询模型，设计了两个系列的林德布拉德算子物理不可克隆函数（林德布拉德算子物理不可克隆函数），其安全性基于上述学习困难性结果。我们平均情形分析的技术基础是一条关于平均总变差距离的线性响应公式，以及一个显式的振幅阻尼模型，在该模型中，相关常数可以精确计算。

输出分布的统计查询困难性。我们首先固定一个具有物理自然性的随机 Lindblad 算子系综 $\mu_{\mathcal{L}}$，它通过参数球面 $\Theta = S^{M-1}$ 上的线性参数化 $\theta \mapsto \mathcal{L}(\theta)$ 构造而成，该参数球面的维数为 M；同时考虑一个单次测量接口（t，ρ_{in}，$\{M_x\}_{x\in X}$），它为每个 Lindblad 算子 $\mathcal{L}$ 诱导一个经典输出分布 $P_{\mathcal{L}} \in \mathcal{D}_X$。在统计查询模型中，学习器只能通过容差为 τ 的统计查询$P_{\mathcal{L}}[\varphi]$ 访问该分布，而不能获取单个样本。

一个关键的几何性质是，对于任意 SQ测试函数 $\varphi : X \to [-1, 1]$，相应的映射

$$F_\varphi(\theta) := P_{\mathcal{L}(\theta)}[\varphi]$$

在参数球面上具有与维数无关的利普希茨常数（引理12），并且 Θ 满足列维型集中不等式（定理10）。等价地，若 Q 表示系综平均分布$Q[\varphi] = \mathbb{E}_{\mathcal{L}\sim\mu_{\mathcal{L}}} P_{\mathcal{L}}[\varphi]$，则最大可区分比例

$$\max_{\varphi:X\to[-1,1]} \Pr_{\mathcal{L}\sim\mu_{\mathcal{L}}} \left[|P_{\mathcal{L}}[\varphi] - Q[\varphi]| > \tau\right]$$

按 exp(−Ω(M)) 衰减。

为了刻画典型实例的复杂度，我们引入开放系统波特–托马斯均值假设（假设 1），该假设指出，对于某个参考分布 Q，平均总变差距离 $\mathbb{E}_{\mathcal{L}\sim\mu_{\mathcal{L}}} d_{\mathrm{TV}}(P_{\mathcal{L}},\ Q)$会收敛到一个常数 $m_0 > 0$，当 $M \to \infty$时。结合参数 $d_{\mathrm{TV}}(P_{\mathcal{L}},\ Q)$ 的 Lipschitz 界θ （引理 19），即可得到一个“远离 Q”的体积估计（定理 14），进而得到平均情形 SQ 下界。

定理 *1*（判定问题的确定性平均情形 *SQ* 困难性（非正式表述））。假设定理 *10* 和假设 *1* 的结论成立，因此定理 *14* 适用。固定精度参数 ϵ、$\tau \in \in (0,\ 1)$ 以及一个与 M 无关的覆盖参数 $\beta \in \in (0,\ 1)$。考虑以下判定问题：给定对未知分布 $P \in \{Q\} \cup \{P_{\mathcal{L}} : L \sim \mu_{\mathcal{L}}\}$ 的统计查询预言机访问，判定 $P = Q$ 或 P 是否来自林德布拉德算子系综 $\mu_{\mathcal{L}}$。

那么，当 M 足够大时，任何使用不超过 q 次查询、容差为 τ 的确定性统计查询算法，若能在 $\mu_{\mathcal{L}}$ 测度至少为 β 的 *Lindblad* 算子子集上正确解决该任务，则必须满足

$$q_{\mathrm{det}}^{\text{avg-dec}}(\epsilon, \tau; \beta) \geq \beta\, \exp(cM),$$

w其中，$c > 0$ 仅取决于系综的几何常数，与 M 无关 .

定理 2（判定问题的随机化平均情形 SQ 困难性（非正式表述））。在与定理 *1* 相同的系综假设下，取常数 ϵ、$\tau \in$（0、1）以及 $\alpha > 1/2$、$\beta \in$（0、1）。任何随机化 *SQ* 算法若以至少 α 的成功概率（关于其内部随机性）在 $P = Q$ 与 $P \sim \mu_{\mathcal{L}}$ 之间作出正确判定，并且该判定在 $\mu_{\mathcal{L}}$ 测度至少为 β 的 *Lindblad* 算子子集上成立，则必须满足

$$q_{\mathrm{rand}}^{\text{avg-dec}}(\epsilon, \tau; \alpha, \beta) \geq (\alpha - \tfrac{1}{2})\, \beta\, \exp(cM),$$

其中，$c > 0$ 与 M 无关。

定理 *3*（学习开放系统动力学的平均情形 *SQ* 困难性（非正式表述））。在定理 *1* 的系综假设下，取常数 ϵ、$\tau \in$（*0*，*1*）以及参数 $\alpha > 1/2$、$\beta \in$（*0*，*1*）。考虑以下 *SQ* 学习任务：通过固定时间 t、输入态 ρ_{in} 和有限 *POVM*$\widehat{\quad}$ $\widehat{\quad}$接口，获取关于未知 $L \sim \mu_{\mathcal{L}}$ 的 *SQ* 预言机访问，输出满足 $d_{\mathrm{TV}}(P,\ P_{\mathcal{L}}) < \epsilon$ 的假设分布 P。我们只要求该目标在 $\mu_{\mathcal{L}}$ 测度至少为 β 的 *Lindblad* 算子子集上成立；对于随机化算法，成功概率还必须至少为 α。

那么，对于充分大的 M，有

$$q_{\mathrm{det}}^{\text{avg-learn}}(\epsilon, \tau; \beta) \gtrsim \beta\, \exp(cM), \qquad q_{\mathrm{rand}}^{\text{avg-learn}}(\epsilon, \tau; \alpha, \beta) \gtrsim (\alpha - \tfrac{1}{2})\, \beta\, \exp(cM),$$

因此，确定性和随机化的平均情形 *SQ* 学习复杂度均关于 M 呈指数级增长。

我们的平均情形学习复杂度结果是利用“远离 Q”技术证明的，但我们还建立了“远离 D”的结果，表明随机 Lindblad 算子的典型输出无法被任何固定的低复杂度经典模型近似。

具体而言，定理 15 表明，对于满足 Lipschitz-Lévy 集中和开放系统波特–托马斯均值假设的参数球面系综，以指数级接近1的概率，输出分布 $P_{\mathcal{L}}$ 与任意预先指定的经典分布 $\varepsilon_* > 0$ 之间的全变差距离至少为一个常数 D，且“坏”集合的测度随 M呈指数级衰减。从计算复杂性理论视角来看，这与 Aaronson 和 Chen 关于随机量子电路输出的猜想 [AC16] 密切相关，也构成了这样一种直觉的基础：不存在固定的低复杂度经典分布族，能够近似大多数随机林布拉德算子的输出。

学习随机 *Lindblad* 信道的 *QPStat* 困难性。 上述统计查询结果是针对经典输出分布表述的。在第 VE节中，我们还考虑一种过程学习模型，其中学习器可以通过 QPStat 预言机访问信道 $E_\theta := \Lambda_t^{(\theta)} = e^{t\mathcal{L}(\theta)}$：对于任意输入态 ρ 和可观测量 O，一次预言机查询会返回 $\mathrm{Tr}(O\,E_\theta(\rho))$ 的近似值，其加性容差为 τ。

对于相同的参数球面系综（Θ，μ_Θ），我们证明，平均而言，将其底层信道学习到较小的菱形距离以内同样具有指数级困难。

定理 4（学习随机 Lindblad 信道的指数级 QPStat 困难性（非正式表述））。 设 $E_\theta = \Lambda_t^{(\theta)}$ 为定义 *1* 中球面随机扰动 *Lindblad* 生成元系综所生成的信道，并令 μ_Θ表示参数球面测度。考虑容差为 τ （如定义 *17* 所述）的 *QPStat* 预言机访问，并固定精度 $\epsilon > 0$ 和覆盖率 $\beta \in$ （0，1）。

任何（可能是量子的）*QPStat* 学习算法，若至多使用 q 次 *QPStat* 查询，并以成功概率^ ^至少为 $\alpha > 1/2$ 输出一个假设通道 E，使其满足 $\|E - E_\theta\|_\diamond \le \epsilon$，且该条件对参数的某个子集成立，该子集的 μ_Θ- 测度至少为 β，则必须满足

$$q \ge (\alpha - \tfrac{1}{2})\,\beta\,\exp\!\Big(c\,\frac{M\tau^2}{L_*^2}\Big) = (\alpha - \tfrac{1}{2})\,\beta\,\exp\big(\Omega(M)\big),$$

其中 L_* 是映射 $\theta \mapsto$迹$\big(O\Lambda_t^{(\theta)}$ （ρ） $\big)$ （引理 *16*）的一个与维数无关的利普希茨常数，而 $c > 0$与 M无关。定理 *12* 给出了精确表述。

因此，对于我们的随机 Lindblad 系系综，不仅诱导的输出分布，而且其底层信道本身，在自然的期望值预言机模型中都难以学习，且困难程度呈指数级。

基于随机 *Lindblad* 算子系综的物理不可克隆函数。 上述学习困难性结果对密码学有直接影响。在第 X节中，我们将利用这些结果，构造两个基于随机 Lindblad 算子系综的物理不可克隆函数族。

(A) 带 SQ 接口的分布级 Lindblad 物理不可克隆函数（方案 A）：挑战是一个参数 θ，设备实现相应的随机 Lindblad 通道 $E_\theta = e^{t\mathcal{L}(\theta)}$，而我们只考虑经过固定测量 $(t, \rho_{\text{in}}, \{M_x\})$ 后得到的经典输出分布 P_θ。在可信工厂阶段，验证者（制造商）拥有样本级访问权限，并为 P_θ 登记概率指纹；部署后，向任何外部用户（包括建模对手 A）开放的物理设备只提供 SQ 接口 $\mathrm{Stat}_\tau(P_\theta)$。方案 A 使用一个规模呈指数级的 Hadamard 型测试函数族 $\mathrm{F}_{\mathrm{Had}} = \{\varphi_{\mathrm{BIT}} : \mathrm{BIT} \in \{0,1\}^L\}$（定义 28）作为挑战空间：在每个认证轮次中，验证者从 $\mathrm{F}_{\mathrm{Had}}$ 中抽取一个新的 φ_{BIT}，并检查 SQ 回复是否与登记的指纹值一致（定义 30）。由于 $\mathrm{F}_{\mathrm{Had}}$ 构成 D_X 的层析完备 Hadamard 型基，通过验证意味着对手实际上已经学会了底层输出分布，且全变差距离很小；与此同时，任何试图预先计算 $\mathrm{F}_{\mathrm{Had}}$ 中所有挑战对应 SQ 答案的查表策略，都需要进行指数级数量的 SQ 查询。SQ 安全性定理（定理 18）对此作了形式化说明：即使不对 A 的内部策略施加任何结构限制，任何仅通过 SQ 接口 $\mathrm{Stat}_\tau(P_\theta)$ 进行访问、并以非忽略成功概率冒充诚实设备的对手，都必须针对参数维数 M 发起指数级数量的 SQ 查询；而诚实验证者的登记与验证成本在 $|X|$ 和 $1/\tau$ 上仍为多项式级。

(B) 基于层析的 Lindbladian-PUF（方案 B）：在具有输入算子和可观测量的一个信息完备族的扩展 QPStat 模型中，我们定义一个层析指纹映射 $\mathcal{T}$，它将每个信道 E_θ 映射为一个有限的期望值列表（定义 32）。引理 33 表明，$\mathcal{T}$是实线性且为单射，并且由此导出的层析范数 $\|\cdot\|_{\mathrm{tom}}$ 与菱形范数 $\|\cdot\|_\diamond$等价。在方案 B 中，验证者在注册时存储 $\mathcal{T}(E_\theta)$，之后通过要求证明者（在容差范围内）重现整个层析指纹矩阵来进行认证（定义 33）。因此，从信息论的角度来看，通过验证等价于已在菱形距离意义下学得 E_θ。

在这两种方案中，任何成功构造出 PUF 经典模拟器的建模对手，都必然解决了相应的统计查询或 QPStat 学习问题，因此面临指数级查询复杂度。

定理 5（基于学习困难性的 Lindbladian-PUF 安全性（非正式表述））。 对于上文考虑的随机 *Lindblad* 系综：

(i) 方案 *A*（带 *SQ* 接口的概率指纹 *Lindbladian-PUF*）。在定理 *3* 的 *SQ* 困难性假设成立，且满足定义 *28* 中的 *Hadamard* 测试函数构造时，任何对手 A在设备离开工厂后与其交互，且仅通过 *SQ* 预言机 $\mathrm{Stat}_\tau(P_\theta)$，并试图在方案 *A* 中冒充诚实设备，且成功概率至少为 $\alpha_{learn} > 1/2$，对至少 $\mu_{\mathcal{L}}$比例的挑战，必须进行

$$q_{\mathrm{adv}}^{\mathrm{SQ}} \gtrsim (\alpha_{learn} - \tfrac{1}{2})\, \beta_{learn}\, \exp(cM)$$

次统计查询（定理 *18*）。这里我们不对 A的内部策略施加任何结构限制：它可以是任意算法（可能经过随机化），只要它与物理设备的所有交互都通过 *SQ* 接口进行即可。相比之下，诚实验证者的登记与验证成本仅随系统规模和 $1/\tau$多项式增长。

(ii) 方案 *B*（基于层析的 *Lindbladian-PUF*）。在定义 *31*的扩展 *QPStat* 模型中，若要在较小的层析范数（等价地，菱形范数）误差范围内冒充方案 *B* 中的设备，就能得到一个 *QPStat* 学习器，使其在系综中占不可忽略比例的部分上以 ε精度学习底层信道。根据定理 *4* 及其正式版本定理 *12*，任何此类对手都必须在参数维数 M *(* 定理 *19)* 下使用指数级数量的 *QPStat* 查询。同时，层析指纹 $\mathcal{T}(E_\theta)$ 有 $D^2 \sim d^4$ 个条目，因此诚实验证者的登记与验证成本也按 d^4的量级增长；对于参数维数 M 关于 d呈多项式增长的典型局域 *Lindbladian* 模型，这一成本与信道本身的信息内容相当。因此，方案 *B* 应被视为信息论基准，而非可高效验证的密码协议。

从概念上说，这些 Lindbladian-PUF 构造展示了如何将随机林德布拉德系综的学习困难性转化为切实的密码学安全保证，这既适用于经典输出分布，也适用于完整的量子信道。方案 A 实现了一种真正可高效验证的 Lindbladian-PUF，其验证成本为多项式级，而任何 SQ 建模攻击都需要指数级计算量；相比之下，方案 B 实现了菱形范数控制，但必须付出量级为 d^4 的自然层析成本，凸显了基于层析的场景中安全性与验证成本之间的权衡。

技术工具：线性响应与显式模型。为支持上述平均情形结果，我们开发了两种技术工具。首先，我们推导出平均总变差距离的线性响应解析表达式

$$m(\delta) := \mathbb{E}_{\theta\sim\mu_\Theta} d_{\mathrm{TV}}\big(P_{\mathcal{L}(\theta)}, Q\big),$$

该表达式明确追踪其对参数维数 M 以及一阶响应系数向量 $\{a_{j,\,x}\}$的依赖，并将非零平均常数这一物理要求归结为关于$\sum_x \|a^{(x)}\|_2$的广延性条件。

定理 6（平均总变差距离的线性响应解析标度（非正式））。 在定义 *1*和引理 *22*的设定下，令

$$F_{\mathrm{TV}}(\theta) := d_{\mathrm{TV}}\big(P_{\mathcal{L}(\theta)}, Q\big) = \frac{1}{2}\sum_{x\in X}\big|P_{\mathcal{L}(\theta)}(x) - Q(x)\big|, \quad m(\delta) := \mathbb{E}_{\theta\sim\mu_\Theta} F_{\mathrm{TV}}(\theta),$$

并定义

$$a^{(x)} := \big(a_{1,x}, \ldots, a_{M,x}\big) \in \mathbb{R}^M, \qquad \|a^{(x)}\|_2 := \Big(\sum_{j=1}^{M} a_{j,x}^2\Big)^{1/2},$$

其中 $a_{j,\,x}$ 由一阶响应公式式（8.2）给出。

那么在小噪声极限 $\delta \to 0$ （线性响应区域）下，有

$$m(\delta) = \delta\, m_0(M) + O(\delta^2), \qquad m_0(M) := \frac{\kappa_M}{2M}\sum_{x\in X}\|a^{(x)}\|_2,$$

其中 κ_M 是由球面几何确定的系数（式 (8.7)），并满足 $\kappa_M \to \sqrt{2/\pi}$ 当 $M \to \infty$时。特别地，在高维极限下，

$$m(\delta) = \delta \cdot \frac{\sqrt{2/\pi}}{2M} \sum_{x \in X} \|a^{(x)}\|_2 + O(\delta^2) + o(\delta).$$

这为开放系统波特–托马斯均值假设提供了一个精确的线性响应解析版本，$\mathbb{E}_\theta d_{\mathrm{TV}}(P_{\mathcal{L}(\theta)}, Q) \approx m_0 > 0$。

(i) 若一阶响应系数在极限 $M \to \infty$下满足广延性标度 ，

$$\frac{1}{M} \sum_{x \in X} \|a^{(x)}\|_2 \longrightarrow c_a > 0,$$

则存在一个与 M 无关的常数 $c'_a > 0$，使得 $m(\delta) \approx c'_a \, \delta$，因此平均总变差距离保持为 $O(\delta)$阶，且其常数前因子非零。

(ii) 反过来，若 $\sum_x \|a^{(x)}\|_2 = o(M)$，则 $m_0(M) \to 0$，且平均总变差距离会随系统规模增大而减小；在此情形下，典型的 $P_{\mathcal{L}(\theta)}$ 在全变差距离意义下趋近于 Q，基于 $d_{\mathrm{TV}}(P_{\mathcal{L}}, Q)$的统计查询困难性判据无法给出非平凡的下界。

严格版本见定理 *16* 和注释 *24*。

其次，我们通过计算该模型中一阶响应系数的平均范数，验证了在一个简单但完全显式的一维随机局域振幅阻尼模型中存在正的均值常数 $m_0 > 0$ 。

定理 7（随机局域振幅阻尼模型中的均值标度常数的显式计算（非正式））。 在定义 *27*的随机局域振幅阻尼林布拉德模型中，考虑由 N 个量子比特组成的一维链，

$$\mathcal{H} = (\mathbb{C}^2)^{\otimes N}, \quad M := N,$$

取平凡的参考演化 $L_{\mathrm{ref}} = 0$，并令初态为 $\rho_{\mathrm{in}} = |1 \cdots 1\rangle\langle 1 \cdots 1|$。在每个位点 j，引入一个局域振幅阻尼跳跃算符

$$J_j^{(-)} := \sqrt{\gamma}\, \sigma_j^-, \qquad G_j := \mathcal{D}_j^{(-)},$$

并使用计算基正算子值测度 $\{M_x = |x\rangle\langle x|\}^{x \in \{0,1\}^N}$ 测量输出。

在这个特定的 模型中，可以显式计算一阶响应系数 $\{a_{j,\,x}\}$，并证明

$$\frac{1}{M} \sum_{x \in X} \|a^{(x)}\|_2 = \gamma t \Big(1 + \frac{1}{\sqrt{M}}\Big),$$

将其代入一般线性响应表达式后，可得

$$m(\delta) = \delta \cdot \frac{\kappa_M}{2} \gamma t \Big(1 + \frac{1}{\sqrt{M}}\Big) + O(\delta^2),$$

其中 κ_M 与上文相同。令 $M \to \infty$，并使用 $\kappa_M \to \sqrt{2/\pi}$，我们得到

$$m(\delta) \xrightarrow[M \to \infty]{} m_\ell \, \delta + O(\delta^2), \qquad m_\ell := \gamma t \sqrt{\frac{1}{2\pi}} > 0.$$

也就是说，

$$\mathbb{E}_\theta \, d_{\mathrm{TV}}\big(P_{\mathcal{L}(\theta)}, Q\big) = m_\ell \, \delta + O(\delta^2), \qquad m_\ell > 0,$$

其线性前因子 m_ℓ 与 M无关。这表明，经过适当归一化后，开放系统波特–托马斯均值假设中的要求$m_0 > 0$，可以在一个简单且物理上可实现的玩具模型中得到严格验证。

这两个技术结果说明，我们在平均情形 SQ 困难性定理中采用的平均距离假设并非随意设定，而是源于明确的几何考量和依赖于模型的因素。

III. 讨论与展望

在这项工作中，我们从一个看似简单却至关重要的问题出发：在演化时间和测量资源有限的条件下，能否仅凭单一时刻演化的统计信息，可靠地重构作用于高维开放量子系统的噪声与耗散结构？为此，我们在 GKSL 生成元锥的仿射包上构造了一类符合物理直觉的随机林德布拉德算子系综，并将经典统计查询（SQ）学习和量子过程统计查询（QPStat）学习的框架系统地应用于开放系统场景。基于这一统一视角，我们得到了关于平均情形学习复杂度的一系列指数下界，继而将这些复杂度结果转化为由随机林德布拉德算子驱动的 Lindblad-PUF 协议的密码学安全性条件，由此确立了开放系统动力学、学习理论与量子密码学之间的清晰联系。

从概念上看，本工作的核心结构要素是线性参数化与度量测度空间的结合。我们首先证明，GKSL 锥的仿射包可以通过超算子的有限维基以及一个参考 Lindblad 生成元实现完整的线性参数化，从而在超算符空间中得到形如 $\mathcal{L}(\theta)$ 的一族局部 Lindblad 算子。在此基础上，我们不直接在 GKSL 锥上施加测度，而是首先在参数空间上选取几何性质良好的度量测度结构（例如具有旋转对称性的高维球面系综，或具有独立局部耦合的乘积系综），即 (Θ, d, μ)，然后将其向前推送到林布拉德空间。这一思想受到随机量子电路中 Haar 测度或设计测度构造的启发，但在技术上，我们必须处理来自刘维尔半群和局部 Lindblad 算子的额外约束，才能得到真正的度量测度 Lindbladian 系综。

在这一几何与测度论框架下，我们系统地分析随机林德布拉德算子的学习复杂度。在分布层面，一旦固定单次测量接口，每个 Lindblad 算子都会诱导一个经典输出分布，而学习器只能通过统计查询（SQ）查询访问该分布的期望值。我们证明，对于任意有界测试函数，从参数到期望值的映射在参数空间上具有与维数无关的利普希茨常数；在球面模型和乘积测度模型中，该映射分别满足列维集中不等式和 McDiarmid 集中不等式。结合现有的一般 SQ 下界技术，我们直接得到测试与学习问题的查询复杂度均随参数维数呈指数增长：即使只要求在一个测度非零的子集上取得成功，对典型随机 Lindblad 输出分布的平均情形学习在 SQ 意义下仍然极其困难。在通道层面，我们提出一种专为 Lindblad 算子设计的 QPStat 访问模型，允许学习器以有限容差查询演化信道的期望值。我们证明，在相同的参数空间结构下，从参数到信道的映射相对于适当的算子范数也满足一致的 Lipschitz 条件，由此得到平均情形下以菱形距离衡量的学习问题具有指数级 QPStat 查询下界。该结果表明，即使在开放系统场景中，即使我们只关心有限时间的 CPTP 演化，典型 Lindblad 通道在过程层面仍表现出很强的平均情形不可学习性；在结构上，这与封闭系统中随机酉电路的 SQ 或 QPStat 困难性结果相类似。

为了赋予上述平均情形下界明确的物理内涵，我们提出并分析了 Porter-Thomas 型“平均总变差距离假设”的开放系统版本：在适当的归一化和参数缩放下，随机 Lindblad 输出分布与固定参考分布之间的平均总变差距离，在高维极限下收敛到一个严格为正的常数。借助类 Kubo 一阶响应展开，我们将这一假设归结为一阶响应系数向量的几何性质。针对局域随机振幅阻尼链这一具体模型，我们明确计算了这些系数的缩放行为，以及平均全变差距离对参数维数和演化时间的依赖，并表明，在物理上自然的小

噪声和局部跳跃算符参数区间内，平均距离始终与零保持正距离。结合数值模拟，这一结果确立了一个统一的物理图景，将微观的 Lipschitz-Lévy 控制与平均全变差距离的宏观缩放联系起来。

在密码学方面，我们基于随机林布拉德算子构造了两类 Lindbladian-PUF 协议。第一类方案完全在分布层面运行。其验证接口被刻意限制为对输出分布的统计查询访问，其安全性直接源于分布学习的 SQ 困难性。第二类方案允许有限次 QPStat 查询或实验层析；我们在一个恰当的算符基中引入层析指纹，并利用相关层析指纹范数与菱形范数之间的等价关系，将信道不可克隆性转化为学习 Lindblad 信道的 QPStat 困难性。尽管从密码学角度看，后一类方案的验证成本并不理想，但两种方案共同展示了开放系统场景中的一个基本观点：只要在协议设计中谨慎约束验证者和对手可获取的信息结构，就能自然地将学习复杂度的平均情形指数下界转化为 Lindbladian-PUF 的安全约束。

展望未来，我们预计这里建立的框架可以沿多个方向扩展和深化。一个直接的延伸方向是考虑更一般的林德布拉德算子系综和非马尔可夫效应。本文目前主要关注局部 GKSL 生成元的线性扰动模型，这些模型具有天然的局限性。因此，进一步研究满足细致平衡的 Davies 生成元、具有能量选择结构的热 Lindbladian，甚至带有弱非马尔可夫记忆核的有效 Lindbladian 近似，都是很有意义的。理解如何在这些更复杂的噪声模型中保持良好的度量测度结构和集中性质，是刻画更现实开放系统“典型复杂度”的关键一步。

其次，我们的结果表明，随机林德布拉德算子在 SQ 和 QPStat 模型下已经表现出某种形式的开放系统伪随机性。一个自然的长期目标是在我们的构造基础上，定义并刻画“伪随机 Lindbladian”，并将其与量子伪随机电路、噪声工程和开放系统密码学联系起来。这最终可能促成酉t-设计和伪随机酉矩阵的开放系统类比。

第三，探索更强访问模型下的量子学习优势是很自然的。本文聚焦于通过统计查询和 QPStat 进行相对较弱的访问。一个重要问题是：在允许使用量子样本、量子统计查询或轨迹级数据的模型中，是否存在经典统计查询困难、但量子统计查询易解的开放系统任务，从而展现植根于耗散和环境的真正量子学习优势。在这方面，将本文引入的林德布拉德算子系综纳入生成式量子优势框架，或可带来新的分离结果。

此外，深入探索与实验噪声和含噪声中等规模量子硬件的联系也很有价值。我们的局部随机 Lindbladian 和振幅阻尼链模型，在结构上与超导量子比特、囚禁离子及其他平台上遇到的噪声有某些相似之处，但它们仍是理想化模型。因此，将满足我们假设的随机林布拉德算子模型拟合到特定硬件架构上，利用实验数据验证 Lipschitz-Lévy 集中性及平均全变差距离的标度关系，并直接在硬件上实现简化的 Lindbladian-PUF 原型，都是自然而重要的方向。

最后，可学习复杂度、统计力学与热力学之间可能存在的联系尤其引人入胜。林德布拉德动力学内在地编码了熵产生率和热流等非平衡热力学量。结合我们的平均情形难学习结果，这引出了一个问题：难以学习的林德布拉德动力学是否必然伴随着某种极端热力学行为？能否据此在学习复杂度、混合时间与非平衡统计力学之间建立更紧密的联系？

总体而言，这项工作表明，在开放系统和林德布拉德动力学的背景下，“典型性”与“复杂度”仍是一体两面：一方面，随机林德布拉德算子表现出强烈的测度集中性，并在参数空间中呈现典型行为；另一方面，在统计查询和 QPStat 等弱访问模型下，它们的输出分布和量子信道表现出内在的平均情形不可学习性。我们希望这项工作能成为进一步研究开放系统中随机性、复杂度与可学习性的起点，并在未来推动这些研究与量子优势、噪声工程和量子密码学之间开展更多交叉探索。

致谢：我们感谢 Ming-Cheng Chen、Chao-Yang Lu、Yi-En Liang 和 Zhong-Xia Shang 提供的

宝贵讨论。C. C. 受到国家自然科学基金（编号：124B100020）的资助。R. B. 受到 JSPS KAKENHI Grant No. 25KJ0766 的资助。

IV. 预备知识

A. 范数约定与基本不等式

在本小节中，我们统一本文后续用于表示 Lipschitz 常数、集中估计以及 Lindblad 算子稳定性分析的几种范数记法。我们主要参考的书籍是 [Bha13]和 [Wat18]。

定义 2（参数空间上的欧几里得范数）。 设参数向量为 $\theta = (\theta_1, \ldots, \theta_M) \in \mathbb{R}^M$。定义

$$\|\theta\|_2 := \Big(\sum_{j=1}^{M} \theta_j^2\Big)^{1/2}, \qquad \|\theta\|_1 := \sum_{j=1}^{M} |\theta_j|, \qquad \|\theta\|_\infty := \max_{1\le j\le M} |\theta_j|. \tag{4.1}$$

特别地，本文中的随机林布拉德算子的参数通常取自单位球面$S^{M-1} := \{\theta \in \mathbb{R}^M : \ \|\theta\|_2 = 1\}$。

定义 3（算子的 Schatten 范数）。 设 $H \cong \mathbb{C}^d$ 且 $B(H)$ 为其上的有界算子代数。对于任意 $A \in B(H)$，以 $s_1, \ldots, s_d \ge 0$ 表示其奇异值。对于 $p \in [1, \infty]$，定义 *Schatten* p-范数为

$$\|A\|_1 := \sum_{i=1}^{d} s_i = \operatorname{Tr}\sqrt{A^\dagger A} \quad \textit{(trace norm)}, \tag{4.2}$$

$$\|A\|_2 := \Big(\sum_{i=1}^{d} s_i^2\Big)^{1/2} = \big(\operatorname{Tr}(A^\dagger A)\big)^{1/2} \quad \textit{(Hilbert-Schmidt norm)}, \tag{4.3}$$

$$\|A\|_\infty := \max_i s_i = \sup_{\|\psi\|=1} \|A\psi\| \quad \textit{(operator norm)}. \tag{4.4}$$

特别地，当 A 是可观测量时，$\|A\|_\infty$ 是其谱半径（特征值绝对值的最大值）。

备注1 (Schatten 范数之间的关系)。 在 d 维空间中，*Schatten* 范数满足标准的夹逼不等式：

$$\|A\|_\infty \le \|A\|_2 \le \|A\|_1 \le \sqrt{d}\,\|A\|_2 \le d\,\|A\|_\infty. \tag{4.5}$$

本文使用迹距离 $\|\rho - \sigma\|_1$ 来量化量子态之间的几何距离，而 $\|O\|_\infty$ 则出现在 *Hölder* 不等式 $|\operatorname{Tr}(OX)| \le \|O\|_\infty \|X\|_1$ 中，并作为许多 *Lipschitz* 界的基本工具。

定义 4 (由 Schatten 范数诱导的超算子范数，参见 [Wat18、Wat04])。 设 $\mathcal{T}\colon \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$ 是一个线性超算子。对于给定的 *Schatten* 范数 $\|\cdot\|_p, \|\cdot\|_q$，定义诱导的 $p \to q$ 范数如下

$$\|\mathcal{T}\|_{p\to q} := \sup_{X\neq 0} \frac{\|\mathcal{T}(X)\|_q}{\|X\|_p}. \tag{4.6}$$

本文中最常用的情形是 $p = q = 1$:

$$\|\mathcal{T}\|_{1\to 1} := \sup_{X\neq 0} \frac{\|\mathcal{T}(X)\|_1}{\|X\|_1}. \tag{4.7}$$

当我们写作 $\|\Lambda^{(\mathcal{L}')}{}_t - \Lambda_t^{(\mathcal{L})}\|_{1\to 1}$ 时，指的是上述意义下由迹范数诱导的 $1 \to 1$ 范数。

注 2（诱导的 $1 \to 1$ 范数与迹距离收缩）。 若 Λ_t 是一个 *CPTP* 映射（例如由 *GKSL* 生成元 L 生成的量子马尔可夫半群中的一个元素），那么对于任意算子 X，

$$\|\Lambda_t(X)\|_1 \le \|X\|_1, \tag{4.8}$$

因此 $\|\Lambda_t\|_{1\to1} \le 1$。对于密度矩阵 ρ,σ，这等价于迹距离收缩： $\|\Lambda_t(\rho) - \Lambda_t(\sigma)\|_1 \le \|\rho-\sigma\|_1$. 本文讨论两种 *Lindblad* 演化之间的差异时，通常通过 $\|\Lambda^{(\mathcal{L}')}{}_t - \Lambda_t^{(\mathcal{L})}\|_{1\to1}$来控制相应测量分布的全变差距离。

定义 5 (菱形范数**)**。 设 T :$B(H) \to B(H)$ 是一个线性超算子。其菱形范数定义为

$$\|\mathcal{T}\|_\diamond := \sup_{k\ge1} \|\mathcal{T}\otimes \mathrm{id}_{\mathcal{H}_k}\|_{1\to1}, \tag{4.9}$$

其中 $H_k \cong \mathbb{C}^k$ ，且 $\mathrm{id}_{\mathcal{H}_k}$ 是恒等信道。在有限维情形下，上确界可限制为$k = d =$维数 H。特别地，对于两个量子信道 Φ,Ψ ，有

$$\frac{1}{2}\|\Phi-\Psi\|_\diamond = \sup_{\rho_{SA}} \frac{1}{2}\big\|(\Phi\otimes \mathrm{id}_A)(\rho_{SA}) - (\Psi\otimes \mathrm{id}_A)(\rho_{SA})\big\|_1, \tag{4.10}$$

也就是说，在允许使用辅助系统时，菱形距离给出了信道间最坏情况下的输出迹距离。

注释 3（菱形范数与诱导 $1 \to 1$ 范数之间的关系）。 一般而言，有

$$\|\mathcal{T}\|_{1\to1} \le \|\mathcal{T}\|_\diamond \le d\,\|\mathcal{T}\|_{1\to1}, \tag{4.11}$$

其中 $d =$ 维数H。因此，在没有辅助系统的情况下， $\|T\|_{1\to1}$ 是 $\|T\|_\diamond$的下界；当维数固定时，两者只相差一个多项式因子。本文主要使用 $\|\cdot\|_{1\to1}$ 来建立 *Lipschitz* 界；需要与标准信道距离（菱形范数）进行比较时，可以通过上述不等式在两者之间转换。

定义 6（经典函数与测量算子的上确界范数）。 在经典域 X 上，对于函数 φ： $X \to \mathbb{R}$ ，定义 $\|\varphi\|_\infty$ ： = 上确界$_{x\in X}|\varphi$（x）|. 在统计查询框架中，我们通常要求φ： $X \to [-1,1]$，从而有 $\|\varphi\|_\infty \le 1$。

在量子情形下，给定 *POVM* 或投影测量，我们通常将一个有界可观测量O_φ 与测试函数 φ 相关联，使得

$$P[\varphi] = \mathbb{E}_{x\sim P}[\varphi(x)] = \mathrm{Tr}(O_\varphi \rho),$$

且 $\|O_\varphi\|_\infty \le 1$(因为 $\|O_\varphi\|_\infty \le \|\varphi\|_\infty$ 在此情形下，证明见引理 *10*）。矩阵 *Hölder* 不等式|$\mathrm{Tr}(O_\varphi X)$ | $\le \|O_\varphi\|_\infty \|X\|_1$ 保证统计查询输出受量子态之间迹距离的 *Lipschitz* 控制。

备注 4 (本文中的统一约定**)**。 总结而言，本文中范数符号的默认含义如下：

- $\|\cdot\|_2$：对于参数向量，表示欧几里得范数；对于算子，表示希尔伯特–施密特范数（视上下文而定）；
- $\|\cdot\|_1$：对于算子，表示迹范数；对于分布之差，表示全变差距离的两倍；
- $\|\cdot\|_\infty$：对于算子，表示谱半径；对于函数，表示上确界范数；
- $\|\cdot\|_{1\to1}$：由迹范数诱导的超算子范数；
- $\|\cdot\|_\diamond$：量子信息中的标准菱形范数，仅在比较信道距离时出现。

下文中的所有利普希茨常数和集中不等式均基于上述范数约定。

B. GKSL生成元与量子马尔可夫半群

在本小节中，我们简要回顾 Gorini-Kossakowski-Sudarshan-Lindblad (GKSL) 定理及其相关结构，并确定本文所使用的 Lindblad 算子的记号和基本性质。我们的主要参考资料是 [RH12] 的第 5 章。

定义 7（量子马尔可夫半群与生成元）。 设 H 是有限维希尔伯特空间，B（H）是 H 上的有界算子代数。一族线性映射

$$\{\Lambda_t\}_{t\geq 0}, \qquad \Lambda_t : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H}),$$

若满足以下条件，则称其为量子马尔可夫半群（*QMS*）：

1. 半群性质： $\Lambda_0 = \mathrm{id}$ 且对于所有 $s, t \geq 0$, $\Lambda_{t+s} = \Lambda_t \circ \Lambda_s$;

2. 完全正性与迹保持性：对于每个 $t \geq 0$, Λ_t ，它都是完全正且保迹的（*CPTP*）；

3. 强连续性：对于每个 $\rho \in B$（H），映射 $t \mapsto \Lambda_t$（ρ）在迹范数下连续 .

在这些条件下，存在唯一的有界线性映射 $L : B(H) \to B(H)$ 使得

$$\Lambda_t = e^{t\mathcal{L}}, \qquad \frac{\mathrm{d}}{\mathrm{d}t}\rho(t)\big|_{t=0} = \mathcal{L}(\rho(0)),$$

其中 $\rho(t) := \Lambda_t(\rho(0))$。映射 L 称为该量子马尔可夫半群的（*Lindblad*）生成元。

定义 8（GKSL 形式与 Lindblad 生成元）。 在有限维情形下，生成元 $\mathcal{L}$ 生成定义 7 中的量子马尔可夫半群，当且仅当它可以写成 *GKSL*（*Lindblad*）形式 *[RH12]*：

$$\mathcal{L}(\rho) = -\mathrm{i}[H, \rho] + \sum_k \gamma_k \Big(L_k \rho L_k^\dagger - \frac{1}{2}\{L_k^\dagger L_k, \rho\} \Big), \tag{4.12}$$

其中

1. $H = H^\dagger$ 是有效系统哈密顿量；*2.* $\{L_k\}$ 是一族 *Lindblad*（跳跃）算子；*3.* 速率满足 $\gamma_k \geq 0$;

4. $\{\cdot, \cdot\}$ 表示反对易子。

满足这些条件的映射 L 称为 *GKSL* 生成元（或 *Lindblad* 算子）。我们将所有此类映射组成的集合记为 $\mathrm{GKSL} \subset \mathrm{End}(B(H))$。

注 5（GKSL 锥与仿射结构）。 由以下形式 (4.12) 可知：

i. 若 $L_1, L_2 \in \mathrm{GKSL}$ 且 $a, b \geq 0$，则 $aL_1 + bL_2$ 仍是 *GKSL* 生成元（可以相应地合并跳跃算符和速率）。因此，GKSL 在 $\mathrm{End}(B(H))$中构成一个闭凸锥。

ii. 固定一个参考 *Lindblad* 生成元 $L_{\mathrm{ref}} \in \mathrm{GKSL}$。其仿射包

$$\mathrm{Aff}(\mathrm{GKSL}) := \big\{ \mathcal{L}_{\mathrm{ref}} + V : \ V \in \mathrm{span}(\mathrm{GKSL} - \mathcal{L}_{\mathrm{ref}}) \big\}$$

是一个有限维实仿射空间。在本文中，我们取 $\mathrm{V} := \mathrm{Aff}(\mathrm{GKSL}) - L_{\mathrm{ref}}$ 作为 *Lindblad* 算子扰动的底层线性参数空间。

从物理上看，GKSL 描述了开放系统动力学中所有完全正、保迹且满足马尔可夫性的有效生成元；其凸性反映了这样一个事实：不同耗散通道的叠加可以用模型来描述。

注 6（Kossakowski 条件及与经典生成元的比较）。 对于经典有限状态马尔可夫过程，生成矩阵 Q 必须满足

$$Q_{ii} \le 0, \quad Q_{ij} \ge 0 \ (i \ne j), \quad \sum_j Q_{ij} = 0,$$

这保证了 e^{Qt} 是一个随机矩阵。*GKSL* 定理可以被视为这些条件的量子类比：根据 *Lumer-Phillips* 定理 *[LP61]* 可以证明，如果 $e^{t\mathcal{L}}$ 在迹范数下的自伴算子空间上构成一个压缩半群，并且$\mathcal{L}$ 是厄米保持且保迹的，那么它必定具有如下结构 (4.12)。反之，任何 $\mathcal{L}$ 若具有 (4.12) 的形式，都会生成一个 *CPTP* 压缩半群 *[RH12]*。

命题 1（迹范数收缩性与完全正性）。 设 L 是一个 *GKSL* 生成元，且 $\Lambda_t = e^{t\mathcal{L}}$。那么对于每个 $t \ge 0$ 以及任意密度算子 ρ、σ，

$$\|\Lambda_t(\rho) - \Lambda_t(\sigma)\|_1 \le \|\rho - \sigma\|_1. \tag{4.13}$$

更一般地，对于任意辅助系统 H_{anc}，映射 $\Lambda_t \otimes \mathrm{id}_{\mathcal{H}_{\text{anc}}}$ 在迹范数下也是一个压缩映射。这等价于 Λ_t的完全正性。

备注 7（海森堡绘景与对偶生成元）。 给定一个薛定谔绘景 *Lindbladian* L，其在海森堡绘景中的对偶生成元 $L^\dagger$满足

$$\frac{\mathrm{d}}{\mathrm{d}t}X(t) = \mathcal{L}^\dagger(X(t)), \qquad \mathrm{Tr}\big[\rho\,\mathcal{L}^\dagger(X)\big] = \mathrm{Tr}\big[\mathcal{L}(\rho)\,X\big],$$

and

$$\mathcal{L}^\dagger(X) = \mathrm{i}[H, X] + \sum_k \gamma_k \Big(L_k^\dagger X L_k - \frac{1}{2}\{L_k^\dagger L_k, X\} \Big).$$

海森堡绘景通常更便于讨论守恒量和能量耗散。在本文中，我们主要采用薛定谔绘景，但在引入能量密度和可观测量时，隐含地运用了上述对偶性。

定义 9（稳态、谱隙与本原性）。 设 $\mathcal{L}$ 是一个 *GKSL* 生成元。

1. 稳态（不动点）是满足 $L(\sigma) = 0.$ 的密度算子 σ 。若稳态唯一且满秩，则称该半群具有本原性。

2. 将 L 视为作用于 $B(H)$ 上的线性算子，其谱通常满足 $\lambda_1 = 0$，$R\lambda_k \le 0.$ 。谱隙定义为

$$\lambda := \min_{k \ge 2} |\Re\lambda_k| > 0.$$

在本原情形下，$\lambda > 0$ 意味着指数混合：$\|\Lambda_t(\rho) - \sigma\|_1 \le Ce^{-\lambda t}$，其中某个常数为 C，且对所有初态 ρ 都成立。

C. 统计查询学习模型

本节简要回顾统计查询（SQ）学习框架中使用的基本概念和符号 [NIS+25, Fel17]。

定义 10（分布、全变差距离与期望记号）。 设 X 为有限域，D_X 为 X上所有概率分布的集合。对于 P, $Q \in D_X$，其全变差（*TV*）距离定义为

$$d_{\text{TV}}(P, Q) := \frac{1}{2} \sum_{x \in X} |P(x) - Q(x)|. \tag{4.14}$$

给定 $\epsilon > 0$，以 P 为中心的开 ϵ球定义为

$$B_\epsilon(P) := \{Q \in \mathcal{D}_X : \ d_{\mathrm{TV}}(P, Q) < \epsilon\}. \tag{4.15}$$

对于任意分布 P和函数 φ： $X \to [-1, 1]$，我们记

$$P[\varphi] := \mathbb{E}_{x\sim P}[\varphi(x)] \tag{4.16}$$

为 φ 关于 P的期望。特别地，我们用 $\boldsymbol{D}_n$ 表示定义在 $\{0,1\}^n$上的分布类。

定义 11 （统计查询预言机）。 设 $P \in \boldsymbol{D}_X$且 $\tau > 0$。统计查询预言机 $\mathrm{Stat}_\tau(P)$ 是一个理想接口，对于任意查询函数 φ： $X \to [-1, 1]$，它会返回一个满足以下条件的实数 v

$$|v - P[\varphi]| \le \tau. \tag{4.17}$$

注 8 （容差参数的单调性与基于样本的含义）。 （*1*）如果 $0 < \zeta < \tau$，那么任意$\mathrm{Stat}_\zeta(P)$ 都会自动成为有效的 $\mathrm{Stat}_\tau(P)$，因为 $|v - P[\varphi]| \le \zeta < \tau$也满足定义 *11*中的条件。因此，对于较小容差 ζ 证明的下界会自动适用于任何较大容差 τ。
（*2*）当 τ 至少为逆多项式（例如 $\tau \ge 1/\mathrm{poly}(n)$）时，可以根据多项式数量的样本近似 $P[\varphi]$，从而实现 $\mathrm{Stat}_\tau(P)$。在此情形下，预言机的复杂度主要由计算查询函数 φ的代价决定。

定义 12 (分布的表示和 ϵ-表示**)**。 在统计查询框架中，必须固定一种分布表示。常见的表示类型有两种：

1. 生成器：一种随机化算法，给定随机比特后输出样本 $x \sim P$。

2. 求值器：当 $P \in \boldsymbol{D}_n$ 时，一个算法 $\mathrm{Eval}_P\colon \{0,1\}^n \to [0, 1]$ 满足 $\mathrm{Eval}_P(x) = P(x)$.

给定一个分布 P，如果与给定表示（生成器或求值器）相对应的分布 Q 满足 $d_{\mathrm{TV}}(P, Q) < \epsilon$，我们就称该表示为 P 的 ϵ-表示 （或 ϵ-近似表示）。在我们的复杂度下界中，对这些表示的计算效率不作任何假设：下界同样适用于计算效率可能低下的表示。

定义 13 (ϵ-统计查询框架中的学习问题)。 设 $\boldsymbol{D}$ 是一个分布类，且 $\epsilon, \tau \in (0,1)$。在固定分布表示方式的前提下，使用容差为 τ 的统计查询来对 $\boldsymbol{D}$ 进行 ϵ-学习的任务定义如下：对于任意未知分布 $P \in \boldsymbol{D}$，给定对预言机 $\mathrm{Stat}_\tau(P)$ 的访问权限，设计一个学习算法，输出 P 的 ϵ-表示（即某个 Q，使得 $d_{\mathrm{TV}}(P, Q) < \epsilon$）。

定义 14 （平均情形查询复杂度）。 设 $\boldsymbol{D}$ 为一个分布类， μ 为定义在 $\boldsymbol{D}$ 上的概率测度，且 $\alpha, \beta \in (0,1)$。

1. 确定性平均情形复杂度：对于给定的 (ϵ, τ)，若确定性 *SQ* 学习算法 A 能以平均不超过 q 次查询的代价ϵ-学习 P，则称其

$$\Pr_{P\sim\mu}\left[\mathcal{A}^{\mathrm{Stat}_\tau(P)} \ \epsilon\text{-}learns\ P\ within\ q\ queries\right] \ \ge \ \beta. \tag{4.18}$$

在所有满足上述条件的算法中，这样的最小值 q 称为问题 *13* 的确定性平均情形查询复杂度。

2. 随机化平均情形复杂度：若 A 是随机化算法，且 $\Pr_{\mathcal{A}}[\cdot]$ 表示对其内部随机性取概率，则我们要求

$$\Pr_{P\sim\mu}\left[\Pr_{\mathcal{A}}\left[\mathcal{A}^{\mathrm{Stat}_\tau(P)} \ \epsilon\text{-}learns\ P\ within\ q\ queries\right] \ \ge \ \alpha\right] \ \ge \ \beta. \tag{4.19}$$

满足该条件的最小 q 称为随机化平均情形查询复杂度。

备注9（确定性与随机化复杂度之间的关系）。 在统计查询框架中，确定性与随机化平均情形复杂度通过标准的极小极大原理相关联：对于给定的 (α, β)，确定性平均情形下界可以转换为随机化平均情形下界，代价是一个依赖于 α 的常数因子（例如，$2(\alpha - 1/2)$）。因此，本文正文主要关注确定性平均情形下界，而扩展到随机化设置则可通过附录中概述的标准论证得到。

这些预备知识使我们能够以统一的方式陈述统计查询下界结果：给定分布类 $\mathcal{D}$ 及其上的先验测度 μ，任何试图在平均情形意义下对 $\mathcal{D}$ 进行 ϵ-学习的统计查询算法（参数为 (α, β)）都必须至少使用 q 次统计查询，其中 q 可由某些信息论量（如统计查询维数或相关的平均情形困难度参数）给出下界。

D. 从学习到判定的归约与平均情形下界

本小节回顾 Feldman 提出的、用于建立统计查询下界的标准学习与判定框架 [Fel17]。不过，我们的记法大多遵循 Nietner [NIS+25]，并采用其工作中的一种便捷的平均情形表述。

定义15（判定问题：$\mathcal{D}$ 与 Q，参见 [NIS+25]）。 设 $\mathcal{D} \subseteq \mathcal{D}_X$ 为一个分布类，且 $Q \in \mathcal{D}_X$为一个固定的参考分布。判定问题 $\mathcal{D}$ 与 Q 定义如下：

给定对未知分布 $P \in \mathcal{D} \cup \{Q\}$ 的统计查询预言机访问，任务是在有限次查询内输出正确的判定：

$$\text{“}P = Q\text{” or “}P \in \mathcal{D}\text{”}.$$

我们继续 使用统计查询预言机 $\mathrm{Stat}_\tau(P)$，其容差为 τ，如定义 *1* 所述 *1*.

Lem题1（学习不比判定容易，参见 [NIS+25]）。设 $\mathcal{D} \subseteq \mathcal{D}_X$ 和 $Q \in \mathcal{D}_X$ 满足

$$d_{\mathrm{TV}}(P, Q) > \epsilon + \tau, \qquad \forall\, P \in \mathcal{D}, \tag{4.20}$$

其中 $0 < \tau \leq \epsilon \leq 1$。若存在确定性算法 $\mathcal{A}$，能够以 ϵ-学习 $\mathcal{D}$，且至多使用 q τ-准确的统计查询（见定义 *13*），则存在确定性算法 $\mathcal{B}$，能够解决判定问题 $\mathcal{D}$ 与 Q（定义 *15*），至多使用 $q+1$ τ-准确的统计查询，且始终正确。

引理2（判定问题的确定性下界，参见 [NIS+25]）。设 $\mathcal{D} \subseteq \mathcal{D}_X$，$Q \in \mathcal{D}_X$，并设 μ是定义在 $\mathcal{D}$上的概率测度。若存在确定性算法 $\mathcal{A}$，能够正确判定 $\mathcal{D}$ 与 Q，且至多使用 q τ-准确的统计查询，则必然有

$$q \;\geq\; \left(\max_{\phi : X \to [-1,1]} \Pr_{P \sim \mu} \big[\, |P[\phi] - Q[\phi]| > \tau \,\big] \right)^{-1}. \tag{4.21}$$

定理 *8*（确定性平均情形 *SQ* 查询复杂度下界，参见 [*NIS*+25]）。设 $D \subseteq D_X$，设 μ为 D 上的概率测度，且 $\epsilon, \tau \in (0, 1)$, $\beta \in (0, 1)$。假设存在一个确定性算法 A，使用至多 q τ-准确的统计查询，在子集 $D' \subseteq D$ 上以 ϵ-学习 P，且该子集的 μ-测度为 β（即 $Pr_{P\sim\mu}[A$ ϵ-学习 $P] \geq \beta$）。那么对于任意参考分布 $Q \in D_X$，有

$$q + 1 \;\geq\; \frac{\beta - \Pr_{P \sim \mu}\big[d_{\mathrm{TV}}(P, Q) \leq \epsilon + \tau\big]}{\max\limits_{\phi : X \to [-1,1]} \Pr\limits_{P \sim \mu} \big[\, |P[\phi] - Q[\phi]| > \tau \,\big]}. \tag{4.22}$$

E. 随机统计查询算法与确定性算法

在本小节中，我们将从统计查询学习框架下平均情形查询复杂度的角度，总结随机算法（包括经典随机算法和量子算法）与确定性算法之间的关系。本文的阐述主要改编自 [NIS+25]的附录 F。

回顾上一小节，我们已经在确定性设置下证明了查询复杂度的一个平均情形下界（对应于 [NIS+25]中的定理 30），其核心思路是将学习问题归约为判定问题，再对该判定问题的统计查询复杂度给出下界。随机化设置下的策略完全类似，只是我们还需要处理学习算法可能利用内部随机性猜对答案的情况。

定义 16 （随机平均情形统计查询复杂度）。 设 D 为一个分布类， μ 为 D 上的概率测度，并令 $\epsilon, \tau \in (0,1)$。给定统计查询预言机 $\mathrm{Stat}_\tau(P)$（如前文所定义），若随机化学习算法 A（可以是经典随机化算法或量子算法）满足以下条件，则称其在参数随机地 ϵ-学习 D，平均情形下的参数为 $(\alpha, \beta) \in (0,1)^2$：存在一个查询上界 q，使得

$$\Pr_{P\sim\mu}\Big[\Pr_{\mathcal{A}}\Big(\mathcal{A}^{\mathrm{Stat}_\tau(P)} \ \epsilon\text{-}learns\ P\ using\ at\ most\ q\ queries\Big) \ \geq\ \alpha\Big] \ \geq\ \beta,$$

其中，外层概率取自 $P \sim \mu$，内层概率取自 A 的内部随机性。这样的最小 q 称为 D 在 μ 和参数 (α, β) 下的随机平均情形统计查询复杂度。

引理 3 （学习至少与判定一样难（随机设置），参见 [NIS+25]）。 设 $\mathcal{D}$ 为一个分布类，且 Q 为一个参考分布，使得对所有 $P \in \mathcal{D}$，均有

$$d_{\mathrm{TV}}(P, Q) > \epsilon + \tau,$$

其中 $0 < \tau \leq \epsilon \leq 1$。如果存在一个随机化算法 A，其内部成功概率至少为 α，能够使用准确度为 τ 的统计查询来 ϵ-学习 D，那么就存在一个随机化算法，它以相同的成功概率 α，仅使用准确度为 τ 的统计查询，就能在“$P = Q$”和“$P \in D$”之间作出判别。

引理 4 (用于随机算法判别 $\mathcal{D}$ 与 Q 的统计查询下界，参见 [NIS+25])。 设 $\mathcal{A}$ 是一个随机化算法，使用至多 q 个 τ 精度的统计查询来判别 $\mathcal{D}$ 与 Q，且其内部成功概率至少为 $\alpha > 1/2$。那么，对于 μ 上的任意概率测度 $\mathcal{D}$，

$$q \ \geq\ \frac{2(\alpha - \frac{1}{2})}{\max\limits_{\phi: X\to[-1,1]} \Pr\limits_{P\sim\mu}\big[\big|P[\phi] - Q[\phi]\big| > \tau\big]}.$$

定理 9 (随机平均情形统计查询复杂度下界，参见 [NIS+25])。 设 $\mathcal{A}$ 是一个随机化学习算法，在测度 μ 和参数 (α, β) 下，解决 ϵ-学习问题，使用至多 q 个 τ 精度的统计查询（即，它在某个子集上的分布上成功，该子集的 μ-测度为 β，且其内部成功概率至少为 α）。那么，对于任意参考分布 Q，

$$q + 1 \ \geq\ 2 \cdot \frac{(\alpha - \frac{1}{2}) \cdot \Big(\beta - \Pr_{P\sim\mu}\big[d_{\mathrm{TV}}(P, Q) \leq \epsilon + \tau\big]\Big)}{\max\limits_{\phi: X\to[-1,1]} \Pr\limits_{P\sim\mu}\big[\big|P[\phi] - Q[\phi]\big| > \tau\big]}.$$

F. QPStat 模型与一般下界

在本小节中，我们回顾所需的 QPStat 模型和一般下界模板，主要遵循 [WD24]。

定义 17 （量子过程统计查询（QPStat）预言机）。 设 $E : B(H) \to B(H)$ 为一个完全正迹保持信道，并令 $\mathsf{S}(H)$ 表示状态空间。对于任意量子态 $\rho \in \mathsf{S}(H)$ 和算子 $O \in B(H)$，满足 $\|\rho\|_1 \leq 1$ 和 $\|O\|_\infty \leq 1$，以及任意容差参数 $\tau > 0$，*QPStat* 预言机定义为

$$QPStat_E : (\rho, O, \tau) \longmapsto \alpha \in \mathbb{R},$$

并且要求输出 α ，使其满足

$$\left|\alpha - \mathrm{Tr}\left[O\,E(\rho)\right]\right| \le \tau. \tag{4.23}$$

与未知信道 E 交互的 *QPStat* 学习算法最多可以自适应地查询该预言机 q次；我们称其使用了精度为 τ 的 q 次 *QPStat* 查询。

在本文中，我们关注平均情形 QPStat 学习复杂度：给定一个信道系综 $(\mathcal{E}\ \mu)$和误差参数 (ε,τ)，我们希望尽可能少地使用 QPStat 查询，使得对于信道的一个 μ-测度 β子集，算法输出的假设通道与真实信道之间的菱形距离至多为 ε，且内部成功概率至少为 α。取特殊情形 $\beta = 1$时，我们便回到最坏情况设置，此时学习器必须在 μ 支撑集中的所有信道上都成功；在这种情况下，引理 5 中的下界自然简化为 $q+1 \ge (2\alpha-1)/\Gamma$。

形式化地，对于一个 配备测度 μ 的 CPTP 信道族 $\mathcal{E}$，我们称学习算法 $\mathcal{A}$ 满足 es:

1. 其使用至多 q QPStat 查询，精度为 τ；

2. 存在常数 $\alpha > 1/2$ 和 $\beta > 0$，使得

$$\mu\Big(\Big\{E \in \mathcal{E} : \Pr_{\text{internal randomness}}\left[d_\diamond(\widehat{E}, E) \le \varepsilon\right] \ge \alpha\Big\}\Big) \ \ge\ \beta,$$

在这种情况下，我们称 $\mathcal{A}$ QPStat 学习具有参数 $(\varepsilon,\tau,\alpha,\beta)$ 的信道系综 $(\mathcal{E}\ \mu)$，且该学习是在平均情形意义下进行的。

引理 5 (QPStat 多对一型下界模板，参见 [WD24])。 设 $(\mathcal{E}\ \mu)$ 是 *CPTP* 信道的一个族¯，它们作用于固定的希尔伯特空间 $\mathcal{H}$，并配备一个概率测度 μ。设 E 是某个参考信道（在¯应用中，我们将取 $E = \mathbb{E}_{E\sim\mu}E$）。

考虑以下 *QPStat* 学习问题：一个（可能是随机化的）学习算法 *A* 接收对随机信道 $E \sim \mu$ 的 *QPStat* 访问，即接收对预言机 $QPStat_E$ 的访问，并且在输出一个假设通道 E 之前，至多使用 q *QPStat* 查询，精度为^ τ。

如果存在常数 $\alpha > 1/2$ 和 $\beta > 0$ 使得，对于

$$\mathcal{G} := \{E \in \mathcal{E} : \Pr_{internal\ randomness}\left[d_\diamond(\widehat{E}, E) \le \varepsilon\right] \ge \alpha\},$$

有 $\mu(G) \ge \beta$，那么必然

$$q+1 \ \ge\ \frac{(2\alpha-1)\,\beta}{\max\limits_{\rho,O}\ \Pr\limits_{E\sim\mu}\Big(\left|\mathrm{Tr}[OE(\rho)] - \mathrm{Tr}[O\bar{E}(\rho)]\right| > \tau\Big)}, \tag{4.24}$$

其中，最大值取遍所有满足 $\|\rho\|_1 \le 1$ 和 $\|O\|_\infty \le 1$的配对(ρ, O)。

备注1 (不失一般性，我们假设 $\tau \le \varepsilon$)。 在本文中，我们始终考虑以下情形$0 < \tau \le \varepsilon$。如果 $\tau > \varepsilon$，则可能存在这样的量子信道（或分布），其 $\varepsilon < d(\cdot,\ \cdot) < \tau$ 无法通过 τ精度的查询答案加以区分，因此在该参数范围内不存在 ε学习器。因此，对于我们的下界陈述 $[$，假设 $\tau \le \varepsilon$ *NIS+25*]成立不失一般性。

G. 弗雷歇导数与扰动公式

本文需要将生成元的微小变化与相应的半群变化联系起来 $e^{t\mathcal{L}}$。对此，自然的数学语言是巴拿赫空间上的弗雷歇导数及其相关的扰动型公式。

定义 18 （巴拿赫空间上的弗雷歇导数[Yos12]）。 设 （E，$\|\cdot\|_E$），（F，$\|\cdot\|_F$）是巴拿赫空间，且$U \subset E$ 是一个开集。映射 F： $U \to F$ 称为在点 $x \in U$ 处弗雷歇可微，如果存在一个

有界线性算子 $DF(x): E \to F$ 使得

$$\lim_{\|h\|_E \to 0} \frac{\|F(x+h) - F(x) - DF(x)[h]\|_F}{\|h\|_E} = 0. \tag{4.25}$$

在此情形下，$DF(x)$ 是唯一的，并称为 F 在 x处的弗雷歇导数。如果 F 在 U上处处弗雷歇可微，且映射 $x \mapsto DF(x)$ 连续，则称 $F \in C^1(U; F)$。

在有限维情形下（例如 $E = \mathbb{R}^n$, $F = \mathbb{R}^m$），弗雷歇导数退化为熟知的雅可比矩阵。在无限维情形下，它给出一阶线性近似的规范形式，$F(x+h) \approx F(x) + DF(x)[h]$，参见任意一本泛函分析教材，例如 [Yos12]。

本文所关注的主要巴拿赫空间是

$$E = \mathsf{B}(\mathcal{B}(\mathcal{H})),$$

所有有界超算子构成的空间 $\mathcal{L}: \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$，配备诱导的 $1 \to 1$ 范数 $\|\mathcal{L}\|_{1\to 1} := \sup_{X \neq 0} \frac{\|\mathcal{L}(X)\|_1}{\|X\|_1}$（参见定义 4）。在此空间上，我们考虑指数映射

$$\mathrm{Exp}_t: \mathcal{L} \mapsto e^{t\mathcal{L}} := \sum_{n=0}^{\infty} \frac{t^n}{n!} \mathcal{L}^n, \qquad t \geq 0,$$

其取值仍为有界超算子 $e^{t\mathcal{L}}: \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$。

命题 2（算子指数的弗雷歇可微性）。设 E 是任意巴拿赫空间，$\mathsf{B}(E)$ 是其有界线性算子空间。对于任意固定的 $t \geq 0$，映射

$$\mathrm{Exp}_t : \mathsf{B}(E) \to \mathsf{B}(E), \qquad A \mapsto e^{tA}$$

是巴拿赫空间 $\mathsf{B}(E)$上的一个 C^∞（事实上是解析）映射。它在 $A \in \mathsf{B}(E)$ 处的弗雷歇导数，$D\mathrm{Exp}_t(A): \mathsf{B}(E) \to \mathsf{B}(E)$，作用于任意扰动 $\Delta A \in \mathsf{B}(E)$ 时为

$$D\mathrm{Exp}_t(A)[\Delta A] = \int_0^t e^{(t-s)A}\, \Delta A\, e^{sA}\, \mathrm{d}s. \tag{4.26}$$

证明概要。首先，利用幂级数 $e^{tA} = \sum_{n \geq 0} t^n A^n / n!$，它在算子范数下是一致收敛的，可以看出 Exp_t 在 $\mathsf{B}(E)$ 上是解析的。设 $A(\alpha) = A + \alpha \Delta A$。将扰动公式应用于$e^{tA(\alpha)}$（见引理6），并考察

$$e^{t(A+\delta\Delta A)} - e^{tA} = \int_0^t e^{(t-s)(A+\delta\Delta A)}\, \delta\Delta A\, e^{sA}\, \mathrm{d}s,$$

将两边除以 δ 并令 $\delta \to 0$，利用 $e^{(t-s)(A+\delta\Delta A)} \to e^{(t-s)A}$ 在算子范数下的连续性，可得极限形式（4.26）。完整严谨的巴拿赫空间证明见 [EN00]。 ∎

我们将使用正文中由扰动公式给出的上述指数映射的弗雷歇导数，即对于每个参数方向 ΔA，导数 $D\mathrm{Exp}_t(A)[\Delta A]$ 由一个算子值积分给出。

引理 6（扰动公式）。设 A, $B \in \mathsf{B}(E)$ 且 $t \geq 0$。则

$$e^{t(A+B)} - e^{tA} = \int_0^t e^{(t-s)(A+B)}\, B\, e^{sA}\, \mathrm{d}s. \tag{4.27}$$

更一般地，如果 $A(\alpha)$ 是一族弗雷歇可微的有界算子，其导数为 $A'(\alpha)$，那么

$$\frac{\mathrm{d}}{\mathrm{d}\alpha} e^{tA(\alpha)} = \int_0^t e^{(t-s)A(\alpha)}\, A'(\alpha)\, e^{sA(\alpha)}\, \mathrm{d}s. \tag{4.28}$$

证明思路。 基本形式（4.27）可通过考察 $U(s) := e^{(t-s)(A+B)}e^{sA}$. 对其关于 s 求导可得

$$\frac{\mathrm{d}}{\mathrm{d}s}U(s) = -e^{(t-s)(A+B)}(A+B)e^{sA} + e^{(t-s)(A+B)}Ae^{sA} = -e^{(t-s)(A+B)}Be^{sA}.$$

对 $s \in [0,t]$ 积分得到 $U(t) - U(0) = -\int_0^t e^{(t-s)(A+B)}Be^{sA}\,\mathrm{d}s$, 即 $e^{tA} - e^{t(A+B)} = -\int_0^t \cdots$, 重新整理后得到式（4.27）。

对于式（4.28），将 B 替换为一个小扰动 $\delta A'(\alpha)$，应用式（4.27），除以 δ，然后令 $\delta \to 0$。详情见 [NH95]；巴拿赫空间中由算子生成的半群的扰动见 [Kat。■

备注 *11*（本文中使用的专门形式）。本文取 $E = B(H)$，并令 $A(\alpha) = L_\alpha$ 为连接两点 L、L' 的直线同伦：$L_\alpha = L + \alpha(L' - L)$，从而 $A'(\alpha) = L' - L$。代入式（*4.28*）恰好得到

$$\frac{\mathrm{d}}{\mathrm{d}\alpha}e^{t\mathcal{L}_\alpha} = \int_0^t e^{(t-s)\mathcal{L}_\alpha}\,(\mathcal{L}' - \mathcal{L})\,e^{s\mathcal{L}_\alpha}\,\mathrm{d}s, \tag{4.29}$$

这正是引理 *11* 中使用的弗雷歇导数表示。估计诱导$1 \to 1$ 范数下的这个积分，即可得到如下形式的利普希茨界：$\|\Lambda^{(\mathcal{L}')}{}_t - \Lambda_t^{(\mathcal{L})}\|_{1\to1} \le t\|L' - L\|_{1\to1}$.

H. Haar 测度、集中性与2范数利普希茨常数

本小节承接 [Led01]，回顾紧群上的 Haar 测度，阐释参数球面上的列维集中性，并给出我们后续所需的2范数利普希茨常数估计。

定义 19 (紧群上的 Haar 测度**)**。 设 G 是第二可数紧拓扑群，$\mathcal{B}(G)$ 是其博雷尔 σ代数。概率测度 μ_{Haar} 称为 G 上的（归一化）*Haar* 测度，当且仅当

$$\mu_{\mathrm{Haar}}(gA) = \mu_{\mathrm{Haar}}(Ag) = \mu_{\mathrm{Haar}}(A), \quad \forall\, g \in G,\ A \in \mathcal{B}(G).$$

Haar 测度存在且唯一。本文最重要的例子是酉群 $G = \mathrm{U}(d)$和 $\mathrm{SU}(d)$；在这些情形下，我们用 μ_{Haar} 表示归一化的 *Haar* 概率测度。

在矩阵群 $\mathrm{U}(d)$ 上，我们选择由希尔伯特–施密特范数诱导的度量作为几何背景。关于量子情形的讨论可见 [BCHJ+21]。

定义 20 （希尔伯特–施密特范数与 2-范数度量）。 对于任意矩阵 $A \in \mathbb{C}^{d\times d}$，希尔伯特–施密特范数定义为

$$\|A\|_2 := \big(\mathrm{Tr}(A^\dagger A)\big)^{1/2}.$$

在酉群 $G = \mathrm{U}(d)$上，我们使用

$$d_2(U,V) := \|U - V\|_2, \qquad U, V \in \mathrm{U}(d)$$

作为度量，并称其为2-范数度量。对于实值函数 $F:\ G \to \mathbb{R}$，我们将其相对于 d_2 的利普希茨常数记为

$$\mathrm{Lip}_2(F) := \sup_{U\neq V} \frac{|F(U) - F(V)|}{d_2(U,V)}.$$

当$\mathrm{Lip}_2(F) \le 1$ 时，我们称 F 关于2-范数是1-*Lipschitz* 的。

在高维中，$(G,\ d_2,\ \mu_{\mathrm{Haar}})$ 构成典型的列维族，这意味着任意 1-Lipschitz 函数在哈尔测度下都具有很强的集中性。关于此主题的系统论述可见 Ledoux 关于集中不等式的专著 [Led01]。

定义 21 (哈尔测度下的列维集中)。 设$(G, d_2, \mu_{\mathrm{Haar}})$为上述度量概率空间。对于任意博雷尔可测函数 $F: G \to \mathbb{R}$，若数值 $m_F \in \mathbb{R}$ 是函数 F 相对于哈尔测度的中位数，则

$$\mu_{\mathrm{Haar}}\big(\{F \le m_F\}\big) \ge \frac{1}{2}, \qquad \mu_{\mathrm{Haar}}\big(\{F \ge m_F\}\big) \ge \frac{1}{2}.$$

我们称 $(G、\ d_2、\ \mu_{\mathrm{Haar}})$ 具有次高斯集中性，如果存在常数 c_G、$C_G > 0$，使得对于任意相对于 2-范数而言为 *L-Lipschitz* 的函数 F，以及任意 $r > 0$，都有

$$\mu_{\mathrm{Haar}}\big(\{|F - m_F| \ge r\}\big) \ \le\ 2\exp\Big(-c_G \frac{r^2}{L^2}\Big). \tag{4.30}$$

特别地，当 $G = \mathrm{U}(d)$ 或 $\mathrm{SU}(d)$ 时，可以取 $c_G = \Theta(d^2)$，这体现了流形维数 $\dim G = \Theta(d^2)$ 所带来的高维效应。

备注12 (从球面到酉群)。 一种标准的证明策略是将 $G = \mathrm{U}(d)$ 视为嵌入 $\mathbb{C}^{d\times d} \cong \mathbb{R}^{2d^2}$ 中的光滑子流形，其黎曼度量等价于希尔伯特–施密特范数。考虑一个包含 G 的大球面 $S^{N-1} \subset \mathbb{R}^N$ （其中 $N \sim 2d^2$），并在其上赋予均匀测度。利用球面列维引理：对于任意 1-*Lipschitz* 函数 $f:\ S^{N-1} \to \mathbb{R}$，

$$\Pr\big(|f - m_f| \ge r\big) \ \le\ 2\exp\big(-cNr^2\big),$$

并将其与 G 上的 *Haar* 测度到球面测度之间的等变嵌入及相应的 *Lipschitz* 收缩结合起来，可得到如下形式的集中界 (4.30) （常数仅有数值上的变化）。

本文分析参数球面时，主要使用以下引理。

引理 7 （参数球面上的列维集中，参见 [Led01]）。 设 S^{M-1} 为实球面，且 μ_S 为标准均匀测度。对于任意 *L-Lipschitz* 函数 $f:\ S^{M-1} \to \mathbb{R}$ 以及任意 $\tau > 0$，存在常数$c_{\mathrm{par}} > 0$（与 M、 f和 τ无关），使得

$$\Pr_{\theta\sim\mu_S}\Big(|f(\theta) - \mathbb{E}_{\mu_S} f| \ge \tau\Big) \le 2\exp\Big(-c_{\mathrm{par}} \frac{M\,\tau^2}{L^2}\Big).$$

V. 随机林德布拉德系综

A. 随机林德布拉德算子系综的线性参数化与集中性

本小节将形式化阐述几点内容。首先，对于任意固定的局部维数，林德布拉德算子族都可以嵌入一个有限维实向量空间；此外，通过在该向量空间上选取一个有界基 $\{G_j\}$，可以对林德布拉德算子进行线性参数化；进而，在参数空间上赋予一种自然的随机系综后，我们便能得到 SQ 测试函数 $F_\varphi(\mathcal{L}) := P_{\mathcal{L}}[\varphi]$ 的集中性，从而在开放系统 SQ 框架下得到 frac($\mu_{\mathcal{L}}$， Q， τ) 的上界；最后，我们将讨论如何从“是否涵盖所有林德布拉德算子”以及学习普适性的角度来理解这种参数化。

这里我们假设底层希尔伯特空间是有限维的，$\mathcal{H} \simeq \mathbb{C}^d$。用$\mathcal{B}(\mathcal{H})$表示有界算子空间，用 End($\mathcal{B}(\mathcal{H})$)表示超算子空间。

定义 22 （GKSL 锥与仿射包）。 令

$$\mathsf{GKSL} \subset \mathrm{End}(\mathcal{B}(\mathcal{H}))$$

表示满足 *Gorini-Kossakowski-Sudarshan-Lindblad (GKSL)* 条件的所有 *Lindblad* 生成元的集合，即，

i. L 是厄米保持且保迹的；

ii. $e^{t\mathcal{L}}$ 对所有 $t \geq 0$ 生成一族 *CPTP*映射（量子马尔可夫半群）。

令 $\mathrm{Aff}(\mathsf{GKSL})$ 为其仿射包（包含 GKSL 的最小仿射子空间），并定义

$$\mathsf{V} := \mathrm{Aff}(\mathsf{GKSL}) - \mathcal{L}_{\mathrm{ref}}$$

为通过平移某个参考 *Lindblad* 算子 $L_{\mathrm{ref}} \in$GKSL 并将其作为原点而得到的线性空间。

在有限维情形下，$\mathrm{End}(\mathcal{B}(\mathcal{H}))$ 是有限维实向量空间（维数为 $\mathcal{O}(d^4)$），因此有：

引理8 (线性参数化的完备性**).** 对于固定的局部维数 d，存在有限多个超算子 $G_1, \ldots, G_M \in \mathrm{End}(B(H))$，构成 V 的线性基，使得：

1. 对任意 $L \in$ GKSL，存在唯一的系数向量 $\theta(L) = (\theta_1, \ldots, \theta_M) \in \mathbb{R}^M$，满足

$$\mathcal{L} = \mathcal{L}_{\mathrm{ref}} + \sum_{j=1}^{M} \theta_j(\mathcal{L})\, G_j.$$

2. 存在一个凸锥 $C_{\mathrm{GKSL}} \subset \mathbb{R}^M$，使得 $L \in$ GKSL 当且仅当 $\theta(L) \in C_{\mathrm{GKS}}$ L.

证明。$\mathrm{End}(\mathcal{B}(\mathcal{H}))$ 是一个有限维实向量空间，而 Aff(GKSL) 是一个仿射子空间。固定一个参考点 $\mathcal{L}_{\mathrm{ref}} \in$ GKSL 并进行平移，可得线性子空间 V $=$ Aff(GKSL) $- \mathcal{L}_{\mathrm{ref}}$. 由于 V 是有限维的，因此存在一个有限基 $\{G_j\}_{j=1}^{M}$。对于任意 $\mathcal{L} \in$ GKSL，都有 $\mathcal{L} - \mathcal{L}_{\mathrm{ref}} \in$ V，因此存在唯一的系数向量 $\theta(\mathcal{L})$，使得

$$\mathcal{L} - \mathcal{L}_{\mathrm{ref}} = \sum_{j} \theta_j(\mathcal{L}) G_j.$$

将线性坐标映射 $\mathcal{L} \mapsto \theta(\mathcal{L})$ 的像记为 $\mathcal{C}_{\mathrm{GKSL}}$。根据 GKSL 条件的凸性，该像是一个凸锥。■

备注 13 (关于覆盖所有林德布拉德算子**).** 上面的引理表明，对于固定的 d，在适当的线性坐标系中，每个 *Lindblad* 算子都可以写成

$$\mathcal{L} = \mathcal{L}_{\mathrm{ref}} + \sum_{j=1}^{M} \theta_j G_j,$$

但需注意，可行参数 θ 必须位于凸锥 C_{GKSL}中。换言之，从纯粹的线性代数角度看，线性参数化在仿射包上是完备的；但一旦考虑完全正迹保持约束，只有锥内的系数才对应真正的 *Lindblad* 算子。

接下来，为了在高维参数球面上应用列维集中性（引理7），我们从$\mathcal{C}_{\mathrm{GKSL}}$ 中选取一个几何上“圆”的高维子集。

定义 23 （参数球面系综）。设

$$S^{M-1} := \{\theta \in \mathbb{R}^M : \ \|\theta\|_2 = 1\}$$

为单位球面。给定一个较小的参数 $\delta > 0$，定义

$$\mathcal{L}(\theta) := \mathcal{L}_{\mathrm{ref}} + \frac{\delta}{\sqrt{M}} \sum_{j=1}^{M} \theta_j G_j.$$

假设存在一个非空子集 $\Theta \subseteq S^{M-1}$，使得对于所有 $\theta \in \Theta$，L（θ） $\in$ GKSL （例如，当 δ 足够小时，L（θ）始终处于 L_{ref} 的一个小 *GKSL* 邻域内）。定义参数测度 μ_Θ 为

球面测度在 Θ 上的归一化限制。于是，随机 *Lindblad* 算子系综定义为推前测度

$$\mu_{\mathcal{L}} := \mathcal{L}_{\#}(\mu_{\Theta}),$$

也就是说，抽取 $L \sim \mu_{\mathcal{L}}$ 等同于对 $\theta \sim \mu_{\Theta}$ 进行采样，并令 $L = L(\theta)$。

注释 14（局部切片与高维邻域）。上述构造仅选取了 *GKSL* 锥内 L_{ref} 附近的一个高维邻域，而非整个 GKSL 集合。因此，随机系综 $\mu_{\mathcal{L}}$ 具有分布特定性，它描述的是围绕物理上自然的林德布拉德模型族的高维随机扰动，而不是所有林德布拉德算子。

注15（球面随机扰动 Lindblad 生成元系综）。在后续关于随机林德布拉德算子系综的讨论中，我们将频繁使用以下参数化

$$\mathcal{L}(\theta) := \mathcal{L}_{\mathrm{ref}} + \frac{\delta}{\sqrt{M}} \sum_{j=1}^{M} \theta_j G_j, \qquad \theta \in S^{M-1} \subset \mathbb{R}^M, \tag{5.1}$$

其中$\mathcal{L}_{\mathrm{ref}}$ 是一个固定的 *GKSL* 生成元（参考 *Lindblad* 生成元），$\{G_j\}_{j=1}^{M}$ 是有界超算子方向（例如由局部跳跃算符、局部噪声通道或 *Kossakowski* 矩阵的基诱导的方向；具体示例将在第 六节给出），θ 在单位球面 S^{M-1}上服从一致分布，且 $\delta > 0$控制扰动强度（关于如何使线段保持在 *GKSL* 锥内，证明见引理 *9*）。我们将由（5.1）定义的随机林德布拉德算子族称为球面随机扰动 *Lindblad* 生成元系综。

从物理角度看，这种参数化可以理解如下：在高维参数空间中，我们围绕某个“平均动力学”添加各向同性的小扰动 $\mathcal{L}_{\mathrm{ref}}$，其中 θ_j 表示沿不同噪声／无序方向的随机幅度，而 $1/\sqrt{M}$ 重新缩放确保扰动的总平方幅度保持在 $O(\delta^2)$ 的量级，$M \to \infty$类似于 $1/\sqrt{N}$ *Wigner* 随机矩阵模型中的归一化。此选择也与 *Denisov* 的工作 *[DLT+ 19]*中的谱重新缩放相一致；不过在这里，我们的动机是确保下文推导的概率界表现出有效集中。

这类系综自然出现在以下物理模型中：

1. 随机自旋链中的开放系统动力学：例如，在具有随机局域场和退相干的 *XXZ／XYZ* 链模型中，随机场强度 h_i、耦合 J_i以及 *Lindblad* 跳跃率在不同样本之间的变化，都可以视为参数向量 θ的不同分量，对应于一组局部超算子方向 $\{G_j\}$，从而围绕某个平均 *Lindblad* 算子 *[Mon17b]*形成多参数静态无序系综。

2. 随机 *Kossakowski* 矩阵的结构化扰动：在 *GKSL* 形式中，噪声部分由一个 *Kossakowski* 矩阵决定 K。将 K 在厄米基 $\{E_j\}$上展开，$K(\theta) = K_{\mathrm{ref}} + \frac{\delta}{\sqrt{M}} \sum_j \theta_j E_j$，并通过 *Lindblad* 公式将基 $\{E_j\}$ 映射为超算子 $\{G_j\}$，即可得到一个围绕参考矩阵 K_{ref}的各向同性随机扰动系综。这可以看作是随机 *Lindblad* 算符文献 *[DLT+ 19]*中所研究的完全随机 *Kossakowski* 系综的一种结构化版本。

3. 大规模量子处理器中的多通道噪声无序：在超导量子比特或囚禁离子等平台上，不同物理量子比特和耦合通道（例如，T_1/T_2时间 *[AAB+ 19、CRJ+ 22]*、退相干率 *[BCMS19]*, 泄漏率 *[WKPT22]*）的噪声强度通常会在不同样本之间以及单个芯片内部呈现静态无序。将平均噪声模型纳入$\mathcal{L}_{\mathrm{ref}}$，并将每个量子比特/信道相对于平均值的偏差归入方向 $\{G_j\}$，即可得到形式为 (5.1)的高维随机 *Lindblad* 算子系综，它刻画了器件级多参数噪声失配。

因此 (5.1) 并非只是一个玩具模型，而是对一大类多参数静态无序 *Lindblad* 生成元系综的抽象描述；这类系综广泛存在于开放量子多体系统和量子信息硬件中。在我们之后对 $\mathcal{L}$ 上的利普希茨性质及高维集中性的分析中，该系综将作为我们的典型示例。

引理 9 (凸 GKSL 切片及保持在 GKSL 内部的线段)。 在上述构造中，存在$\delta_0 > 0$，使得对于任意 $0 < \delta \le \delta_0$:

1. 对于所有 $\theta \in S^{M-1}$，L（θ）都是 *GKSL* 生成元。

2. 令 F: $= \{L$（θ）： $\theta \in S^{M-1}\}$。那么对于任意 θ、$\theta' \in S^{M-1}$ 和任意 $\alpha \in [0,1]$，凸组合

$$\mathcal{L}_\alpha := (1-\alpha)\,\mathcal{L}(\theta) + \alpha\,\mathcal{L}(\theta')$$

仍然是 *GKSL* 生成元。

证明。 (1) GKSL生成元构成一个凸锥，而$\mathcal{L}_{\mathrm{ref}}$ 是该凸锥的内点。因此存在$r > 0$，使得只要 $\|\mathcal{L} - \mathcal{L}_{\mathrm{ref}}\|_{1\to 1} \le r$，算子$\mathcal{L}$ 仍然是 GKSL 生成元。对于$\mathcal{L}$（θ），我们估计

$$\begin{aligned}\|\mathcal{L}(\theta) - \mathcal{L}_{\mathrm{ref}}\|_{1\to 1} &\le \frac{\delta}{\sqrt{M}} \sum_{j=1}^{M} |\theta_j|\,\|G_j\|_{1\to 1} \\ &\le \frac{\delta C_G}{\sqrt{M}} \|\theta\|_1 \\ &\le \delta C_G,\end{aligned}$$

其中最后一步使用了对于 $\theta \in S^{M-1}$ 的 $\|\theta\|_1 \le \sqrt{M}\|\theta\|_2 = \sqrt{M}$。因此，只要 $\delta C_G \le r$ （例如，取 δ_0 : $= r/C_G$ 并要求 $0 < \delta \le \delta_0$），该界就保证$\mathcal{L}$（θ）对于所有 $\theta \in S^{M-1}$都是 GKSL。
(2) 对于 θ, $\theta' \in S^{M-1}$和 $\alpha \in [0,1]$, 定义

$$\mathcal{L}_\alpha := (1-\alpha)\,\mathcal{L}(\theta) + \alpha\,\mathcal{L}(\theta').$$

Then

$$\mathcal{L}_\alpha - \mathcal{L}_{\mathrm{ref}} = \frac{\delta}{\sqrt{M}} \sum_{j=1}^{M} \big[(1-\alpha)\theta_j + \alpha\theta'_j\big] G_j,$$

从而

$$\begin{aligned}\|\mathcal{L}_\alpha - \mathcal{L}_{\mathrm{ref}}\|_{1\to 1} &\le \frac{\delta C_G}{\sqrt{M}} \sum_{j=1}^{M} \big|(1-\alpha)\theta_j + \alpha\theta'_j\big| \\ &\le \frac{\delta C_G}{\sqrt{M}} \big((1-\alpha)\|\theta\|_1 + \alpha\|\theta'\|_1\big) \\ &\le \frac{\delta C_G}{\sqrt{M}} \big((1-\alpha)\sqrt{M} + \alpha\sqrt{M}\big) \\ &= \delta C_G \le r.\end{aligned}$$

因此，对于所有 $\alpha \in [0,1]$ 和所有 $0 < \delta \le \delta_0$，$\mathcal{L}_\alpha$ 仍处于$\mathcal{L}_{\mathrm{ref}}$ 的 GKSL 邻域内，因而是一个 GKSL 生成元。■

B. $P_{\mathcal{L}}[\varphi]$的接口和 Lipschitz 连续性

现在固定开放系统统计查询接口：对于固定的时间 $t > 0$、固定的输入态 ρ_{in} 和 POVM $\{M_x\}_{x\in X}$，我们为每个 Lindblad 算子$\mathcal{L}$ 定义量子马尔可夫半群元素 $\Lambda_t^{(\mathcal{L})} := e^{t\mathcal{L}}$ 及其对应的经典输出分布

$$P_{\mathcal{L}}(x) := \mathrm{Tr}\big(M_x \Lambda_t^{(\mathcal{L})}(\rho_{\mathrm{in}})\big), \qquad x \in X.$$

对于任意测试函数 φ： $X \to [-1,1]$，我们定义相应的统计查询期望

$$P_{\mathcal{L}}[\varphi] := \sum_{x\in X} \varphi(x) P_{\mathcal{L}}(x) = \mathrm{Tr}\Big(O_\varphi\, \Lambda_t^{(\mathcal{L})}(\rho_{\mathrm{in}})\Big),$$

其中 $O_\varphi := \sum_{x\in X} \varphi(x) M_x$.

引理10（可观测量 O_φ的范数界）。 对于任意 $\varphi: X \to [-1,1]$，有 $\|O_\varphi\|_\infty \le 1$.

证明。 对于任意满足 $\mathrm{Tr}\,\rho = 1$ 的量子态 $\rho \ge 0$，

$$\mathrm{Tr}(O_\varphi \rho) = \sum_x \varphi(x)\,\mathrm{Tr}(M_x \rho),$$

其中 $\mathrm{Tr}(M_x\rho) \ge 0$ 且 $\sum_x \mathrm{Tr}(M_x\rho) = 1$。因此，$\mathrm{Tr}(O_\varphi\rho)$ 是取值 $\varphi(x) \in [-1,1]$的凸组合，故对所有 ρ，$|\mathrm{Tr}(O_\varphi\rho)| \le 1$。由于 $\|O_\varphi\|_\infty = \sup_{|\psi\rangle} \left|\langle\psi|O_\varphi|\psi\rangle\right|$，且任意纯态下的期望值都可以通过密度矩阵期望来表示，因此可得 $\|O_\varphi\|_\infty \le 1$. ■

引理11（关于生成元的 Lipschitz 连续性）。 设 L、$L' \in \mathrm{GKSL}$，并假设对于所有$\alpha \in [0,1]$，直线同伦 $L_\alpha := L + \alpha(L' - L)$ 始终处于 GKSL 中。那么对于任意 $t \ge 0$，有

$$\left\|\Lambda_t^{(\mathcal{L}')} - \Lambda_t^{(\mathcal{L})}\right\|_{1\to 1} \le t\,\|\mathcal{L}' - \mathcal{L}\|_{1\to 1},$$

其中 $\|\cdot\|_{1\to 1}$ 是诱导的 $1\to 1$ 超算子范数。

证明。 考虑映射 $\alpha \mapsto e^{t\mathcal{L}_\alpha}$。在有限维情形下，指数映射在算子范数拓扑中可微，其弗雷歇导数由扰动公式（定义 18）给出：

$$\frac{\mathrm{d}}{\mathrm{d}\alpha} e^{t\mathcal{L}_\alpha} = \int_0^t e^{(t-s)\mathcal{L}_\alpha}\,(\mathcal{L}' - \mathcal{L})\,e^{s\mathcal{L}_\alpha}\,\mathrm{d}s.$$

取诱导的 $1\to 1$ 范数，并利用次乘性以及由每个$\mathcal{L}_\alpha$ 生成的量子马尔可夫半群都是完全正迹保持的这一事实（因此，对所有 $r \ge 0$均有 $\|e^{r\mathcal{L}_\alpha}\|_{1\to 1} \le 1$），我们得到

$$\begin{aligned}
\left\|\frac{\mathrm{d}}{\mathrm{d}\alpha} e^{t\mathcal{L}_\alpha}\right\|_{1\to 1} &\le \int_0^t \left\|e^{(t-s)\mathcal{L}_\alpha}\,(\mathcal{L}' - \mathcal{L})\,e^{s\mathcal{L}_\alpha}\right\|_{1\to 1} \mathrm{d}s \\
&\le \int_0^t \|e^{(t-s)\mathcal{L}_\alpha}\|_{1\to 1}\,\|\mathcal{L}' - \mathcal{L}\|_{1\to 1}\,\|e^{s\mathcal{L}_\alpha}\|_{1\to 1}\,\mathrm{d}s \\
&\le \int_0^t \|\mathcal{L}' - \mathcal{L}\|_{1\to 1}\,\mathrm{d}s \\
&= t\,\|\mathcal{L}' - \mathcal{L}\|_{1\to 1}.
\end{aligned}$$

对 $\alpha \in [0,1]$ 上的这一界积分可得

$$\begin{aligned}
\left\|e^{t\mathcal{L}'} - e^{t\mathcal{L}}\right\|_{1\to 1} &= \left\|\int_0^1 \frac{\mathrm{d}}{\mathrm{d}\alpha} e^{t\mathcal{L}_\alpha}\,\mathrm{d}\alpha\right\|_{1\to 1} \\
&\le \int_0^1 \left\|\frac{\mathrm{d}}{\mathrm{d}\alpha} e^{t\mathcal{L}_\alpha}\right\|_{1\to 1} \mathrm{d}\alpha \\
&\le \int_0^1 t\,\|\mathcal{L}' - \mathcal{L}\|_{1\to 1}\,\mathrm{d}\alpha \\
&= t\,\|\mathcal{L}' - \mathcal{L}\|_{1\to 1}.
\end{aligned}$$

这正是关于生成元所声称的 Lipschitz 界。 ■

推论1（关于生成元的 SQ 期望值的 Lipschitz 连续性）。 在引理 *11*的假设下，对于任意测试函数 $\varphi: X \to [-1,1]$ 有

$$\left|P_{\mathcal{L}}[\varphi] - P_{\mathcal{L}'}[\varphi]\right| \le t\,\|\mathcal{L}' - \mathcal{L}\|_{1\to 1}.$$

证明。 根据定义，

$$P_{\mathcal{L}}[\varphi] - P_{\mathcal{L}'}[\varphi] = \mathrm{Tr}\Big(O_\varphi\big(\Lambda_t^{(\mathcal{L})} - \Lambda_t^{(\mathcal{L}')}\big)(\rho_{\mathrm{in}})\Big).$$

利用矩阵霍尔德不等式（参见注 1），结合引理 10 以及诱导范数的定义（定义4），我们得到

$$\begin{aligned}\left|P_{\mathcal{L}}[\varphi]-P_{\mathcal{L}'}[\varphi]\right| &= \left|\mathrm{Tr}\Big(O_\varphi\big(\Lambda_t^{(\mathcal{L})}-\Lambda_t^{(\mathcal{L}')}\big)(\rho_{\mathrm{in}})\Big)\right| \\ &\le \|O_\varphi\|_\infty \left\|\big(\Lambda_t^{(\mathcal{L})}-\Lambda_t^{(\mathcal{L}')}\big)(\rho_{\mathrm{in}})\right\|_1 \\ &\le \|O_\varphi\|_\infty \left\|\Lambda_t^{(\mathcal{L})}-\Lambda_t^{(\mathcal{L}')}\right\|_{1\to1} \|\rho_{\mathrm{in}}\|_1 \\ &\le \left\|\Lambda_t^{(\mathcal{L})}-\Lambda_t^{(\mathcal{L}')}\right\|_{1\to1},\end{aligned}$$

其中我们使用了 $\|O_\varphi\|_\infty \le 1$ （引理 10）以及 $\|\rho_{\mathrm{in}}\|_1 = 1$ 对于一个密度算子。应用引理 11 即可得到所需的界

$$\left|P_{\mathcal{L}}[\varphi]-P_{\mathcal{L}'}[\varphi]\right| \le t\,\|\mathcal{L}'-\mathcal{L}\|_{1\to1}.$$

■

C. 参数球面上的Lipschitz常数与Lévy集中

现在我们使用定义 $\mathcal{L}$（θ）中 引入的参数化，该定义为 23。

引理 12 （参数球面上的Lipschitz常数）。 假设存在常数 $C_G > 0$ 使得$\|G_j\|_{1\to1} \le C_G$ 对所有 $1 \le j \le M$均成立。定义 F_φ（θ）：$= P_{\mathcal{L}(\theta)}[\varphi]$ 对于 $\theta \in \Theta$。那么对于任意 θ、$\theta' \in \Theta$,

$$|F_\varphi(\theta)-F_\varphi(\theta')| \le L_0\,\|\theta-\theta'\|_2, \qquad L_0 := t\,\delta\,C_G,$$

且 L_0 与测试函数 φ 和维数 M无关。

证明。 根据参数化的定义,

$$\mathcal{L}(\theta')-\mathcal{L}(\theta) = \frac{\delta}{\sqrt{M}}\sum_{j=1}^{M}(\theta'_j-\theta_j)\,G_j.$$

取 $1\to1$ 范数得

$$\begin{aligned}\left\|\mathcal{L}(\theta')-\mathcal{L}(\theta)\right\|_{1\to1} &\le \frac{\delta}{\sqrt{M}}\sum_{j=1}^{M}|\theta'_j-\theta_j|\,\|G_j\|_{1\to1} \\ &\le \frac{\delta C_G}{\sqrt{M}}\sum_{j=1}^{M}|\theta'_j-\theta_j| \\ &\le \frac{\delta C_G}{\sqrt{M}}\sqrt{M}\,\|\theta'-\theta\|_2 \\ &= \delta C_G\,\|\theta'-\theta\|_2,\end{aligned}$$

其中在最　　后一步我们使用了柯西-施瓦茨不等式。 $\sum_{j=1}^{M}|a_j| \le \sqrt{M}\,\|a\|_2$。 然后根据推论　　1,

$$\begin{aligned}|F_\varphi(\theta)-F_\varphi(\theta')| &= \left|P_{\mathcal{L}(\theta)}[\varphi]-P_{\mathcal{L}(\theta')}[\varphi]\right| \\ &\le t\left\|\mathcal{L}(\theta')-\mathcal{L}(\theta)\right\|_{1\to1} \\ &\le t\,\delta C_G\,\|\theta'-\theta\|_2.\end{aligned}$$

因此 $L_0 = t\delta C_G$ 是一致 Lipschitz 常数，与 φ 和参数维数 M 无关　　. ■

定理 10 （开放系统 SQ 框架中最大可区分比例的上界）。 设参数系综 $(\Theta, \mu_\Theta, \mathcal{L}(\theta))$ 如定义 *23*所述，且利普希茨常数 L_0 如引理 *12*所述。

在统计查询接口中，对每个测试函数 $\varphi:\ X \to [-1,1]$ 定义

$$F_\varphi(\theta) := P_{\mathcal{L}(\theta)}[\varphi], \qquad Q[\varphi] := \mathbb{E}_{\mathcal{L}\sim\mu_{\mathcal{L}}} P_{\mathcal{L}}[\varphi] = \mathbb{E}_{\theta\sim\mu_\Theta} F_\varphi(\theta).$$

定义

$$\mathrm{frac}(\mu_{\mathcal{L}}, Q, \tau) := \sup_{\varphi: X\to[-1,1]} \Pr_{\mathcal{L}\sim\mu_{\mathcal{L}}} \big(|P_{\mathcal{L}}[\varphi] - Q[\varphi]| \geq \tau\big).$$

那么对任意 $\tau > 0$,

$$\mathrm{frac}(\mu_{\mathcal{L}}, Q, \tau) \leq 2\exp\!\left(-c_{\mathrm{par}}\,\frac{M\,\tau^2}{L_0^2}\right),$$

其中 c_{par} 是引理 7中的常数， M 是参数维数。

证明。 对每个固定的 φ，引理 12 告诉我们， F_φ 在 L_0-Lipschitz 连续，定义于 $\Theta \subseteq S^{M-1}$上。将 μ_Θ 视为 μ_S 在 Θ上的归一化限制，我们可以直接应用引理 7 （这会为球面上任意满测度子集上的归一化测度给出同类型的集中性），从而得到

$$\Pr_{\theta\sim\mu_\Theta}\big(|F_\varphi(\theta) - \mathbb{E}_{\theta\sim\mu_\Theta} F_\varphi(\theta)| \geq \tau\big) \leq 2\exp\!\left(-c_{\mathrm{par}}\,\frac{M\,\tau^2}{L_0^2}\right).$$

用推前测度 $\mu_{\mathcal{L}}$ 表示，这等价于

$$\Pr_{\mathcal{L}\sim\mu_{\mathcal{L}}}\Big(|P_{\mathcal{L}}[\varphi] - Q[\varphi]| \geq \tau\Big) \leq 2\exp\!\left(-c_{\mathrm{par}}\,\frac{M\,\tau^2}{L_0^2}\right),$$

其中 $Q[\varphi] = \mathbb{E}_{\mathcal{L}} P_{\mathcal{L}}[\varphi]$。由于右侧与 φ 无关，对所有 $\varphi:\ X \to[-1,1]$ 取上确界可得

$$\mathrm{frac}(\mu_{\mathcal{L}}, Q, \tau) \leq 2\exp\!\left(-c_{\mathrm{par}}\,\frac{M\,\tau^2}{L_0^2}\right).$$

■

备注16 （随机林德布拉德算子系综中的度量、测度与几何）。 定理 *10* 的形式可以很自然地在集中框架 *[Led01],* 中得到理解：我们真正使用的是一个度量概率空间

$$(\Theta, d_2, \mu_\Theta), \qquad d_2(\theta,\theta') := \|\theta - \theta'\|_2,$$

其中， $\Theta \subseteq S^{M-1}$ 是参数球面上的一个满测度子集，而 μ_Θ 是通过限制并重新归一化球面上的旋转不变测度（归一化表面测度）得到的概率测度。对于每个测试函数 $\varphi:\ X \to [-1,1]$ ，我们考虑

$$F_\varphi : \Theta \to \mathbb{R}, \qquad F_\varphi(\theta) := P_{\mathcal{L}(\theta)}[\varphi].$$

引理 *12* 指出， F_φ 是 L_0-*Lipschitz* 函数，其度量基于 d_2；而引理 *7*是关于 $(S^{M-1},\ d_2,\ \mu_S)$的列维型集中定理。结合二者即可得到参数空间上的所需集中不等式。

这种结构与量子信息中的哈尔随机态和酉算子完全类似 *[Mel24, BHH16, Haf22]*。对于随机纯态，其空间是希尔伯特空间中的 2-范数球面 S^{2d-1} ，距离是由内积诱导的欧几里得度量，测度则是由 $U(d)$ 在球面上诱导的唯一酉不变概率测度（也称为哈尔测度）。在这种几何结构中，对于任意 1-*Lipschitz* 函数 $f:\ S^{2d-1} \to \mathbb{R}$ 可得

$$\Pr_{\psi\sim\mu_{\mathrm{Haar}}}\big(|f(\psi) - \mathbb{E}f| \geq s\big) \leq 2\exp(-c\,d\,s^2),$$

这正是用随机纯态的语言表述的列维集中。

在我们的参数球面系综中，欧几里得度量 d_2 与旋转不变测度 μ_Θ 发挥着相同的作用：它们保证参数空间中的所有坐标方向在几何上都不存在偏向，并确保列维 *[Led01]* 意义下的等周常数随维数线性增长 M，从而得到一个带有关于 M 的指数因子的集中界：

$$\Pr_{\theta\sim\mu_\Theta}\left(|F_\varphi(\theta)-\mathbb{E}_{\mu_\Theta}F_\varphi|\geq\tau\right)\leq 2\exp\left(-c_{\text{par}}\,\frac{M\tau^2}{L_0^2}\right).$$

参数化中引入的归一化因子 $\delta/\sqrt{M}$ 恰好能防止利普希茨常数$L_0 = t\delta C_G$ 随维数增大而发散。

更一般地，正如 *[Led01]*, 所强调的，集中理论并不局限于 2-范数球面和 *Haar* 测度；它适用于任意度量概率空间 (X, d, μ)。如果我们愿意改变参数空间上的度量和测度，例如：

*i.*选择独立坐标的乘积测度（每个局部耦合参数 θ_j 都是一个独立随机变量），并采用 ℓ_1 或汉明距离；

ii. 或者选择一种对称对数凹测度（类似于高维高斯分布），并配合欧几里得度量；

那么，只要(X, d, μ) 具有良好的等周性质（例如满足庞加莱不等式或对数索博列夫不等式），仍然可以得到关于 F_φ 的集中不等式，不过常数和指数标度结构会随底层几何而变化。在这种情况下，所诱导的 $\mu_{\mathcal{L}}$ 描述了另一种随机林布拉德算子系综，对应于不同的物理建模假设（例如，局部跳跃强度彼此独立随机），而不是本文所讨论的基于欧几里得球面的“参数 *Haar*”系综。

值得再次强调的是，这些集中性和 *SQ* 困难性结果本质上取决于分布，且总是相对于选定的先验分布 $\mu_{\mathcal{L}}$ 来表述。这与随机电路领域 *[Mel24*、*BHH16*、*Haf22]* 以及随机矩阵理论领域 *[Meh04*、*KHM19]*中的情形完全类似：

i. 在随机电路文献中，人们会选择 *Haar* 随机酉算子，或更符合物理实际的局部随机门集，从而定义一个电路系综 $\mu_{\mathcal{C}}$，随后研究相对于该系综的典型输出分布的集中性和平均情形困难性 *[NIS+ 25]*。

ii. 在随机矩阵理论中，高斯酉系综（*GUE*）等系综 *[KHM19]*, 吉布雷系综 *[HKKU20]*,和局部随机哈密顿量 *[SHU21* 、 *NO14]* 是无结构混沌哈密顿量和开放系统非厄米生成元的标准随机模型；所有关于谱统计和典型性的论述，都是相对于这些系综而言的 μ_H。

iii. 对于 *Lindblad* 算子，我们的定义 *23* 采用无偏的欧几里得球面参数系综作为基准示例。类似地，也可以考虑更能反映特定物理平台的其他随机 *GKSL* 系综（例如随机局部跳跃与随机 *Kossakowski* 矩阵），并在各自对应的 $(X,\ d,\ \mu)$ 上应用列维型工具，以得到相应的开放系统集中性和统计查询困难性结果。

因此，定理 *10*以及前述引理表明，一旦我们在林布拉德空间上固定一个具有物理自然性且几何性质良好的随机系综 $(\mathcal{F}\ \mu_{\mathcal{L}})$，典型的统计查询期望 $P_{\mathcal{L}}[\varphi]$ 将在参数空间上呈现出很强的列维型集中性。在第 *VD* 节中，我们将介绍另一个基于 ℓ_1度量以及独立局部耦合的乘积测度系综的例子。

D. 独立局部耦合的乘积测度集中

上面对参数球面（Θ，μ_Θ）的讨论依赖于欧几里得球面 S^{M-1} 上的旋转不变测度和列维引理。本小节介绍一个相应的系综，其中局部耦合彼此独立，每个局部耦合常数都是一个幅度较小的独立随机变量，由此在参数空间上得到乘积测度以及一个 ℓ_1 度量。与球面情形不同，此处无需引入 $\delta/\sqrt{M}$ 归一化，即可使 Lipschitz 常数与维数 M 无关；代价是通过麦克迪尔米德型不等式，使 $\underline{M}$ 对集中指数产生影响。

定义24 (具有独立局部耦合的随机林布拉德算子系综)。 令 $M \in \mathbb{N}$ 为参数维数。设单坐标分布 μ_1 的支撑集为区间 $[-\delta, \delta] \subset \mathbb{R}$ （其中 $\delta > 0$ 确定耦合的典型尺度），并定义

$$\Theta_{\mathrm{prod}} := [-\delta, \delta]^M, \qquad \mu_{\mathrm{prod}} := \mu_1^{\otimes M}.$$

对于 $\theta = (\theta_1, \ldots, \theta_M) \in \Theta_{\mathrm{prod}}$，定义线性参数化

$$\mathcal{L}(\theta) := \mathcal{L}_{\mathrm{ref}} + \sum_{j=1}^{M} \theta_j G_j,$$

其中 L_{ref} 是一个固定的 *Lindblad* 算子，$\{G_j\}_{j=1}^M$ 是一族线性映射，且对于某个常数 $C_G > 0$，有 $\|G_j\|_{1\to 1} \le C_G$ 。定义推前测度

$$\mu_{\mathcal{L}}^{\mathrm{prod}} := (\mathcal{L})_{\#}\mu_{\mathrm{prod}},$$

即，对于任意可测集合 A， $\mu^{\mathrm{prod}}{}_{\mathcal{L}}(A) := \mu_{\mathrm{prod}}\{\theta : L(\theta) \in A\}$。在参数空间上赋予 ℓ_1 度量

$$d_1(\theta, \theta') := \|\theta - \theta'\|_1 = \sum_{j=1}^{M} |\theta_j - \theta'_j|.$$

引理13(Lip 乘积测度参数空间上的施密茨常数)。在定义 24 的设定下，l et

$$F_\varphi(\theta) := P_{\mathcal{L}(\theta)}[\varphi], \qquad \theta \in \Theta_{\mathrm{prod}},$$

对于任意测试函数 φ： $X \to [-1, 1]$。那么对于所有 θ、 $\theta' \in \Theta_{\mathrm{prod}}$，

$$|F_\varphi(\theta) - F_\varphi(\theta')| \le L_1 \|\theta - \theta'\|_1, \qquad L_1 := t\, C_G,$$

并且 L_1 与 φ 以及维数 M无关。

证明。 根据参数化的线性性，

$$\mathcal{L}(\theta') - \mathcal{L}(\theta) = \sum_{j=1}^{M} (\theta'_j - \theta_j)\, G_j.$$

取 $1 \to 1$ 范数并利用 $\|G_j\|_{1\to 1} \le C_G$，可得

$$\begin{aligned} \big\|\mathcal{L}(\theta') - \mathcal{L}(\theta)\big\|_{1\to 1} &\le \sum_{j=1}^{M} |\theta'_j - \theta_j|\, \|G_j\|_{1\to 1} \\ &\le C_G \sum_{j=1}^{M} |\theta'_j - \theta_j| \\ &= C_G\, \|\theta' - \theta\|_1. \end{aligned}$$

根据推论 1 （关于 $P_{\mathcal{L}}[\varphi]$相对于 $\mathcal{L}$的 Lipschitz 连续性），可得

$$\begin{aligned} |F_\varphi(\theta) - F_\varphi(\theta')| &= \big|P_{\mathcal{L}(\theta)}[\varphi] - P_{\mathcal{L}(\theta')}[\varphi]\big| \\ &\le t\, \big\|\mathcal{L}(\theta') - \mathcal{L}(\theta)\big\|_{1\to 1} \\ &\le t\, C_G\, \|\theta' - \theta\|_1. \end{aligned}$$

因此， $L_1 = tC_G$ 是关于 ℓ_1 度量 d_1的一致 Lipschitz 常数，与 φ 和 M无关。■

现在，我们使用 McDiarmid 型有界差异不等式，得到乘积测度下的集中性。由于 μ_{prod} 是一个乘积测度，其坐标的支撑集包含在有界区间 $[-\delta, \delta]$ 中，因此

适用于这一经典工具。

引理14（McDiarmid有界差分不等式，参见 [Led01]）。设 $\theta = (\theta_1, \dots, \theta_M)$ 具有独立坐标，$\theta_j \sim \mu_1$ 支撑集包含于 $[-\delta, \delta]$。设 $F\colon \Theta_{\mathrm{prod}} \to \mathbb{R}$ 满足：对每个 j，都存在 $c_j \geq 0$，使得对于任意 θ 以及任意 a，$a' \in [-\delta, \delta]$，

$$\left|F(\theta_1, \dots, \theta_{j-1}, a, \theta_{j+1}, \dots, \theta_M) - F(\theta_1, \dots, \theta_{j-1}, a', \theta_{j+1}, \dots, \theta_M)\right| \leq c_j.$$

那么，对所有 $\tau > 0$，

$$\Pr_{\theta \sim \mu_{\mathrm{prod}}}\left(|F(\theta) - \mathbb{E}F| \geq \tau\right) \leq 2\exp\left(-\frac{2\tau^2}{\sum_{j=1}^{M} c_j^2}\right).$$

结合引理13 与引理14 可得针对具有独立局部耦合的系综的集中定理。

定理 11（独立局部耦合系综的最大可区分比例上界）。设（Θ_{prod}，μ_{prod}，$\mathcal{L}$（θ）如定义*24*所述，并设利普希茨常数 L_1 如引理*13*所述。在统计查询接口中，对每个测试函数 φ： $X \to [-1, 1]$ 定义

$$F_\varphi(\theta) := P_{\mathcal{L}(\theta)}[\varphi], \qquad Q[\varphi] := \mathbb{E}_{\mathcal{L} \sim \mu_{\mathcal{L}}^{\mathrm{prod}}} P_{\mathcal{L}}[\varphi] = \mathbb{E}_{\theta \sim \mu_{\mathrm{prod}}} F_\varphi(\theta).$$

定义最大可区分比例

$$\mathrm{frac}(\mu_{\mathcal{L}}^{\mathrm{prod}}, Q, \tau) := \sup_{\varphi: X \to [-1,1]} \Pr_{\mathcal{L} \sim \mu_{\mathcal{L}}^{\mathrm{prod}}}\left(|P_{\mathcal{L}}[\varphi] - Q[\varphi]| \geq \tau\right).$$

那么，对任意 $\tau > 0$，

$$\mathrm{frac}(\mu_{\mathcal{L}}^{\mathrm{prod}}, Q, \tau) \;\leq\; 2\exp\left(-c_{\mathrm{prod}}\,\frac{\tau^2}{M\,\delta^2\,L_1^2}\right), \qquad L_1 = tC_G,$$

其中 $c_{\mathrm{prod}} > 0$ 是一个绝对常数（例如，可取 *McDiarmid* 不等式所建议的 $c_{\mathrm{prod}} = \frac{1}{2}$）。

证明。固定一个测试函数 φ。对于任意 j，考虑仅改变第 j 个坐标：给定 $\theta \in \Theta_{\mathrm{prod}}$ 和 a，$a' \in [-\delta, \delta]$，定义

$$\theta^{(j,a)} := (\theta_1, \dots, \theta_{j-1}, a, \theta_{j+1}, \dots, \theta_M), \quad \theta^{(j,a')} := (\theta_1, \dots, \theta_{j-1}, a', \theta_{j+1}, \dots, \theta_M).$$

根据引理 L_1-Lipschitz 性质13，

$$\begin{aligned}\left|F_\varphi(\theta^{(j,a)}) - F_\varphi(\theta^{(j,a')})\right| &\leq L_1 \left\|\theta^{(j,a)} - \theta^{(j,a')}\right\|_1 \\ &= L_1\,|a - a'| \\ &\leq 2\delta\,L_1.\end{aligned}$$

因此，我们可以取 $c_j := 2\delta L_1$ 对所有 $1 \leq j \leq M$。将其代入引理14 可得

$$\begin{aligned}\Pr_{\theta \sim \mu_{\mathrm{prod}}}\left(|F_\varphi(\theta) - \mathbb{E}_{\theta \sim \mu_{\mathrm{prod}}} F_\varphi(\theta)| \geq \tau\right) &\leq 2\exp\left(-\frac{2\tau^2}{\sum_{j=1}^{M} c_j^2}\right) \\ &\leq 2\exp\left(-\frac{2\tau^2}{M \cdot (2\delta L_1)^2}\right) \\ &= 2\exp\left(-\frac{\tau^2}{2M\delta^2 L_1^2}\right).\end{aligned}$$

就推前测度 μ^{prod} 而言，这等价于

$$\Pr_{\mathcal{L}\sim\mu_{\mathcal{L}}^{\mathrm{prod}}}\Big(|P_{\mathcal{L}}[\varphi]-Q[\varphi]|\geq\tau\Big)\leq 2\exp\!\Big(-\frac{\tau^2}{2M\delta^2L_1^2}\Big),$$

其中 $Q[\varphi]=\mathbb{E}_{\mathcal{L}}P_{\mathcal{L}}[\varphi]$。由于右侧与 φ 无关，对所有 φ 取上确界： $X\to[-1,1]$ 可得

$$\mathrm{frac}(\mu_{\mathcal{L}}^{\mathrm{prod}},Q,\tau)\leq 2\exp\!\Big(-c_{\mathrm{prod}}\,\frac{\tau^2}{M\,\delta^2\,L_1^2}\Big),$$

对于某个绝对常数 c_{prod} （例如 $c_{\mathrm{prod}}=\frac{1}{2}$ ）。 - ■

备注 17 （恢复 $\exp(-\Omega(M))$ 标度）。 若希望在乘积测度模型中恢复 $\exp(-\Omega(M))$ 标度，有多种方法可供选择。例如，可以通过将每个局部参数的取值范围缩小至 M 来强化小耦合假设，即令

$$\theta_j\in\Big[-\frac{\delta}{M},\frac{\delta}{M}\Big].$$

那么 $\|L^{\mathrm{prod}}(\theta)-L_{\mathrm{ref}}\|_{1\to1}\leq\sum_j|\theta_j|\|G_j\|_{1\to1}\leq M\cdot\frac{\delta}{M}C_G=\delta C_G$，因此扰动的整体尺度仍为 $O(\delta)$，而有界差分常数变为 $c_j\leq 2(\delta/M)L_1$，并且

$$\sum_{j=1}^{M}c_j^2\leq M\cdot\big(2\delta L_1/M\big)^2=\mathcal{O}\big(\delta^2L_1^2/M\big).$$

代入 *McDiarmid* 得

$$\Pr(|F_\varphi-\mathbb{E}F_\varphi|\geq\tau)\lesssim\exp\!\Big(-\Omega\Big(M\,\frac{\tau^2}{\delta^2L_1^2}\Big)\Big),$$

这与球面情形中的$\exp(-\Omega(M))$ 缩放相呼应。从参数化的角度来看，这等价于将整体归一化因子 $\delta/\sqrt{M}$ （在球面系综中使用）“移入”坐标范围：一种表述是 $L=L_{\mathrm{ref}}+\frac{\delta}{\sqrt{M}}\sum_j\theta_jG_j$，$\|\theta\|_2=1$；另一种是 $L=L_{\mathrm{ref}}+\sum_j\theta_jG_j$，$|\theta_j|\lesssim1/M$；在这两种情况下，$L$ 空间中的扰动尺度都是 $O(\delta)$，但参数空间上的度量和测度以不同方式分配这一尺度。

因此，我们的 Lipschitz 和列维工具为分母提供了一个指数级小的上界$\max_\varphi\Pr[|P[\varphi]-Q[\varphi]|>\tau]$，而对于平均情形 SQ 学习，我们还需要控制分子中的“远离Q”区域体积（即 $\beta-\Pr[d_{\mathrm{TV}}(P,Q)\leq\epsilon+\tau]$的行为），我们将在第 VII 节中详细讨论这一点。

E. 平均情形下学习随机 Lindblad 通道的 QPStat 困难性

Pr接下来，我们转而讨论学习随机 Lindblad 通道系综的困难性 .

引理 15 （QPStat 期望值关于生成元参数的 Lipschitz 连续性）。 采用定义 *23* 的记号，设 $\mathcal{L}(\theta)$ 是由参数空间 $(\Theta,\ d,\ \mu_\Theta)$ 索引的一族 *Lindblad* 算子，并假设：

1. 每个 $\mathcal{L}(\theta)$， $\theta\in\Theta$，都是 *GKSL* 生成元，且线段插值 $\mathcal{L}_\alpha:=(1-\alpha)\mathcal{L}(\theta)+\alpha\mathcal{L}(\theta')$ 对于所有 $\alpha\in[0,1]$ （根据引理 *9*）始终处于 *GKSL* 锥内；

2. 存在一个与参数维数 M 无关的常数 $L_{\mathcal{L}}>0$，使得

$$\|\mathcal{L}(\theta)-\mathcal{L}(\theta')\|_{1\to1}\leq L_{\mathcal{L}}\,\|\theta-\theta'\|_2,\qquad\forall\,\theta,\theta'\in\Theta. \tag{5.2}$$

令 $E_\theta := e^{t\mathcal{L}(\theta)}$ 为量子马尔可夫半群在固定时间 $t>0$ 下的一步信道。对于任意量子态 ρ 和算子 O，满足 $\|\rho\|_1 \le 1$ 和 $\|O\|_\infty \le 1$，定义

$$f_{\rho,O}(\theta) := \mathrm{Tr}\big[O\, E_\theta(\rho)\big] = \mathrm{Tr}\big[O\, e^{t\mathcal{L}(\theta)}(\rho)\big]. \tag{5.3}$$

那么存在一个常数

$$L_{\mathrm{QP}} := t\, L_{\mathcal{L}}, \tag{5.4}$$

使得对于所有 $\theta, \theta' \in \Theta$,

$$\big|f_{\rho,O}(\theta) - f_{\rho,O}(\theta')\big| \le L_{\mathrm{QP}}\, \|\theta - \theta'\|_2. \tag{5.5}$$

换言之，$f_{\rho,\,O}$ 在$(\Theta, \|\cdot\|_2)$上是 L_{QP}-*Lipschitz* 的，且该 *Lipschitz* 常数与$(\rho, O$无关$)$.

证明。 证明与引理 12 和定理 10几乎完全相同。

步骤 *1*：从信道差异到期望差异。 对于任意 θ, θ' 我们有

$$\begin{aligned}
\big|f_{\rho,O}(\theta) - f_{\rho,O}(\theta')\big| &= \big|\mathrm{Tr}\big[O\,(E_\theta - E_{\theta'})(\rho)\big]\big| \\
&\le \|O\|_\infty \,\big\|(E_\theta - E_{\theta'})(\rho)\big\|_1 \\
&\le \|O\|_\infty \,\|E_\theta - E_{\theta'}\|_{1\to 1}\, \|\rho\|_1 \\
&\le \|E_\theta - E_{\theta'}\|_{1\to 1},
\end{aligned}$$

其中我们用到了矩阵 Hölder 不等式、诱导的 $1\to 1$ 范数的定义以及界 $\|O\|_\infty \le 1$,$\|\rho\|_1 \le 1$。

步骤 *2*：通过生成元之差界定信道之差。沿线段定义$\mathcal{L}_\alpha := (1-\alpha)\mathcal{L}(\theta) + \alpha\mathcal{L}(\theta')$ 并令 $E_\alpha := e^{t\mathcal{L}_\alpha}$。根据引理 9，$\mathcal{L}_\alpha$ 对所有 $\alpha \in [0,1]$都是 GKSL，因此 E_α 是完全正迹保持的，并满足 $\|E_\alpha\|_{1\to 1} \le 1$。

根据弗雷歇导数公式（引理6），我们有

$$\frac{d}{d\alpha} E_\alpha = \int_0^t e^{(t-s)\mathcal{L}_\alpha}\, \big(\mathcal{L}(\theta') - \mathcal{L}(\theta)\big)\, e^{s\mathcal{L}_\alpha}\, ds. \tag{5.6}$$

取诱导的 $1\to 1$ 范数并利用完全正迹保持映射的压缩性，可得

$$\begin{aligned}
\Big\|\frac{d}{d\alpha} E_\alpha\Big\|_{1\to 1} &\le \int_0^t \big\|e^{(t-s)\mathcal{L}_\alpha}\big\|_{1\to 1}\, \big\|\mathcal{L}(\theta') - \mathcal{L}(\theta)\big\|_{1\to 1}\, \big\|e^{s\mathcal{L}_\alpha}\big\|_{1\to 1}\, ds \\
&\le \int_0^t \big\|\mathcal{L}(\theta') - \mathcal{L}(\theta)\big\|_{1\to 1}\, ds \\
&= t\, \big\|\mathcal{L}(\theta') - \mathcal{L}(\theta)\big\|_{1\to 1}.
\end{aligned}$$

步骤 *3*：沿参数空间中的线段积分。根据微积分基本定理,

$$E_\theta - E_{\theta'} = E_1 - E_0 = \int_0^1 \frac{d}{d\alpha} E_\alpha\, d\alpha,$$

因此

$$\begin{aligned}
\|E_\theta - E_{\theta'}\|_{1\to 1} &\le \int_0^1 \Big\|\frac{d}{d\alpha} E_\alpha\Big\|_{1\to 1}\, d\alpha \\
&\le \int_0^1 t\, \big\|\mathcal{L}(\theta') - \mathcal{L}(\theta)\big\|_{1\to 1}\, d\alpha \\
&= t\, \big\|\mathcal{L}(\theta') - \mathcal{L}(\theta)\big\|_{1\to 1}.
\end{aligned}$$

将其与生成元利普希茨条件（5.2）结合可得

$$\|E_\theta - E_{\theta'}\|_{1\to 1} \le t\, L_{\mathcal{L}}\, \|\theta - \theta'\|_2.$$

将此上界代入步骤 1 中的估计，得到

$$\left|f_{\rho,O}(\theta) - f_{\rho,O}(\theta')\right| \le t\, L_{\mathcal{L}}\, \|\theta - \theta'\|_2,$$

这恰好就是（5.5），其中 $L_{\mathrm{QP}} := tL_{\mathcal{L}}$。此 Lipschitz 常数对所有满足 ρ 和 O 的 $\|\rho\|_1 \le 1$，$\|O\|_\infty \le 1$均一致成立。 ■

注 18。对于定义 *26*中的具体随机局域林德布拉德系综，结合（6.1）和（6.2）可得 $L_{\mathcal{L}} \lesssim \delta C_G$，因此 $L_{\mathrm{QP}} = tL_{\mathcal{L}}$ 与引理 $L_0 = t\delta C_G$ *17*中的量级相同。这表明，经典 *SQ* 和 *QPStat* 访问模型在底层 *Lipschitz* 结构层面自然兼容。

接下来，我们将前面在参数空间上证明的列维/McDiarmid 型集中结果改写为一种可直接作用于 QPStat 期望值的形式。

引理 16（QPStat 偏差的参数空间集中）。设（Θ，d，μ_Θ）是本文所考虑的随机 *Lindbladian* 参数系综之一，其参数维数为 M，并假设它满足球面系综（定理*10*）和乘积测度系综（定理 *11* 及注 *17*）所确立的集中性结论：也就是说，存在常数 $c_{\mathrm{par}} > 0$ 和 $L > 0$，使得对于任意可测的 *L-Lipschitz* 函数 $F:\ \Theta \to \mathbb{R}$ 以及任意 $\tau > 0$，

$$\Pr_{\theta\sim\mu_\Theta}\left(|F(\theta) - \mathbb{E}_\Theta F| \ge \tau\right) \le 2\exp\!\left(-c_{\mathrm{par}}\frac{M\tau^2}{L^2}\right). \tag{5.7}$$

令 $E_\theta := e^{t\mathcal{L}(\theta)}$，并定义平均通道

$$\bar{E} := \mathbb{E}_{\theta\sim\mu_\Theta} E_\theta.$$

对于任意一对（ρ、O），满足 $\|\rho\|_1 \le 1$ 和 $\|O\|_\infty \le 1$，令

$$F_{\rho,O}(\theta) := \mathrm{Tr}\big[O\, E_\theta(\rho)\big].$$

若 $L(\theta)$ 满足引理 *15* 的生成元利普希茨条件，则 $F_{\rho,\,O}$ 是 L_{QP}-*Lipschitz* 的，并且对于所有 $\tau > 0$，

$$\Pr_{\theta\sim\mu_\Theta}\Big(\big|\mathrm{Tr}[OE_\theta(\rho)] - \mathrm{Tr}[O\bar{E}(\rho)]\big| \ge \tau\Big) \le 2\exp\!\Big(-c_{\mathrm{par}}\frac{M\tau^2}{L_{\mathrm{QP}}^2}\Big), \tag{5.8}$$

其中 $L_{\mathrm{QP}} = tL_{\mathcal{L}}$。

证明。根据引理 15，$F_{\rho,\,O}$ 在 $(\Theta,\ \|\cdot\|_2)$ 上是 L_{QP}-Lipschitz 的，其中 $L_{\mathrm{QP}} = tL_{\mathcal{L}}$。另一方面，

$$\begin{aligned}\mathbb{E}_{\theta\sim\mu_\Theta} F_{\rho,O}(\theta) &= \mathbb{E}_{\theta\sim\mu_\Theta}\,\mathrm{Tr}[OE_\theta(\rho)]\\ &= \mathrm{Tr}\big[O\,(\mathbb{E}_{\theta\sim\mu_\Theta}E_\theta)(\rho)\big]\\ &= \mathrm{Tr}[O\bar{E}(\rho)].\end{aligned}$$

因此 $F := F_{\rho,\,O}$ 的 Lipschitz 常数为 L_{QP}，均值为 $\mathbb{E}_\Theta F = \mathrm{Tr}[OE(\rho)]$。应用（5.7），取 $L := L_{\mathrm{QP}}$即可立即得到（5.8）。 ■

定义 25（随机 Lindblad 通道系综与 QPStat 模型）。设 $(\Theta,\ d,\ \mu_\Theta)$ 是前文定义的林德布拉德生成元参数空间之一（例如，定义 *26*中的球面随机扰动系综或独立局部耦合乘积测度系综），其参数维数为 M。

对于每个参数 $\theta \in \Theta$，令

$$\mathcal{L}(\theta):\ \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$$

为一个 *Lindblad* 生成元。令相应的量子马尔可夫半群为 $\Lambda_t^{(\theta)} := e^{t\mathcal{L}(\theta)}$，并假设其对所有 $t \geq 0$ 均为完全正迹保持。在固定的演化时间 $t > 0$，我们得到 *CPTP* 通道系综

$$E_\theta := \Lambda_t^{(\theta)} = e^{t\mathcal{L}(\theta)}, \qquad \theta \sim \mu_\Theta,$$

以及平均通道

$$\bar{E} := \mathbb{E}_{\theta\sim\mu_\Theta} E_\theta.$$

对于每个信道 E，*QPStat* 预言机 $QPStat_E$ 定义同定义 *17*。一个 *QPStat* 学习算法$\mathcal{A}$ 与未知参数 $\theta \sim \mu_\Theta$ 及其关联信道 E_θ 交互时，最多可自适应地调用该预言机 q 次；我们称其使用了 q 次精度为 τ的 *QPStat* 查询。

注意，在定义 6.2中的线性参数化 26下，引理 9保证 $\mathcal{L}(\theta)$ 构成一个 GKSL 切片，而引理 17 和引理15 给出了一致 Lipschitz 常数:

$$\|\mathcal{L}(\theta) - \mathcal{L}(\theta')\|_{1\to1} \leq \delta C_G \|\theta - \theta'\|_2, \qquad L_{\mathrm{QP}} = t\delta C_G.$$

因此，对于这些 conc 引理 16的假设自动满足。

定理 12 (随机 Lindblad 通道的指数级平均情形 QPStat 下界)。 设 $(\Theta,\ d,\ \mu_\Theta)$是本文考虑的随机 *Lindbladian* 参数系综之一，其参数维数为 M，¯并设 $\mathcal{L}(\theta)$、 E_θ 以及平均通道 E 定义同定义 *25*。

假设:

(i) （生成元利普希茨性质）存在一个常数 $L_\mathcal{L} > 0$，与 M 无关，使得 at

$$\|\mathcal{L}(\theta) - \mathcal{L}(\theta')\|_{1\to1} \leq L_\mathcal{L} \|\theta - \theta'\|_2, \qquad \forall\, \theta, \theta' \in \Theta,$$

and 线段插值 $\mathcal{L}_\alpha$ 始终处于 *GKSL* 锥中（由引理 *9*保证） *);*

(ii) （参数空间上的集中性）参数空间 (Θ, μ_Θ) 满足引理 (5.8) 中的集中不等式，其中 *16*，即对任意 $\|\rho\|_1 \leq 1$, $\|O\|_\infty \leq 1$ 以及任意 $\tau > 0$,

$$\Pr_{\theta\sim\mu_\Theta}\Big(\big|\mathrm{Tr}[OE_\theta(\rho)] - \mathrm{Tr}[O\bar{E}(\rho)]\big| \geq \tau\Big) \leq 2\exp\Big(-c_{\mathrm{par}}\frac{M\tau^2}{L_{\mathrm{QP}}^2}\Big),$$

其中 $L_{\mathrm{QP}} = tL_\mathcal{L}$ 与 M 无关。

考虑任意一个针对随机信道 E_θ （具有 $\theta \sim \mu_\Theta$）的 *QPStat* 学习算法 *A*，使得:

i. *A* 至多使用 q 次 *QPStat* 查询，精度为 τ;

ii.存在常数 $\alpha > 1/2$ 和 $\beta > 0$，使得对于

$$\Theta_{\mathrm{good}} := \Big\{\theta \in \Theta : \Pr_{internal\ randomness}\big[d_\diamond(\widehat{E}, E_\theta) \leq \varepsilon\big] \geq \alpha\Big\},$$

有 $\mu_\Theta(\Theta_{\mathrm{good}}) \geq \beta$。

那么存在一个与 M 无关的常数 $c > 0$，使得对于所有充分大的 M （特别是在可以取 $\beta = 1$ 的最坏情况设置下），

$$q \ \geq\ c\,(2\alpha - 1)\,\beta\,\exp\big(c\,M\big). \tag{5.9}$$

特别是， q 必须至少随参数维数 M 指数级增长，也就是说，

$$q \geq \exp\big(\Omega(M)\big). \tag{5.10}$$

换言之，在 *QPStat* 访问模型下，随机林德布拉德信道系综在平均意义上难以学习，且所需资源呈指数增长。

证明。 根据引理 16，对于任意一对 $(\rho,\ O)$ 满足 $\|\rho\|_1 \le 1$ 且 $\|O\|_\infty \le 1$ 的对象，我们有

$$\Pr_{\theta\sim\mu_\Theta}\Big(\big|\mathrm{Tr}[OE_\theta(\rho)] - \mathrm{Tr}[O\bar{E}(\rho)]\big| \ge \tau\Big) \le 2\exp\Big(-c_{\mathrm{par}}\frac{M\tau^2}{L_{\mathrm{QP}}^2}\Big). \tag{5.11}$$

因此

$$\Gamma := \max_{\rho,O}\Pr_{\theta\sim\mu_\Theta}\Big(\big|\mathrm{Tr}[OE_\theta(\rho)] - \mathrm{Tr}[O\bar{E}(\rho)]\big| \ge \tau\Big) \le 2\exp\Big(-c_{\mathrm{par}}\frac{M\tau^2}{L_{\mathrm{QP}}^2}\Big), \tag{5.12}$$

其中最大值取遍所有 $\|\rho\|_1 \le 1$、 $\|O\|_\infty \le 1$。

另一方面，将测度为 $\{E_\theta\}$ 的信道系综 μ_Θ 视为引理 $(\mathcal{E}\ \mu)$ 中的5，并取¯参考信道为 E，可得

$$q+1 \ge \frac{(2\alpha-1)\,\beta}{\Gamma}. \tag{5.13}$$

结合（5.12）和（5.13），得到

$$\begin{aligned} q+1 &\ge \frac{(2\alpha-1)\,\beta}{\Gamma} \\ &\ge \frac{(2\alpha-1)\,\beta}{2}\exp\Big(\frac{c_{\mathrm{par}}M\tau^2}{L_{\mathrm{QP}}^2}\Big). \end{aligned}$$

定义

$$c := \frac{c_{\mathrm{par}}\tau^2}{2L_{\mathrm{QP}}^2} > 0. \tag{5.14}$$

Then

$$q+1 \ \ge\ \frac{(2\alpha-1)\,\beta}{2}\,\exp(2cM). \tag{5.15}$$

当 M 足够大时，加法常数 **1** 可以吸收到指数项中：存在 M_0，使得对所有 $M \ge M_0$，

$$q \ge \frac{(2\alpha-1)\,\beta}{4}\,\exp(2cM).$$

将固定乘法常数吸收到 c 中（并在必要时调整 M_0），这意味着存在一个与 M 无关的常数 $c>0$，使得

$$q \ \ge\ c\,(2\alpha-1)\,\beta\,\exp\big(cM\big),$$

这恰好就是所声称的下界（5.9）。特别地，

$$q \ge \exp\big(\Omega(M)\big),$$

也就是说，QPStat 查询的数量必须至少随参数维数 M 呈指数增长。至此，证明完毕。■

备注19 （物理解释）。 与我们关于输出分布的 *SQ* 困难性结果相比，定理 *12* 表明，即使赋予学习器更强大的 *QPStat* 访问能力（允许使用任意输入态，并对任意有界可观测量进行测量），只要参数维数 M 足够大，典型的 *Lindblad* 通道在平均意义下仍然难以通过菱形距离来学习，且困难性呈指数级。

从物理角度看，定理 *12* 表明，对于一种高维且具有物理自然性的随机 *Lindblad* 算子系综，即使学习器能够在每次 *QPStat* 查询中以全局且纠缠的方式探测信道，典型 *Lindblad* 算子噪声的参数刚性和统计集中性仍会迫使任何

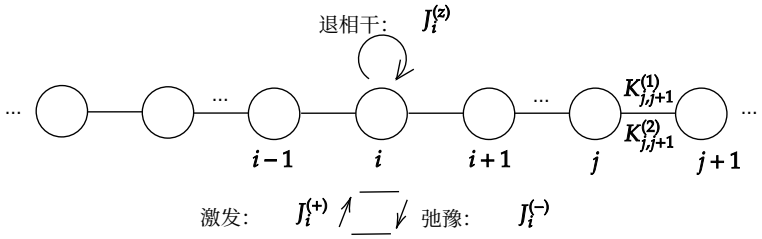

图 3. 一维自旋链上的随机局域林布拉德算符。每个圆圈代表链上的一个量子比特。在位点 i，局域退相干由跳跃算符 $J_i^{(z)}$ 描述，并以环形箭头表示。激发和弛豫过程分别由振幅升算符和振幅降算符 $J_i^{(+)}$ and $J_i^{(-)}$ 实现。在每条键 $(j,\ j+1)$ 上，我们加入二体耗散通道 $K_j^{(1)},\ _{j+1}$ and $K_j^{(2)},\ _{j+1}$，例如非相干自旋交换和关联退相干。在我们的构造中，相应的耗散子被汇集为一组局部方向 $\{G_j\}$，并纳入球面随机扰动参数化 $\mathcal{L}(\theta) = \mathcal{L}_{\mathrm{ref}} + \frac{\delta}{\sqrt{M}} \sum_j \theta_j G_j$。

旨在重构微观 *Lindblad* 算子结构（以菱形距离较小为标准）的程序平均需要使用指数级数量的统计查询。结合我们此前关于分布层面 *SQ* 困难性的结果，这描绘出了一幅连贯的图景：在开放系统场景中，无论是学习诱导输出分布，还是学习底层量子信道本身，在 *QPStat/SQ* 框架下通常都具有指数级困难性。

VI. 物理上自然的球面随机扰动林德布拉德算子系综

在本小节中，我们提出一种物理上自然的随机 Lindblad 算子系综模型，并在该模型中严格实现此前提出的“随机 Lindblad 算子系综的集中性”这一抽象假设。具体而言，在一个高维参数球面上，对于所有 SQ 测试函数 φ，映射

$$\mathcal{L} \mapsto P_{\mathcal{L}}[\varphi]$$

是一致 Lipschitz 的，因此在参数空间上满足列维型集中不等式，进而在 $\mathrm{frac}(\mu_{\mathcal{L}},\ Q,\ \tau)$ 方面蕴含 SQ 框架中的指数衰减。基于该模型，我们还讨论参数维数 M 如何依赖于系统量子比特的数量。图 3 展示了一条一维自旋链：每个位点上都有局域退相干和振幅阻尼跳跃算符，每条键上都有二体耗散通道；它们共同生成了 G_j 中所使用的球面嵌入方向。

定义 26（随机局部 Lindblad 算子系综）。考虑一条由 N 个量子比特组成的一维链，其希尔伯特空间 $H := (\mathbb{C}^2)^{\otimes N}$ 的维数为 $d = 2^N$。令 $B(H)$ 表示该系统上的算子代数。

1. 令 $\sigma \in S_d^+$ 为一个固定的满秩稳态（例如，某个局域哈密顿量 H 的吉布斯态），并设 $L_{\mathrm{ref}} : B(H) \to B(H)$ 为给定的 *GKSL* 生成元，其唯一不动点为 σ：

$$\mathcal{L}_{\mathrm{ref}}(\sigma) = 0, \qquad \Lambda_t^{(\mathrm{ref})} := e^{t\mathcal{L}_{\mathrm{ref}}} \ \textit{is a CPTP QMS.}$$

2. 在每个晶格位点 $i = 1, \ldots, N$ 上，选取一些局域林德布拉德跳跃算符，例如

$$J_i^{(z)} := \sqrt{\gamma_z}\,\sigma_i^z, \quad J_i^{(+)} := \sqrt{\gamma_+}\,\sigma_i^+, \quad J_i^{(-)} := \sqrt{\gamma_-}\,\sigma_i^-,$$

并在每个最近邻对 $(i, i+1)$ 上选取一些二体跳跃算符，例如

$$K_{i,i+1}^{(1)} := \sqrt{\kappa_1}\,\sigma_i^+\sigma_{i+1}^-, \qquad K_{i,i+1}^{(2)} := \sqrt{\kappa_2}\,\sigma_i^z\sigma_{i+1}^z.$$

对于每个跳跃算符 L_α（其中索引 α 编码了位置和类型），定义耗散子

$$\mathcal{D}_\alpha(\rho) := L_\alpha \rho L_\alpha^\dagger - \frac{1}{2}\{L_\alpha^\dagger L_\alpha, \rho\}.$$

每个 D_α 单独来看都是一个 *GKSL* 生成元（忽略哈密顿量部分）。

现在将所有这些局部耗散子依次编号为 $G_1, \ldots, G_M$，即

$$\{G_j\}_{j=1}^{M} = \{\mathcal{D}_\alpha\}_{\alpha\in\mathcal{I}},$$

其中 指标集 I 的基数为 M，且随系统规模 N 增长（例如 $M = O(N)$ 或 $O(N^2$ $))$.

3. 假设存在一个常数 $C_G > 0$ （与参数维数 M 无关），使得 t

$$\|G_j\|_{1\to 1} \le C_G, \qquad \forall j = 1, \ldots, M. \tag{6.1}$$

4. 令参数空间为实球面

$$S^{M-1} := \{\theta \in \mathbb{R}^M : \ \|\theta\|_2 = 1\},$$

选取一个足够小的 $\delta > 0$，并定义线性参数化

$$\mathcal{L}(\theta) := \mathcal{L}_{\mathrm{ref}} + \frac{\delta}{\sqrt{M}} \sum_{j=1}^{M} \theta_j G_j, \qquad \theta \in S^{M-1}. \tag{6.2}$$

5. 在 S^{M-1} 上，取均匀球面测度 μ_{sph}，并通过映射 $\theta \mapsto L(\theta)$ 将其向前推，得到

$$\mu_{\mathcal{L}} := (\mathcal{L})_{\#}\mu_{\mathrm{sph}},$$

这是定义在 *Lindblad* 算子空间上的随机局域林布拉德算符系综。我们将这个族记为

$$\mathcal{F} := \{\mathcal{L}(\theta) : \ \theta \in S^{M-1}\}.$$

引理 17 (统计查询期望的一致利普希茨界)。 保持上述设置。对于固定的演化时间 $t > 0$、输入态 $\rho_{\mathrm{in}} \in S_d^+$ 和 *POVM* $\{M_x\}_{x\in X}$，对任意 *Lindblad* 算子 L，定义测量分布

$$P_{\mathcal{L}}(x) := \mathrm{Tr}\Big(M_x\, \Lambda_t^{(\mathcal{L})}(\rho_{\mathrm{in}})\Big), \qquad x \in X,$$

对于任意测试函数 $\varphi:\ X \to [-1, 1]$,

$$P_{\mathcal{L}}[\varphi] := \sum_{x\in X} \varphi(x) P_{\mathcal{L}}(x) = \mathrm{Tr}\Big(O_\varphi\, \Lambda_t^{(\mathcal{L})}(\rho_{\mathrm{in}})\Big), \quad O_\varphi := \sum_{x\in X} \varphi(x) M_x.$$

令 C_G 如 (6.1)所示，令 $\mathcal{L}(\theta)$ 对于 $\theta \in S^{M-1}$ 由 (6.2)定义，并设

$$F_\varphi(\theta) := P_{\mathcal{L}(\theta)}[\varphi].$$

那么存在一个常数

$$L_0 := t\,\delta\, C_G,$$

使得对于任意 $\varphi:\ X \to [-1, 1]$ 以及任意 $\theta, \theta' \in S^{M-1}$,

$$|F_\varphi(\theta) - F_\varphi(\theta')| \le L_0\, \|\theta - \theta'\|_2. \tag{6.3}$$

换句话 说， F_φ 在参数球面上是 *Lipschitz* 连续的，其 *Lipschitz* 常数与 φ 无关 .

证明。 与第 VB 节中的证明类似，我们分四个步骤进行。

步骤 *1*：界定 $\|O_\varphi\|_\infty$。由于$\{M_x\}$ 是一个 POVM，我们有 $M_x \geq 0$ 和 $\sum_x M_x = \mathbb{I}$。对于任意量子态 ρ，

$$\mathrm{Tr}(O_\varphi \rho) = \sum_x \varphi(x)\,\mathrm{Tr}(M_x \rho),$$

其中 $\mathrm{Tr}(M_x\rho) \geq 0$ 且 $\sum_x \mathrm{Tr}(M_x\rho) = 1$。因此，右侧是值 $\varphi(x) \in [-1,1]$ 的加权平均，所以对所有 ρ，都有 $|\mathrm{Tr}(O_\varphi\rho)| \leq 1$。由于算子范数定义为 $\|O\|_\infty = \sup_\rho |\mathrm{Tr}(O\rho)|$，因此我们有$\|O_\varphi\|_\infty \leq 1$。

Step 2：从信道差异到期望差异。对于任意林德布拉德算子 L, L'，我们计算 te

$$\begin{aligned}
\left|P_{\mathcal{L}}[\varphi] - P_{\mathcal{L}'}[\varphi]\right| &= \left|\mathrm{Tr}\Big(O_\varphi\big[\Lambda_t^{(\mathcal{L})} - \Lambda_t^{(\mathcal{L}')}\big](\rho_{\mathrm{in}})\Big)\right| \\
&\leq \|O_\varphi\|_\infty \left\|\big[\Lambda_t^{(\mathcal{L})} - \Lambda_t^{(\mathcal{L}')}\big](\rho_{\mathrm{in}})\right\|_1 \\
&\leq \|O_\varphi\|_\infty \left\|\Lambda_t^{(\mathcal{L})} - \Lambda_t^{(\mathcal{L}')}\right\|_{1\to 1} \|\rho_{\mathrm{in}}\|_1 \\
&\leq \left\|\Lambda_t^{(\mathcal{L})} - \Lambda_t^{(\mathcal{L}')}\right\|_{1\to 1},
\end{aligned}$$

这里我们使用了矩阵霍尔德不等式 $|\mathrm{Tr}(AB)| \leq \|A\|_\infty \|B\|_1$、诱导 $1\to 1$ 范数的定义，以及界 $\|O_\varphi\|_\infty \leq 1$，$\|\rho_{\mathrm{in}}\|_1 = 1$。

步骤 *3*：通过扰动公式界定 $\left\|\Lambda_t^{(\mathcal{L})} - \Lambda^{(\mathcal{L}')}{}_t \quad\right\|_{1\to 1}$。对于 $\alpha \in [0,1]$ 定义

$$\mathcal{L}_\alpha := (1-\alpha)\mathcal{L} + \alpha\mathcal{L}',$$

并且根据引理 9可知，沿着线段 $\mathcal{L}_\alpha$ 始终是 GKSL，因此 $\Lambda_t^{(\alpha)} := e^{t\mathcal{L}_\alpha}$ 是完全正迹保持的，并且 $\|\Lambda_t^{(\alpha)}\|_{1\to 1} \leq 1$。扰动（Duhamel）公式给出

$$\frac{\mathrm{d}}{\mathrm{d}\alpha}\Lambda_t^{(\alpha)} = \int_0^t \Lambda_{t-s}^{(\alpha)} \circ (\mathcal{L}' - \mathcal{L}) \circ \Lambda_s^{(\alpha)}\,\mathrm{d}s.$$

取 $1\to 1$ 范数并利用 CPTP 映射的压缩性，可得

$$\begin{aligned}
\left\|\frac{\mathrm{d}}{\mathrm{d}\alpha}\Lambda_t^{(\alpha)}\right\|_{1\to 1} &\leq \int_0^t \left\|\Lambda_{t-s}^{(\alpha)}\right\|_{1\to 1} \|\mathcal{L}' - \mathcal{L}\|_{1\to 1} \left\|\Lambda_s^{(\alpha)}\right\|_{1\to 1} \mathrm{d}s \\
&\leq \int_0^t \|\mathcal{L}' - \mathcal{L}\|_{1\to 1}\,\mathrm{d}s \\
&= t\|\mathcal{L}' - \mathcal{L}\|_{1\to 1}.
\end{aligned}$$

对 $\alpha \in [0,1]$ 积分可得

$$\begin{aligned}
\left\|\Lambda_t^{(\mathcal{L}')} - \Lambda_t^{(\mathcal{L})}\right\|_{1\to 1} &= \left\|\int_0^1 \frac{\mathrm{d}}{\mathrm{d}\alpha}\Lambda_t^{(\alpha)}\,\mathrm{d}\alpha\right\|_{1\to 1} \\
&\leq \int_0^1 \left\|\frac{\mathrm{d}}{\mathrm{d}\alpha}\Lambda_t^{(\alpha)}\right\|_{1\to 1} \mathrm{d}\alpha \\
&\leq \int_0^1 t\|\mathcal{L}' - \mathcal{L}\|_{1\to 1}\,\mathrm{d}\alpha \\
&= t\|\mathcal{L}' - \mathcal{L}\|_{1\to 1}.
\end{aligned}$$

步骤 *4*：令 $\mathcal{L}(\theta)$，$\mathcal{L}(\theta')$。由（6.2），

$$\mathcal{L}(\theta') - \mathcal{L}(\theta) = \frac{\delta}{\sqrt{M}} \sum_{j=1}^{M} (\theta'_j - \theta_j) G_j,$$

因此

$$\begin{aligned}\big\|\mathcal{L}(\theta')-\mathcal{L}(\theta)\big\|_{1\to 1} &\le \frac{\delta}{\sqrt{M}}\sum_{j=1}^{M}|\theta'_j-\theta_j|\,\|G_j\|_{1\to 1}\\ &\le \frac{\delta C_G}{\sqrt{M}}\sum_{j=1}^{M}|\theta'_j-\theta_j|\\ &\le \frac{\delta C_G}{\sqrt{M}}\sqrt{M}\,\|\theta'-\theta\|_2\\ &= \delta C_G\,\|\theta'-\theta\|_2,\end{aligned}$$

其中我们使用了柯西–施瓦茨不等式 $\sum_j |a_j| \le \sqrt{M}\|a\|_2$。结合前面的界，我们得到

$$\big\|\Lambda_t^{(\mathcal{L}(\theta'))}-\Lambda_t^{(\mathcal{L}(\theta))}\big\|_{1\to 1} \le t\,\delta C_G\,\|\theta'-\theta\|_2.$$

代入步骤 2 中的估计可得

$$|F_\varphi(\theta')-F_\varphi(\theta)| \le t\,\delta C_G\,\|\theta'-\theta\|_2.$$

设定 $L_0 := t\delta C_G$ 得到（6.3）。由于右侧与 φ无关，该 Lipschitz 常数对所有测试函数一致适用。■

注 20。引理 *17* 给出了抽象假设的第二部分："对于每个测试函数 φ，映射$F_\varphi(\mathcal{L}) := P_{\mathcal{L}}[\varphi]$ 在 L_0上是 - *Lipschitz* 的，其中 L_0 与 φ无关。"

定理 13（列维集中与 frac随机局域林德布拉德系综的上界）。在定义 和引理 的假设下，设参数维数 M 足够大，且球面测度 μ_{sph} 满足标准列维集中不等式：存在常数 $c_{\mathrm{sph}} > 0$，使得对于任意 L_0-*Lipschitz* 函数 $f: S^{M-1} \to \mathbb{R}$ 以及任意 $\tau > 0$,

$$\Pr_{\theta\sim\mu_{\mathrm{sph}}}\big(|f(\theta)-\mathbb{E}f| \ge \tau\big) \le 2\exp\Big(-c_{\mathrm{sph}}\frac{M\tau^2}{L_0^2}\Big). \tag{6.4}$$

对于任意测试函数 φ： $X \to [-1,1]$，设

$$Q[\varphi] := \mathbb{E}_{\mathcal{L}\sim\mu_{\mathcal{L}}}\big[P_{\mathcal{L}}[\varphi]\big] = \mathbb{E}_{\theta\sim\mu_{\mathrm{sph}}}\big[F_\varphi(\theta)\big],$$

并在统计查询框架中定义

$$\mathrm{frac}(\mu_{\mathcal{L}}, Q, \tau) := \sup_{\varphi: X\to[-1,1]} \Pr_{\mathcal{L}\sim\mu_{\mathcal{L}}}\big(|P_{\mathcal{L}}[\varphi]-Q[\varphi]| \ge \tau\big).$$

那么对于任意 $\tau > 0$，我们有指数小的界

$$\mathrm{frac}(\mu_{\mathcal{L}}, Q, \tau) \le 2\exp\Big(-c_{\mathrm{sph}}\frac{M\tau^2}{L_0^2}\Big), \qquad L_0 = t\delta C_G. \tag{6.5}$$

证明。根据引理 17，对于每个固定的测试函数 φ 函数 $F_\varphi(\theta) = P_{\mathcal{L}(\theta)}[\varphi]$ 在 L_0上是 S^{M-1}-Lipschitz 的。应用列维不等式（6.4），我们得到对于任意 $\tau > 0$,

$$\Pr_{\theta\sim\mu_{\mathrm{sph}}}\big(|F_\varphi(\theta)-\mathbb{E}F_\varphi| \ge \tau\big) \le 2\exp\Big(-c_{\mathrm{sph}}\frac{M\tau^2}{L_0^2}\Big).$$

注意到 μ_{sph} 在 $\mathcal{L}(\theta)$ 下的推前测度恰好是 $\mu_{\mathcal{L}}$，且 $\mathbb{E}F_\varphi = Q[\varphi]$，我们得到

$$\Pr_{\mathcal{L}\sim\mu_{\mathcal{L}}}\big(|P_{\mathcal{L}}[\varphi]-Q[\varphi]| \ge \tau\big) \le 2\exp\Big(-c_{\mathrm{sph}}\frac{M\tau^2}{L_0^2}\Big),$$

其中右侧与 φ 无关。随后对 φ 取上确界，得到

$$\mathrm{frac}(\mu_{\mathcal{L}}, Q, \tau) \le 2\exp\Big(-c_{\mathrm{sph}}\frac{M\tau^2}{L_0^2}\Big),$$

这恰好就是（6.5）。 ■

因此，（6.5）为随机局域林德布拉德系综给出了 $\mathrm{frac}(\mu_{\mathcal{L}}, Q, \tau)$ 形式的李乌维尔浓缩，可直接代入一般的 SQ-困难性判据。QPStat 的证明也类似。为避免重复，此处不再赘述。

VII. 远离-Q

在第V 节中，我们针对随机 Lindblad 算子参数球面系综，为 SQ 测试函数 $L_0 = t\delta C_G \quad F_\varphi(\theta) = P_{\mathcal{L}(\theta)}[\varphi]$建立了一致 Lipschitz 常数，并利用球面上的列维引理，得到了 $\mathrm{frac}(\mu_{\mathcal{L}}, Q, \tau)$ 的指数上界（定理 10）。本节将利用测度论框架，进一步推导：

1. 参数球面上 $d_{\mathrm{TV}}(P_{\mathcal{L}}, Q)$ 的集中性（远离-Q）；
2. 对任意固定的 D，一个远离-D 的结果。

A. 关于参数的全变差距离的 Lipschitz 连续性

我们首先将引理 12 提升到全变差距离的层面。为便于计算利普希茨常数，我们给出全变差距离的一个等价变分形式。

引理 18（全变差距离的变分刻画）。设 X 为有限集，且 P、$Q \in \mathcal{D}_X$ 是定义在 X上的两个概率分布。根据定义 *10*，它们的全变差距离为

$$d_{\mathrm{TV}}(P, Q) := \frac{1}{2}\sum_{x\in X}\big|P(x) - Q(x)\big|.$$

则以下等价刻画成立：

$$d_{\mathrm{TV}}(P, Q) = \max_{S\subseteq X}\big|P(S) - Q(S)\big|, \tag{7.1}$$

$$= \frac{1}{2}\sup_{\varphi: X\to[-1,1]}\big|P[\varphi] - Q[\varphi]\big|, \tag{7.2}$$

其中，$P[\varphi] := \sum_{x\in X}\varphi(x)\,P(x)$ 表示在 P 下对 φ 的期望。

证明。定义

$$S_+ := \{x \in X : P(x) \ge Q(x)\}, \qquad S_- := X \setminus S_+.$$

Then

$$\sum_{x\in X}\big|P(x) - Q(x)\big| = \sum_{x\in S_+}\big(P(x) - Q(x)\big) + \sum_{x\in S_-}\big(Q(x) - P(x)\big).$$

另一方面，由于 P 和 Q 都是概率分布，

$$\sum_{x\in X}\big(P(x) - Q(x)\big) = 0,$$

so

$$\sum_{x\in S_+}(P(x)-Q(x)) = -\sum_{x\in S_-}(P(x)-Q(x)).$$

因此

$$\sum_{x\in S_+}\big(P(x)-Q(x)\big) = \sum_{x\in S_-}\big(Q(x)-P(x)\big) = \frac{1}{2}\sum_{x\in X}\big|P(x)-Q(x)\big|.$$

因此

$$d_{\mathrm{TV}}(P,Q) = \frac{1}{2}\sum_{x\in X}\big|P(x)-Q(x)\big| = P(S_+)-Q(S_+).$$

接下来，对任意子集 $S\subseteq X$，将其分解为 $S=(S\cap S_+)\cup(S\cap S_-)$。在 $S\cap S_-$ 上，我们有 $P(x)-Q(x)<0$，因此舍弃这一部分只会使总和增大；然后将 $S\cap S_+$ 扩展到整个 S_+，可以进一步增大总和。因此

$$\begin{aligned} P(S)-Q(S) &= \sum_{x\in S}\big(P(x)-Q(x)\big) \\ &= \sum_{x\in S\cap S_+}\big(P(x)-Q(x)\big) + \sum_{x\in S\cap S_-}\big(P(x)-Q(x)\big) \\ &\le \sum_{x\in S_+}\big(P(x)-Q(x)\big) = d_{\mathrm{TV}}(P,Q), \end{aligned}$$

类似地，$Q(S)-P(S)\le d_{\mathrm{TV}}(P,Q)$。因此，

$$\big|P(S)-Q(S)\big| \le d_{\mathrm{TV}}(P,Q) \quad \text{for all } S\subseteq X.$$

取 $S=S_+$ 可得 最大值$_S\,|P(S)-Q(S)| = d_{\mathrm{TV}}(P,Q)$，这就证明了（7.1）。

现在我们来证明

$$\sup_{\varphi:X\to[-1,1]}\big|P[\varphi]-Q[\varphi]\big| \le 2\,d_{\mathrm{TV}}(P,Q).$$

对任意 $\varphi:\ X\to[-1,1]$,

$$P[\varphi]-Q[\varphi] = \sum_{x\in X}\varphi(x)\big(P(x)-Q(x)\big),$$

so

$$\begin{aligned} \big|P[\varphi]-Q[\varphi]\big| &\le \sum_{x\in X}|\varphi(x)|\,\big|P(x)-Q(x)\big| \\ &\le \sum_{x\in X}\big|P(x)-Q(x)\big| \\ &= 2\,d_{\mathrm{TV}}(P,Q), \end{aligned}$$

其中我们使用了 $|\varphi(x)|\le 1$。对所有 φ 取上确界可得

$$\sup_{\varphi:X\to[-1,1]}\big|P[\varphi]-Q[\varphi]\big| \le 2\,d_{\mathrm{TV}}(P,Q).$$

接下来，我们构造一个达到此界的测试函数。定义

$$\varphi_*(x) := \begin{cases} +1, & P(x)\ge Q(x), \\ -1, & P(x)<Q(x), \end{cases}$$

（当 $P(x)=Q(x)$ 时，我们可以在 $[-1,1]$ 中取任意值，而不影响下面的计算）。于是

$$\begin{aligned} P[\varphi_*]-Q[\varphi_*] &= \sum_{x\in X}\varphi_*(x)\big(P(x)-Q(x)\big) \\ &= \sum_{x\in S_+}(+1)\big(P(x)-Q(x)\big)+\sum_{x\in S_-}(-1)\big(P(x)-Q(x)\big) \\ &= \sum_{x\in S_+}\big(P(x)-Q(x)\big)+\sum_{x\in S_-}\big(Q(x)-P(x)\big) \\ &= \sum_{x\in X}\big|P(x)-Q(x)\big| \\ &= 2\,d_{\mathrm{TV}}(P,Q). \end{aligned}$$

因此

$$\sup_{\varphi:X\to[-1,1]}\big|P[\varphi]-Q[\varphi]\big| \ge \big|P[\varphi_*]-Q[\varphi_*]\big| = 2\,d_{\mathrm{TV}}(P,Q).$$

结合上界和下界，我们得到

$$\sup_{\varphi:X\to[-1,1]}\big|P[\varphi]-Q[\varphi]\big| = 2\,d_{\mathrm{TV}}(P,Q),$$

这等价于

$$d_{\mathrm{TV}}(P,Q)=\frac{1}{2}\sup_{\varphi:X\to[-1,1]}\big|P[\varphi]-Q[\varphi]\big|.$$

这证明了（7.2）。 ■

引理 19（关于参数的全变差距离 Lipschitz 连续性）。在引理 *12*的假设下，对于任意参考分布 $Q\in\mathcal{D}_X$，利用引理 *18*定义：

$$F_{\mathrm{TV}}(\theta):=d_{\mathrm{TV}}(P_{\mathcal{L}(\theta)},Q)=\frac{1}{2}\sup_{\varphi:X\to[-1,1]}\big|P_{\mathcal{L}(\theta)}[\varphi]-Q[\varphi]\big|.$$

那么对于任意 θ、$\theta'\in\Theta$，

$$\big|F_{\mathrm{TV}}(\theta)-F_{\mathrm{TV}}(\theta')\big|\le L_{\mathrm{TV}}\,\|\theta-\theta'\|_2,\qquad L_{\mathrm{TV}}:=\frac{L_0}{2}=\frac{t\delta C_G}{2}.$$

证明。设 $P_\theta:=P_{\mathcal{L}(\theta)}$。根据全变差距离的变分表示，

$$F_{\mathrm{TV}}(\theta)=\frac{1}{2}\sup_{\varphi:X\to[-1,1]}|P_\theta[\varphi]-Q[\varphi]|.$$

Thus

$$\begin{aligned} \big|F_{\mathrm{TV}}(\theta)-F_{\mathrm{TV}}(\theta')\big| &= \frac{1}{2}\Big|\sup_\varphi|P_\theta[\varphi]-Q[\varphi]|-\sup_\varphi|P_{\theta'}[\varphi]-Q[\varphi]|\Big| \\ &\le \frac{1}{2}\sup_\varphi\Big||P_\theta[\varphi]-Q[\varphi]|-|P_{\theta'}[\varphi]-Q[\varphi]|\Big| \\ &\le \frac{1}{2}\sup_\varphi|P_\theta[\varphi]-P_{\theta'}[\varphi]|. \end{aligned}$$

在最后一个不等式中，我们用到了：对于任意实数 x,y,a，$\big||x-a|-|y-a|\big|\le|x-y|$。根据引理 12，对于任意 $\varphi:\ X\to[-1,1]$，

$$|P_\theta[\varphi]-P_{\theta'}[\varphi]|=|F_\varphi(\theta)-F_\varphi(\theta')|\le L_0\,\|\theta-\theta'\|_2.$$

代入前一个不等式可得

$$|F_{\mathrm{TV}}(\theta) - F_{\mathrm{TV}}(\theta')| \le \frac{1}{2} L_0 \, \|\theta - \theta'\|_2,$$

因此 $L_{\mathrm{TV}} = L_0/2$。 ■

B. 均值假设与远离-Q 的集中性

我们现在引入一个非零均值假设。直观而言，这是“Porter-Thomas 均值假设的开放系统版本”。这一假设很自然：在足够深的随机电路下，输出概率分布会趋近于 Porter-Thomas 分布 [BIS+18]，因此许多全局指标（例如交叉熵差异和重输出概率）在高维极限下会收敛到常数 [HE23]。对于 Nietner 的随机酉电路 [NIS+25]，这个常数可以通过高斯积分计算得到：$\mathbb{E} d_{\mathrm{TV}}(P_U,\ U) \approx 1/e$。这一计算依赖于全变差距离仅取决于少数相互独立的高斯变量这一事实。然而，在我们的设定中，指数映射使其对整个参数向量的依赖变成非线性的，因此我们无法再以同样的方式精确计算均值。尽管如此，在线性响应区域内，我们可以给出一个显式公式，具体将在第 VIII节展示；在第 IX节中，我们将给出一个简单但具体的例子，其中该均值取一个简单的常数值，并进行一些数值模拟，为我们的假设提供支持。

假设 1（开放系统波特–托马斯均值假设）。存在常数 $m_0 > 0$ 和一个误差项 $\epsilon_{\mathrm{mean}} > 0$，当系统参数（例如希尔伯特空间维数 d 或参数维数 M）增大时，该误差项趋于0，使得全变差距离

$$F_{\mathrm{TV}}(\theta) = d_{\mathrm{TV}}(P_{\mathcal{L}(\theta)}, Q)$$

在参数球面系综 (Θ, μ_Θ) 上的均值满足

$$m := \mathbb{E}_{\theta\sim\mu_\Theta} F_{\mathrm{TV}}(\theta) \in [m_0 - \epsilon_{\mathrm{mean}},\ m_0 + \epsilon_{\mathrm{mean}}].$$

给定利普希茨常数和均值假设，我们可以在参数球面上应用列维引理（引理 7），得到关于 $d_{\mathrm{TV}}(P_{\mathcal{L}}, Q)$ 的集中性结果。

定理 14（相对于参考分布 Q 的全变差距离集中性）。在定义 *23*的设定下，假设引理 *12* 和 *19* 以及假设 *1* 均成立。那么对于任意 $\xi > 0$,

$$\Pr_{\theta\sim\mu_\Theta}\Big(\big|d_{\mathrm{TV}}(P_{\mathcal{L}(\theta)}, Q) - m_0\big| \ge \xi + \epsilon_{\mathrm{mean}}\Big) \le 2\exp\!\left(-c_{\mathrm{par}}\,\frac{M\,\xi^2}{L_{\mathrm{TV}}^2}\right),$$

w这里 c_{par} 是引理 7中的常数，M 是参数维数，而 $L_{\mathrm{TV}} = t\delta C_G/2$.

证明。根据引理 19，$F_{\mathrm{TV}}(\theta)$ 在 $\Theta \subseteq S^{M-1}$上是 L_{TV}-Lipschitz 的。应用引理 7，可得其在均值 m附近集中 $= \mathbb{E}F_{\mathrm{TV}}$:

$$\Pr_{\theta\sim\mu_\Theta}\big(|F_{\mathrm{TV}}(\theta) - m| \ge s\big) \le 2\exp\!\left(-c_{\mathrm{par}}\,\frac{M\,s^2}{L_{\mathrm{TV}}^2}\right).$$

根据假设1，$|m - m_0| \le \epsilon_{\mathrm{mean}}$，因此

$$|F_{\mathrm{TV}}(\theta) - m_0| \ge \xi + \epsilon_{\mathrm{mean}} \ \Rightarrow\ |F_{\mathrm{TV}}(\theta) - m| \ge \xi.$$

Thus

$$\Pr_\theta\Big(|F_{\mathrm{TV}}(\theta) - m_0| \ge \xi + \epsilon_{\mathrm{mean}}\Big) \le \Pr_\theta\big(|F_{\mathrm{TV}}(\theta) - m| \ge \xi\big) \le 2\exp\!\left(-c_{\mathrm{par}}\,\frac{M\,\xi^2}{L_{\mathrm{TV}}^2}\right).$$

■

推论 2（远离-的典型性）。 在定理14的假设下，取 $\xi = m_0/4$ 并假设系统规模足够大，使得 $\epsilon_{\text{mean}} \le m_0/4$。此外，我们有

$$\Big\{\theta:\ d_{\mathrm{TV}}(P_{\mathcal{L}(\theta)}, Q) \le \frac{m_0}{2}\Big\} \subseteq \Big\{\theta : |F(\theta) - m_0| \ge \frac{m_0}{2}\Big\},$$

因此，概率界给出

$$\Pr_{\theta\sim\mu_\Theta}\Big(d_{\mathrm{TV}}(P_{\mathcal{L}(\theta)}, Q) \le \frac{m_0}{2}\Big) \le 2\exp\Big(-c_{\text{par}}\,\frac{M\,m_0^2}{16 L_{\mathrm{TV}}^2}\Big).$$

换言之，随着参数维数 M 线性增长，对于绝大多数 *Lindblad* 算子，输出分布 $P_{\mathcal{L}}$ 与参考分布 Q 之间的全变差距离至少为一个常数 $m_0/2$ 。

C. 平均情形统计查询复杂度

基于

(a) 参数球面系综上的 Lipschitz 性与列维集中性（定理 10），它给出了 $\max_{\varphi:X\to[-1,1]} \Pr_{\mathcal{L}\sim\mu_{\mathcal{L}}}[|P_{\mathcal{L}}[\varphi] - Q[\varphi]| > \tau]$ (分母) 的指数级小上界；

(b) 开放系统波特–托马斯均值假设及其导出的“远离 Q/远离任意固定的 D”体积估计（定理 14及其推论 2），它们对 β–$\Pr_{\mathcal{L}\sim\mu_{\mathcal{L}}}[d_{\mathrm{TV}}(P_{\mathcal{L}},\ Q) \le \epsilon+\tau]$（分子）提供了控制。

结合统计查询学习与判定框架 [Fel17、NIS+25]（定理 8、9 及相关引理），我们可以在论文开篇就陈述以下平均情形统计查询复杂度结论。

i. 确定性判定问题的平均情形统计查询下界同样呈指数级 al.

设 $\mu_{\mathcal{L}}$ 为由参数球面系综诱导的 Lindblad 算子分布，并将参考分布 Q 定义为系综平均 $Q[\varphi] = \mathbb{E}_{\mathcal{L}\sim\mu_{\mathcal{L}}} P_{\mathcal{L}}[\varphi]$。根据定理 10 以及全变差-Lipschitz连续性，我们已经知道，对于任意 $\tau > 0$,

$$\max_{\varphi:X\to[-1,1]} \Pr_{\mathcal{L}\sim\mu_{\mathcal{L}}}\big[|P_{\mathcal{L}}[\varphi] - Q[\varphi]| > \tau\big] \ =:\ \mathrm{frac}(\mu_{\mathcal{L}}, Q, \tau) \ \le\ 2\exp\Big(-c_{\text{par}}\frac{M\tau^2}{L_0^2}\Big),$$

另一方面，“远离 Q”结果（定理14 及其推论）表明，对于适当的常数$m_0 > 0$ 以及足够大的系统规模,

$$\Pr_{\mathcal{L}\sim\mu_{\mathcal{L}}}\big[d_{\mathrm{TV}}(P_{\mathcal{L}}, Q) \le \epsilon + \tau\big] \ \le\ 2\exp\big(-c'_{\text{par}} M\big).$$

因此，对于任意固定的 $\beta \in (0,\ 1)$，如果我们只要求算法在至少占据$\mu_{\mathcal{L}}$-测度 β 的林德布拉德算子子集上成功，那么“分子”

$$\beta - \Pr_{\mathcal{L}\sim\mu_{\mathcal{L}}}\big[d_{\mathrm{TV}}(P_{\mathcal{L}}, Q) \le \epsilon + \tau\big]$$

对于充分大的 M （例如 $\ge \beta/2$），其仍保持为常数量级。将这两个估计代入平均情形判定下界（定理8的一个特例）后，我们得到：任何试图在一个 $\mu_{\mathcal{L}}$-测度至少为 β的子集上正确判定“$P \in \mathcal{D}$”与“$P = Q$”的确定性 SQ 算法，都必须具有平均情形统计查询复杂度

$$q + 1 \ \gtrsim\ \frac{\beta}{4}\exp\Big(c_{\text{par}}\frac{M\tau^2}{L_0^2}\Big) \ =\ \exp\Big(\Omega(M)\Big).$$

也就是说，该判定问题的平均情形 SQ 查询复杂度仍随参数维数 M 呈指数增长。

ii. 随机化判定问题的平均情形 SQ 下界带有一个 $(\alpha,\ \beta)$ 因子，但仍然是指数级的。

对于随机化（包括经典概率或量子）判定算法，定理 9 指出：如果该算法凭借内部随机性，以至少 $\alpha > 1/2$ 的概率成功，并正确判定$\mathcal{D}$ 与 Q，且其作用于一组 Lindblad 算子，该子集的 $\mu_{\mathcal{L}}$-测度至少为 β，那么

$$q+1 \ \geq\ 2\cdot \frac{\left(\alpha-\frac{1}{2}\right)\cdot\left(\beta-\Pr_{\mathcal{L}\sim\mu_{\mathcal{L}}}[d_{\mathrm{TV}}(P_{\mathcal{L}},Q)\leq\epsilon+\tau]\right)}{\max\limits_{\varphi:X\to[-1,1]}\Pr\limits_{\mathcal{L}\sim\mu_{\mathcal{L}}}[|P_{\mathcal{L}}[\varphi]-Q[\varphi]|>\tau]}.$$

再次代入上述“分子”和“分母”的估计，对于充分大的 M，我们得到

$$q+1 \ \gtrsim\ \left(\alpha-\tfrac{1}{2}\right)\beta\,\exp\!\left(c_{\mathrm{par}}\frac{M\tau^2}{L_0^2}\right).$$

因此，只要我们在平均意义下要求固定的常数成功概率 $\alpha > 1/2$ 和固定的常数覆盖率$\beta > 0$，随机化判定算法的平均情形 SQ 查询复杂度同样关于 M呈指数增长，并带有额外的自然线性前因子（$\alpha-\frac{1}{2}$）β。

iii. 随机林德布拉德微观结构的平均情形 SQ 学习复杂度：学习不比判定容易。

此外，利用一般性的“学习不比判定容易”归约（定理8 本身及其随机化变体 9），我们可以直接得到开放系统 SQ 学习问题的平均情形指数下界。考虑如下 SQ 学习任务：给定对未知 $\mathcal{L}\ \sim\mu_{\mathcal{L}}$ 的 SQ 预言机访问权限（通过固定时间 t、固定输入态 ρ_{in} 和有限 POVM 接口），要求我们输出一个分布 $\widehat{\ }\qquad\qquad\sim P$，使得 $d_{\mathrm{TV}}(P,\ P_{\mathcal{L}})\ <\epsilon$。

1. 确定性平均情形学习算法：假设某个确定性算法使用至多q 个 τ-精确统计查询，并在 ϵ-学习一个由林德布拉德算子构成的子族时成功，该子族的$\mu_{\mathcal{L}}$-测度至少为 β。那么定理 8 表明

$$q+1 \ \geq\ \frac{\beta-\Pr_{\mathcal{L}\sim\mu_{\mathcal{L}}}\left[d_{\mathrm{TV}}(P_{\mathcal{L}},Q)\leq\epsilon+\tau\right]}{\max\limits_{\varphi:X\to[-1,1]}\Pr\limits_{\mathcal{L}\sim\mu_{\mathcal{L}}}[|P_{\mathcal{L}}[\varphi]-Q[\varphi]|>\tau]}.$$

代入估计值“分子 $\sim\beta$”和“分母 $\sim\exp(-cM)$”，对于充分大的 M，得到

$$q+1 \ \gtrsim\ \beta\,\exp\!\left(c_{\mathrm{par}}\frac{M\tau^2}{L_0^2}\right),\qquad q_{\mathrm{det}}^{\text{avg-learn}}(\epsilon,\tau;\beta)\ =\ \exp\big(\Omega(M)\big).$$

换言之，对完整的开放系统动力学族进行确定性 SQ 学习，仍然需要指数数量的统计查询。

2. 随机化（经典或量子）平均情形学习算法：若某个具有内部随机性的算法以至少 $\alpha > 1/2$ 的概率成功，并完成 ϵ-学习一个由林德布拉德算子构成的子族，该子族的 $\mu_{\mathcal{L}}$-测度至少为 β，那么根据定理 9，

$$q+1 \ \geq\ 2\cdot \frac{\left(\alpha-\frac{1}{2}\right)\cdot\left(\beta-\Pr_{\mathcal{L}\sim\mu_{\mathcal{L}}}[d_{\mathrm{TV}}(P_{\mathcal{L}},Q)\leq\epsilon+\tau]\right)}{\max\limits_{\varphi:X\to[-1,1]}\Pr\limits_{\mathcal{L}\sim\mu_{\mathcal{L}}}[|P_{\mathcal{L}}[\varphi]-Q[\varphi]|>\tau]}.$$

代入我们对“分子”和“分母”的估计，并令 M 足够大，我们得到

$$q+1 \ \gtrsim\ \left(\alpha-\tfrac{1}{2}\right)\beta\,\exp\!\left(c_{\mathrm{par}}\frac{M\tau^2}{L_0^2}\right),\qquad q_{\mathrm{rand}}^{\text{avg-learn}}(\epsilon,\tau;\alpha,\beta)\ =\ \exp\big(\Omega(M)\big).$$

这表明，随机性（包括量子算法的内部随机性）无法显著降低开放系统动力学学习的平均情形 SQ 查询复杂度。

我们可以得出结论：只要随机参数化的 Lindblad 算子族在高维参数球面上满足 Lipschitz 条件和列维集中性，并且其与参考分布 Q 的全变差距离具有类似Porter-Thomas的非零均值性质，那么在统计查询模型中，无论是判定问题还是学习问题，无论是确定性方法还是随机化方法，平均情形下的统计查询复杂度都会随参数维数 M 指数增长。

D. 从远离-Q 到远离任意-D

我们还有一个有趣的推论：可以从远离-Q 的结果推导出“远离任意-D”的开放系统版本，从而控制相对于任意固定分布 D 的全变差距离。

引理 20 (远离-Q $\Rightarrow$ 远离-D)。 假设 Q， $D \in \mathcal{D}_X$ 满足 $d_{\mathrm{TV}}(Q,\ D) > \epsilon + \tau$ 对于某些 ϵ， $\tau > 0$。令 $\mu_{\mathcal{L}}$ 为上述随机 *Lindblad* 算子系综。对于每个 φ : $X \to [-1,1]$，定义 $P_{\mathcal{L}}[\varphi]$ 和 $Q[\varphi]$ ，如定理*10*中所述，并令

$$\mathrm{frac}(\mu_{\mathcal{L}}, Q, \tau) := \sup_{\varphi: X\to[-1,1]} \Pr_{\mathcal{L}\sim\mu_{\mathcal{L}}} \big(|P_{\mathcal{L}}[\varphi] - Q[\varphi]| \geq \tau\big).$$

Then

$$\Pr_{\mathcal{L}\sim\mu_{\mathcal{L}}} \big[d_{\mathrm{TV}}(P_{\mathcal{L}}, D) < \epsilon\big] \leq \mathrm{frac}(\mu_{\mathcal{L}}, Q, \tau).$$

证明。 根据全变差距离的变分表示，存在一个可测子集 $S \subseteq X$ 使得

$$d_{\mathrm{TV}}(Q, D) = |Q(S) - D(S)|,$$

并令 $\varphi := \mathbf{1}_S$: $X \to \{0,1\}$。则 $d_{\mathrm{TV}}(Q, D) = |D[\varphi] - Q[\varphi]|$。对于满足 $d_{\mathrm{TV}}(P_{\mathcal{L}}, D) < \epsilon$ 的任意 $\mathcal{L}$，我们有

$$|P_{\mathcal{L}}[\varphi] - D[\varphi]| \leq d_{\mathrm{TV}}(P_{\mathcal{L}}, D) < \epsilon.$$

因此

$$\begin{aligned} \big|P_{\mathcal{L}}[\varphi] - Q[\varphi]\big| &\geq |D[\varphi] - Q[\varphi]| - |P_{\mathcal{L}}[\varphi] - D[\varphi]| \\ &> d_{\mathrm{TV}}(Q, D) - \epsilon \\ &> (\epsilon + \tau) - \epsilon = \tau. \end{aligned}$$

所以

$$\big\{d_{\mathrm{TV}}(P_{\mathcal{L}}, D) < \epsilon\big\} \subseteq \big\{|P_{\mathcal{L}}[\varphi] - Q[\varphi]| > \tau\big\} \subseteq \big\{|P_{\mathcal{L}}[\varphi] - Q[\varphi]| \geq \tau\big\},$$

并在 $\mu_{\mathcal{L}}$ 下取概率，利用 frac 的定义即可得到该结论。 ■

引理 21(反证 olling the “heaviest ϵ-球”)。 在引理 *20*的设定下，对于任意 ϵ， $\tau > 0$ 以及任意 $D \in \mathcal{D}_X$，

$$\Pr_{\mathcal{L}\sim\mu_{\mathcal{L}}} \big[d_{\mathrm{TV}}(P_{\mathcal{L}}, D) < \epsilon\big] \leq \max\Big\{\mathrm{frac}(\mu_{\mathcal{L}}, Q, \tau),\ \Pr_{\mathcal{L}\sim\mu_{\mathcal{L}}} \big[d_{\mathrm{TV}}(P_{\mathcal{L}}, Q) \leq 2\epsilon + \tau\big]\Big\}.$$

证明。 我们根据 $d_{\mathrm{TV}}(D,\ Q)$ 分两种情况讨论。

情况 *1*： 若 $d_{\mathrm{TV}}(D, Q) > \epsilon + \tau$，则由引理 20，

$$\Pr_{\mathcal{L}\sim\mu_{\mathcal{L}}} \big[d_{\mathrm{TV}}(P_{\mathcal{L}}, D) < \epsilon\big] \leq \mathrm{frac}(\mu_{\mathcal{L}}, Q, \tau).$$

情形 2： 若 $d_{\mathrm{TV}}(D,Q) \le \epsilon+\tau$，则对于任意满足 $d_{\mathrm{TV}}(P_{\mathcal{L}},D) < \epsilon$ 的$\mathcal{L}$，由三角不等式可得

$$d_{\mathrm{TV}}(P_{\mathcal{L}},Q) \le d_{\mathrm{TV}}(P_{\mathcal{L}},D) + d_{\mathrm{TV}}(D,Q) < \epsilon + (\epsilon+\tau) = 2\epsilon+\tau,$$

因此

$$\big\{d_{\mathrm{TV}}(P_{\mathcal{L}},D) < \epsilon\big\} \subseteq \big\{d_{\mathrm{TV}}(P_{\mathcal{L}},Q) \le 2\epsilon+\tau\big\},$$

取概率可得

$$\Pr_{\mathcal{L}\sim\mu_{\mathcal{L}}}\big[d_{\mathrm{TV}}(P_{\mathcal{L}},D) < \epsilon\big] \le \Pr_{\mathcal{L}\sim\mu_{\mathcal{L}}}\big[d_{\mathrm{TV}}(P_{\mathcal{L}},Q) \le 2\epsilon+\tau\big].$$

结合这两种情况，即得到所需的上界。 ■

结合定理 10（它给出了关于 $\mathrm{frac}(\mu_{\mathcal{L}},Q,\tau)$ 的指数上界）与推论 2（它以高概率给出了关于 $d_{\mathrm{TV}}(P_{\mathcal{L}},Q)$ 保持在某个常数阈值之上的下界），我们得到以下“远离任意 D”结果：

定理 15（随机林德布拉德算子系综关于任意固定分布 D 的远离 D）。 在定理 *10* 和 *14*（以及推论 *2*）的假设下，存在常数 $\epsilon_* > 0$ 和 $c_* > 0$，使得对于充分大的参数维数 M 以及任意 $D \in \mathcal{D}_X$，

$$\Pr_{\mathcal{L}\sim\mu_{\mathcal{L}}}\big[d_{\mathrm{TV}}(P_{\mathcal{L}},D) \ge \epsilon_*\big] \;\ge\; 1 - 2\exp(-c_* M).$$

换言之，对于随机 *Lindblad* 算子参数球面系综，几乎所有 *Lindblad* 算子的输出分布 $P_{\mathcal{L}}$ 与任意固定的经典分布 D之间的全变差距离至少为一个常数 ϵ_*，且坏集合的测度随参数维数 M呈指数衰减。

证明。 我们从现有的两个指数级小上界出发，并将它们代入引理 21。首先，根据定理 10，对于任意固定的 $\tau > 0$,

$$\mathrm{frac}(\mu_{\mathcal{L}},Q,\tau) := \sup_{\varphi:X\to[-1,1]} \Pr_{\mathcal{L}\sim\mu_{\mathcal{L}}}\big(|P_{\mathcal{L}}[\varphi] - Q[\varphi]| \ge \tau\big) \le 2\exp\!\left(-c_{\mathrm{par}}\,\frac{M\,\tau^2}{L_0^2}\right),$$

其中 $L_0 = t\delta C_G$ 是引理 12中的一致 Lipschitz 常数。

其次，根据定理 14 和开放系统波特–托马斯均值假设，存在常数 $m_0 > 0$和 $\epsilon_{\mathrm{mean}} \to 0$，使得对于满足 $\epsilon_{\mathrm{mean}} \le m_0/4$ 的充分大的系统规模，推论 2 给出

$$\Pr_{\mathcal{L}\sim\mu_{\mathcal{L}}}\big[d_{\mathrm{TV}}(P_{\mathcal{L}},Q) \le m_0/2\big] \le 2\exp\!\left(-c_{\mathrm{par}}\,\frac{M\,m_0^2}{4L_0^2}\right),$$

这里我们用到了 $L_{\mathrm{TV}} = L_0/2$。

现在固定具体常数

$$\epsilon_* := \frac{m_0}{8}, \qquad \tau := \frac{m_0}{8},$$

使得 $2\epsilon_* + \tau = \frac{3m_0}{8} < \frac{m_0}{2}$，由概率上界的单调性可得

$$\Pr_{\mathcal{L}\sim\mu_{\mathcal{L}}}\big[d_{\mathrm{TV}}(P_{\mathcal{L}},Q) \le 2\epsilon_*+\tau\big] \le \Pr_{\mathcal{L}\sim\mu_{\mathcal{L}}}\big[d_{\mathrm{TV}}(P_{\mathcal{L}},Q) \le m_0/2\big] \le 2\exp(-c_2 M),$$

其中 $c_2 := c_{\mathrm{par}}\,m_0^2/(4L_0^2)$。另一方面，对于 $\tau = m_0/8$,

$$\mathrm{frac}(\mu_{\mathcal{L}},Q,\tau) \le 2\exp(-c_1 M), \qquad c_1 := c_{\mathrm{par}}\,\frac{m_0^2}{64L_0^2}.$$

将这两个界代入引理 21，我们对任意 $D \in \mathcal{D}_X$，

$$\Pr_{\mathcal{L}\sim\mu_{\mathcal{L}}}\left[d_{\mathrm{TV}}(P_{\mathcal{L}}, D) < \epsilon_*\right] \le \max\left\{2e^{-c_1 M},\ 2e^{-c_2 M}\right\} = 2e^{-c_* M},$$

其中 $c_* := \min\{c_1,\ c_2\} > 0$。取补集可得

$$\Pr_{\mathcal{L}\sim\mu_{\mathcal{L}}}\left[d_{\mathrm{TV}}(P_{\mathcal{L}}, D) \ge \epsilon_*\right] \ge 1 - 2e^{-c_* M},$$

这对任意固定的 $D \in \mathcal{D}_X$ 都成立，从而证明了该定理。 ■

VIII. 随机林德布拉德系综中平均全变差距离的线性响应标度

在本节中，对于前文介绍的具体随机局域林德布拉德系综 $\{\mathcal{L}(\boldsymbol{\theta})\}_{\theta\in S^{M-1}}$，我们推导平均值的显式渐近标度

$$F_{\mathrm{TV}}(\theta) := d_{\mathrm{TV}}\big(P_{\mathcal{L}(\theta)}, Q\big), \qquad m(\delta) := \mathbb{E}_{\theta\sim\mu_{\mathrm{sph}}} F_{\mathrm{TV}}(\theta),$$

在线性响应（小扰动 $\delta \to 0$）范围内。这里 $\delta > 0$ 是随机林德布拉德参数化中的扰动幅度。本分析的技术灵感源自久保线性响应理论 [久保57]；更详细的讨论请参见备注 22 。

我们关注全变差距离

$$F_{\mathrm{TV}}(\theta) := d_{\mathrm{TV}}\big(P_{\mathcal{L}(\theta)}, Q\big) = \frac{1}{2}\sum_{x\in X}\big|P_{\mathcal{L}(\theta)}(x) - Q(x)\big|.$$

我们分三步进行：首先，根据扰动公式推导线性响应展开；然后分析球面上线性泛函的绝对值期望；最后将二者结合，得到 $m(\delta)$ 的线性响应标度。

A. 根据扰动公式进行线性响应展开

引理 22（扰动公式和一阶响应系数）。 在定义 *1*的设定下，定义

$$K(\theta) := \frac{1}{\sqrt{M}}\sum_{j=1}^{M}\theta_j G_j, \qquad \mathcal{L}(\theta) = \mathcal{L}_{\mathrm{ref}} + \delta K(\theta).$$

那么存在 一个常数 $C_{\mathrm{rem}}(t, C_G)$，与 θ 和 M 无关，使得对每个 $x \in X$，都有如下展开 *on*

$$\Delta p_x(\theta) := P_{\mathcal{L}(\theta)}(x) - Q(x) = \frac{\delta}{\sqrt{M}}\sum_{j=1}^{M}\theta_j a_{j,x} + R_x(\theta,\delta), \tag{8.1}$$

其中

$$a_{j,x} := \mathrm{Tr}\left(M_x \int_0^t \Lambda_{t-s}^{(\mathrm{ref})} \circ G_j \circ \Lambda_s^{(\mathrm{ref})}(\rho_{\mathrm{in}})\,\mathrm{d}s\right), \tag{8.2}$$

且余项满足一致有界条件

$$\sup_{\theta\in S^{M-1}} |R_x(\theta,\delta)| \le C_{\mathrm{rem}}(t, C_G)\,\delta^2. \tag{8.3}$$

证明。令

$$\Lambda_t^{(\theta)} = e^{t(\mathcal{L}_{\mathrm{ref}} + \delta K(\theta))},$$

并在 δ 中进行微扰展开。定义插值生成元

$$\mathcal{L}_\alpha := \mathcal{L}_{\mathrm{ref}} + \alpha\delta K(\theta),$$

及相应的量子马尔可夫半群

$$\Lambda_t^{(\alpha)} := e^{t\mathcal{L}_\alpha}.$$

标准微扰公式给出

$$\Lambda_t^{(\theta)} - \Lambda_t^{(\mathrm{ref})} = \int_0^1 \frac{\mathrm{d}}{\mathrm{d}\alpha}\Lambda_t^{(\alpha)}\,\mathrm{d}\alpha,$$

with

$$\frac{\mathrm{d}}{\mathrm{d}\alpha}\Lambda_t^{(\alpha)} = \int_0^t \Lambda_{t-s}^{(\alpha)} \circ (\delta K(\theta)) \circ \Lambda_s^{(\alpha)}\,\mathrm{d}s.$$

将 $\Lambda_t^{(\alpha)}$ 本身关于 δ 再展开一次，可得到标准二阶公式

$$\Lambda_t^{(\theta)} = \Lambda_t^{(\mathrm{ref})} + \delta\int_0^t \Lambda_{t-s}^{(\mathrm{ref})} \circ K(\theta) \circ \Lambda_s^{(\mathrm{ref})}\,\mathrm{d}s + \delta^2 R_t(\theta,\delta), \tag{8.4}$$

其中余项 $R_t(\theta,\delta)$ 可以写成二重积分

$$R_t(\theta,\delta) = \int_0^t\int_0^s \Lambda_{t-s}^{(\mathrm{ref})} \circ K(\theta) \circ \Lambda_{s-r}^{(\alpha_{s,r})} \circ K(\theta) \circ \Lambda_r^{(\mathrm{ref})}\,\mathrm{d}r\,\mathrm{d}s,$$

其中的某个插值参数为 $\alpha_{s,r} \in [0,1]$。

取 $1\to1$ 范数可得

$$\begin{aligned}\|R_t(\theta,\delta)\|_{1\to1} &\le \int_0^t\int_0^s \big\|\Lambda_{t-s}^{(\mathrm{ref})}\big\|_{1\to1} \big\|K(\theta)\big\|_{1\to1} \big\|\Lambda_{s-r}^{(\alpha_{s,r})}\big\|_{1\to1} \big\|K(\theta)\big\|_{1\to1} \big\|\Lambda_r^{(\mathrm{ref})}\big\|_{1\to1}\,\mathrm{d}r\,\mathrm{d}s \\ &\le \|K(\theta)\|_{1\to1}^2 \int_0^t\int_0^s \mathrm{d}r\,\mathrm{d}s,\end{aligned}$$

这里我们利用了所有 $\Lambda_\cdot^{(\cdot)}$都是完全正迹保持的，因此 $\|\Lambda_\cdot^{(\cdot)}\|_{1\to1} \le 1$。另一方面，由式（2.1）以及 $K(\theta) = \frac{1}{\sqrt{M}}\sum_j \theta_j G_j$ 可得

$$\begin{aligned}\|K(\theta)\|_{1\to1} &\le \frac{1}{\sqrt{M}}\sum_{j=1}^M |\theta_j|\,\|G_j\|_{1\to1} \\ &\le \frac{C_G}{\sqrt{M}}\sum_{j=1}^M |\theta_j| \\ &\le \frac{C_G}{\sqrt{M}}\sqrt{M}\,\|\theta\|_2 \\ &= C_G,\end{aligned}$$

其中我们利用了 $\|G_j\|_{1\to1} \le C_G$ 以及 $\|\theta\|_1 \le \sqrt{M}\overline{\|\theta\|}_2 = \sqrt{M}$，$\overline{\ }$对于 $\theta \in S^{M-1}$。因此

$$\|R_t(\theta,\delta)\|_{1\to1} \le C_G^2\int_0^t\int_0^s \mathrm{d}r\,\mathrm{d}s = \frac{C_G^2 t^2}{2} =: C_{\mathrm{rem}}(t, C_G),$$

其在 θ 和 M 中是一致的。

将（8.4）应用于 ρ_{in}，然后用 M_x 取迹，可得

$$\begin{aligned}\Delta p_x(\theta) &= P_{\mathcal{L}(\theta)}(x) - Q(x)\\ &= \delta\ \mathrm{Tr}\Big(M_x \int_0^t \Lambda_{t-s}^{(\mathrm{ref})} \circ K(\theta) \circ \Lambda_s^{(\mathrm{ref})}(\rho_{\mathrm{in}})\,\mathrm{d}s\Big) + \delta^2\,\mathrm{Tr}\big(M_x R_t(\theta,\delta)(\rho_{\mathrm{in}})\big).\end{aligned}$$

利用 $|\text{迹}(AB)| \le \|A\|_\infty \|B\|_1$ 和 $\|M_x\|_\infty \le 1$，我们得到

$$\begin{aligned}\big|\mathrm{Tr}\big(M_x R_t(\theta,\delta)(\rho_{\mathrm{in}})\big)\big| &\le \|M_x\|_\infty \big\|R_t(\theta,\delta)(\rho_{\mathrm{in}})\big\|_1\\ &\le \|R_t(\theta,\delta)\|_{1\to 1}\\ &\le C_{\mathrm{rem}}(t, C_G).\end{aligned}$$

将 $K(\theta)$ 展开为 $K(\theta) = \frac{1}{\sqrt{M}}\sum_{j=1}^M \theta_j G_j$，我们得到 (8.1)–(8.3)。 ■

注释 21 (一阶响应系数的物理意义$a_{j,\,x}$)。 系数 $a_{j,\,x}$ 刻画了沿第 j 个局部耗散方向 G_j 的线性响应：将 G_j 插入参考动力学 $\Lambda_t^{(\mathrm{ref})}$ 中，对该响应在时间窗口 $[0,t]$ 上积分，然后读取 *POVM* 结果 x，即可得到该系数。所有成对的 (j,x) 对应的 $a_{j,\,x}$ 共同刻画了随机扰动对测量统计数据的一阶影响。

注释 22 (与 Kubo线性响应的关系)。 值得注意的是，此处使用的微扰展开在结构上类似于久保线性响应理论。在哈密顿量封闭系统情形中，外场$f_j(t)$ 与算子 B_j耦合，而某个可观测量 A 的响应写作 *[Kam23]*

$$\delta\langle A(t)\rangle = \sum_j \int_{-\infty}^t \chi_{A,B_j}(t-s)\, f_j(s)\,\mathrm{d}s,$$

其中 $\chi_{A,\,B_j}$ 用未扰动动力学下 A 和 B_j 的时间关联函数表示。在我们的开放系统框架中， $\delta\theta_j$ 起静态外场的作用， G_j 起耦合信道的作用，而 $a_{j,\,x}$ 是测量概率 $P_{\mathcal{L}}(x)$ 关于信道 j的响应核。区别如下：

1. 动力学由 *GKSL*量子马尔可夫半群 $\Lambda_t = e^{t\mathcal{L}}$ 支配，而非幺正流；

2. 我们关注的可观测量是整个输出分布 $P_{\mathcal{L}}$，并以其与参考分布 Q之间的全变差距离衡量，即一种非线性可区分性泛函。在定理 *16* 中，我们进一步对 θ 中的高维参数球面取平均，得到平均总变差距离的线性响应标度$m(\delta)$。

从这一角度看，本节的线性响应分析可视为将久保理论推广至 *GKSL*开放系统框架，并采用专为可学习性设计的非标准可观测量。

B. 球面上线性形式的绝对值期望

现在我们给出一个纯几何引理，用于描述高维球面上 $|\langle\theta, b\rangle|$ 的期望。

引理 23 （球面上一维投影的绝对值期望）。 设 $M \ge 2$，令 $\theta \sim \mu_{\mathrm{sph}}$为 $S^{M-1} \subset \mathbb{R}^M$上的均匀随机向量，并令 $b \in \mathbb{R}^M$ 为任意非零向量。则

$$\mathbb{E}_{\theta\sim\mu_{\mathrm{sph}}}\big|\langle\theta,b\rangle\big| = \|b\|_2\, \frac{\Gamma\big(\frac{M}{2}\big)}{\sqrt{\pi}\,\Gamma\big(\frac{M+1}{2}\big)}. \tag{8.5}$$

特别是在高维极限下 $M \to \infty$,

$$\mathbb{E}_{\theta\sim\mu_{\mathrm{sph}}}\big|\langle\theta,b\rangle\big| = \|b\|_2 \sqrt{\frac{2}{\pi M}}\,(1+o(1)). \tag{8.6}$$

证明。 根据球对称性，我们可以假设 b 与第一坐标方向对齐，即 $b = \|b\|_2\, e_1$，其中 $e_1 = (1,\ 0,\ \ldots\ldots,\ 0)$。于是 $\langle \theta,\ b\rangle = \|b\|_2\, \theta_1$，因此

$$\mathbb{E}_{\theta\sim\mu_{\mathrm{sph}}}\big|\langle \theta, b\rangle\big| = \|b\|_2\, \mathbb{E}_{\theta\sim\mu_{\mathrm{sph}}}|\theta_1|.$$

因此，只需确定 θ_1 的分布及其绝对值期望。

若 θ 在 S^{M-1}上一致分布，则 θ_1 在 $[-1,1]$ 上的密度为（Beta型密度）

$$f_M(u) = c_M (1-u^2)^{\frac{M-3}{2}}, \qquad u \in [-1,1],$$

其中归一化常数 c_M 为

$$\begin{aligned} c_M^{-1} &= \int_{-1}^{1} (1-u^2)^{\frac{M-3}{2}}\, \mathrm{d}u \\ &= 2\int_{0}^{1} (1-u^2)^{\frac{M-3}{2}}\, \mathrm{d}u. \end{aligned}$$

令 $v = u^2$ ，得到

$$\begin{aligned} c_M^{-1} &= 2\int_{0}^{1} (1-u^2)^{\frac{M-3}{2}}\, \mathrm{d}u \\ &= 2\int_{0}^{1} (1-v)^{\frac{M-3}{2}} \frac{\mathrm{d}v}{2\sqrt{v}} \\ &= \int_{0}^{1} v^{-1/2}(1-v)^{\frac{M-3}{2}}\, \mathrm{d}v \\ &= \mathrm{B}\Big(\tfrac{1}{2}, \tfrac{M-1}{2}\Big), \end{aligned}$$

其中 B 为 Beta函数。利用 $\mathrm{B}(x,y) = \frac{\Gamma(x)\Gamma(y)}{\Gamma(x+y)}$，我们得到

$$c_M = \frac{\Gamma\big(\frac{M}{2}\big)}{\sqrt{\pi}\,\Gamma\big(\frac{M-1}{2}\big)}.$$

现在计算

$$\mathbb{E}_{\theta\sim\mu_{\mathrm{sph}}}|\theta_1| = 2c_M \int_{0}^{1} u(1-u^2)^{\frac{M-3}{2}}\, \mathrm{d}u.$$

再次令 $v = u^2$，$\mathrm{d}v = 2u\mathrm{d}u$，得到

$$\begin{aligned} \mathbb{E}_{\theta\sim\mu_{\mathrm{sph}}}|\theta_1| &= 2c_M \int_{0}^{1} u(1-u^2)^{\frac{M-3}{2}}\, \mathrm{d}u \\ &= c_M \int_{0}^{1} (1-v)^{\frac{M-3}{2}}\, \mathrm{d}v \\ &= c_M\, \mathrm{B}\Big(1, \tfrac{M-1}{2}\Big). \end{aligned}$$

由于

$$\mathrm{B}\Big(1, \tfrac{M-1}{2}\Big) = \frac{\Gamma(1)\Gamma\big(\frac{M-1}{2}\big)}{\Gamma\big(\frac{M+1}{2}\big)} = \frac{\Gamma\big(\frac{M-1}{2}\big)}{\Gamma\big(\frac{M+1}{2}\big)},$$

我们发现

$$\begin{aligned}\mathbb{E}_{\theta\sim\mu_{\mathrm{sph}}}|\theta_1| &= c_M\,\frac{\Gamma\!\left(\frac{M-1}{2}\right)}{\Gamma\!\left(\frac{M+1}{2}\right)}\\ &= \frac{\Gamma\!\left(\frac{M}{2}\right)}{\sqrt{\pi}\,\Gamma\!\left(\frac{M+1}{2}\right)}.\end{aligned}$$

这就得到（8.5）。

对于渐近式（8.6），应用 Gamma函数的斯特林公式，

$$\frac{\Gamma(z+\frac{1}{2})}{\Gamma(z)} \sim z^{1/2} \quad (z\to\infty),$$

这意味着

$$\frac{\Gamma\!\left(\frac{M}{2}\right)}{\Gamma\!\left(\frac{M+1}{2}\right)} \sim \left(\frac{M}{2}\right)^{-1/2},$$

因此

$$\mathbb{E}_{\theta\sim\mu_{\mathrm{sph}}}|\theta_1| = \frac{1}{\sqrt{\pi}}\frac{\Gamma\!\left(\frac{M}{2}\right)}{\Gamma\!\left(\frac{M+1}{2}\right)} \sim \frac{1}{\sqrt{\pi}}\left(\frac{2}{M}\right)^{1/2} = \sqrt{\frac{2}{\pi M}}.$$

代入 $\mathbb{E}_{\theta\sim\mu_{\mathrm{sph}}}|\langle\theta,b\rangle|$ 可得（8.6）。 ■

注 23（与高斯近似的关系）。 当 M 较大时， θ 的坐标可以看作是受 $\sum_j \theta_j^2 = 1$约束的“近似独立高斯变量”；引理 *23* 可以视为对这一直觉的精确表述。在高维极限下，$\langle\theta,b\rangle$ 的分布趋近于方差为 $1/M$的高斯变量的分布，因此 $\mathbb{E}|\langle\theta,b\rangle| \approx \|b\|_2\sqrt{2/(\pi M)}$。

为方便后续讨论，定义

$$\kappa_M := \sqrt{M}\,\frac{\Gamma\!\left(\frac{M}{2}\right)}{\sqrt{\pi}\,\Gamma\!\left(\frac{M+1}{2}\right)}, \tag{8.7}$$

从而引理 23 等价于

$$\mathbb{E}_{\theta\sim\mu_{\mathrm{sph}}}\big|\langle\theta,b\rangle\big| = \frac{\kappa_M}{\sqrt{M}}\,\|b\|_2, \qquad \kappa_M \to \sqrt{\frac{2}{\pi}} \quad (M\to\infty). \tag{8.8}$$

C. 平均总变差距离的线性响应标度

现在我们结合上述两个要素，推导出 $m(\delta)$ 的线性响应表达式。

定理 16（线性响应区域中平均总变差距离的渐近标度）。 在定义 *1*和引理 *22*的设定下，定义

$$F_{\mathrm{TV}}(\theta) := d_{\mathrm{TV}}\big(P_{\mathcal{L}(\theta)}, Q\big) = \frac{1}{2}\sum_{x\in X}\big|P_{\mathcal{L}(\theta)}(x) - Q(x)\big|, \quad m(\delta) := \mathbb{E}_{\theta\sim\mu_{\mathrm{sph}}}F_{\mathrm{TV}}(\theta).$$

引入一阶响应向量

$$a^{(x)} := (a_{1,x},\dots,a_{M,x}) \in \mathbb{R}^M, \qquad \|a^{(x)}\|_2 := \Big(\sum_{j=1}^{M} a_{j,x}^2\Big)^{1/2},$$

其中$a_{j,\,x}$ 定义于（8.2）。那么在线性响应区域 $\delta\to 0$中，我们有

$$m(\delta) = \delta\, m_0(M) + \mathcal{O}(\delta^2), \tag{8.9}$$

其中

$$m_0(M) := \frac{\kappa_M}{2M} \sum_{x \in X} \|a^{(x)}\|_2, \tag{8.10}$$

其中 κ_M 定义于 (8.7)。特别是，在高维极限 $M \to \infty$，

$$m(\delta) = \delta \, \frac{1}{2M} \sqrt{\frac{2}{\pi}} \sum_{x \in X} \|a^{(x)}\|_2 + \mathcal{O}(\delta^2) + o(\delta), \tag{8.11}$$

其中，$o(\delta)$ 项来自 $\kappa_M \to \sqrt{2/\pi}$ 中的渐近误差。

证明。 根据引理 22，

$$\Delta p_x(\theta) = \frac{\delta}{\sqrt{M}} \sum_{j=1}^{M} \theta_j a_{j,x} + R_x(\theta, \delta) = \frac{\delta}{\sqrt{M}} \, \langle \theta, a^{(x)} \rangle + R_x(\theta, \delta),$$

其中 $\sup_\theta |R_x(\theta, \delta)| \le C_{\mathrm{rem}} \delta^2$。因此

$$\big|\Delta p_x(\theta)\big| \le \frac{\delta}{\sqrt{M}} \big|\langle \theta, a^{(x)} \rangle\big| + |R_x(\theta, \delta)|.$$

根据三角不等式，

$$\Big| \, \big|\Delta p_x(\theta)\big| - \frac{\delta}{\sqrt{M}} \big|\langle \theta, a^{(x)} \rangle\big| \, \Big| \le |R_x(\theta, \delta)| \le C_{\mathrm{rem}} \delta^2.$$

对 θ 取期望并应用引理 23 可得

$$\begin{aligned} \mathbb{E}_\theta \big|\Delta p_x(\theta)\big| &= \frac{\delta}{\sqrt{M}} \, \mathbb{E}_\theta \big|\langle \theta, a^{(x)} \rangle\big| + \mathcal{O}(\delta^2) \\ &= \frac{\delta}{\sqrt{M}} \, \frac{\kappa_M}{\sqrt{M}} \, \|a^{(x)}\|_2 + \mathcal{O}(\delta^2) \\ &= \delta \, \frac{\kappa_M}{M} \, \|a^{(x)}\|_2 + \mathcal{O}(\delta^2), \end{aligned}$$

其中，$\mathcal{O}(\delta^2)$ 中隐藏的常数可由 $C_{\mathrm{rem}}(t, \ C_G)$ 和 $|X|$ 控制，且与 M 和 θ 无关。根据全变差距离的定义，

$$F_{\mathrm{TV}}(\theta) = \frac{1}{2} \sum_{x \in X} |\Delta p_x(\theta)|,$$

并对 θ 取期望，得到

$$\begin{aligned} m(\delta) = \mathbb{E}_\theta F_{\mathrm{TV}}(\theta) &= \frac{1}{2} \sum_{x \in X} \mathbb{E}_\theta \big|\Delta p_x(\theta)\big| \\ &= \frac{1}{2} \sum_{x \in X} \Big[\delta \, \frac{\kappa_M}{M} \, \|a^{(x)}\|_2 + \mathcal{O}(\delta^2) \Big]. \end{aligned}$$

分离一阶项和 $\mathcal{O}(\delta^2)$ 项，

$$m(\delta) = \delta \, \frac{\kappa_M}{2M} \sum_{x \in X} \|a^{(x)}\|_2 + \mathcal{O}(\delta^2),$$

这正是 (8.9)–(8.10)。

最后，利用引理 $\kappa_M \to \sqrt{2/\pi}$ 中的渐近行为 23，我们可以写成 $\kappa_M = \sqrt{2/\pi} + \mathcal{O}(M^{-1})$，将其代入 $m_0(M)$ 可得（8.11）：δ 中的主导线性项系数为 $\frac{1}{2M} \sqrt{2/\pi} \sum_{x \in X} \|a^{(x)}\|_2$，而 κ_M 偏离 $\sqrt{2/\pi}$ 所带来的贡献则是一个额外的 $o(\delta)$项。 ■

注 24（与开放系统波特–托马斯均值假设的关系）。 定理 $m(\delta) = \mathbb{E} d_{\mathrm{TV}}(P_{\mathcal{L}(\theta)}, Q)$ 中的表达式 *16* 为“开放系统波特–托马斯均值假设”提供了一种线性响应的解析体现。我们可以区分以下几种情况：

1. 如果 $\sum_x \|a^{(x)}\|_2$ 的尺度随 $M \to \infty$ 增长而保持广延，例如

$$\frac{1}{M} \sum_{x \in X} \|a^{(x)}\|_2 \to c_a > 0,$$

then

$$m(\delta) \approx \delta \cdot \frac{\sqrt{2/\pi}}{2} c_a,$$

也就是说，在大系统极限下，平均总变差距离保持 $O(\delta)$ 常数级尺度。

2. 如果在某些具体模型中， $\sum_x \|a^{(x)}\|_2$ 的增长慢于 M，例如 $\sum_x \|a^{(x)}\|_2 = o(M)$，那么 $m_0(M) \to 0$，且平均总变差距离会随系统规模增大而缩小。这意味着，在此类系综和给定的测量接口下，大多数 $P_{\mathcal{L}(\theta)}$ 都与参考分布 Q 在全变差意义下接近；在此情形下，基于 $d_{\mathrm{TV}}(P_{\mathcal{L}}, Q)$ 的统计查询困难性判据无法给出非平凡的下界。

注释 *25*（参数维数 M 与线性响应的有效性）。需要强调的是，在线性响应展开 *(8.1)* 中， δ 是小参数，而参数维数 M 的增长则通过 $\|K(\theta)\|_{1\to 1} \le C_G$ 以及引理 *23* 中的 $1/\sqrt{M}$ 尺度得到明确控制。只要 δ 足够小，使得二阶余项 $O(\delta^2)$ 相较于一阶项可以忽略，即使 M 很大，线性响应仍然有效。高维并不会破坏线性响应；它只是通过 $\mathbb{E}|\langle \theta, a^{(x)} \rangle|$ 的 $1/\sqrt{M}$ 尺度，影响 $m_0(M)$ 的定义。

—

第九节. 随机局域振幅阻尼 Lindblad 算子中的线性响应均值缩放与数值模拟

在本节中，我们在随机局域林德布拉德系综（定义 26）的框架下，选取一个具体且可显式计算的一维振幅阻尼模型。在该模型中，我们显式计算一阶线性响应系数 $\{a_{j,\ x}\}$ 及其平均范数 $\frac{1}{M}\sum_x \|a^{(x)}\|_2$，进而得到小噪声极限下平均总变差距离 $m_0 > 0$ 的标度常数 $\mathbb{E}_\theta d_{\mathrm{TV}}(P_{\mathcal{L}(\theta)}, Q)$。我们还对定义 27中的一维局域振幅阻尼模型进行了数值模拟，以检验定理 17并为假设 1提供数值支持。

A. 平均总变差距离的标度常数 $m_0 > 0$

定义 27（随机局域振幅阻尼 Lindblad 算子模型）。 基于定义 *26*的设定，我们作出以下具体选择：

1. 该系统是一条由 N 个量子比特组成的一维链，其希尔伯特空间

$$\mathcal{H} = (\mathbb{C}^2)^{\otimes N}, \qquad d = 2^N.$$

2. 为便于进行一阶线性响应分析，在此玩具模型中我们设定

$$\mathcal{L}_{\mathrm{ref}} = 0,$$

使参考演化为恒等映射 $\Lambda_t^{(\mathrm{ref})} = e^{t\mathcal{L}_{\mathrm{ref}}} = \mathrm{id}$。输入态选为全1计算基态

$$\rho_{\mathrm{in}} := |1 \ldots 1\rangle\langle 1 \ldots 1|.$$

3. 在每个位点 $j = 1, \ldots, N$ 上，我们引入一个局域振幅阻尼跳跃算符

$$J_j^{(-)} := \sqrt{\gamma}\,\sigma_j^-,$$

其中 σ_j^- 是作用于第 j 个量子比特的降算符，$\gamma > 0$ 是单量子比特衰减率。对于每个 $J_j^{(-)}$，我们定义相应的耗散子

$$G_j := \mathcal{D}_j^{(-)}, \qquad \mathcal{D}_j^{(-)}(\rho) := J_j^{(-)} \rho J_j^{(-)\dagger} - \frac{1}{2}\{J_j^{(-)\dagger} J_j^{(-)}, \rho\}.$$

因此，参数维数为

$$M := N.$$

4. 测量为全局计算基 *POVM*

$$\{M_x\}_{x \in \{0,1\}^N}, \qquad M_x := |x\rangle\langle x|, \quad X := \{0,1\}^N.$$

我们写作 $\left|1^N\right\rangle := |1 \ldots 1\rangle$，并对每个 j 定义比特串

$$x_j^{(0)} \in \{0,1\}^N$$

该比特串的第 j 位为 0，其余各位均为 1。显然，$\{1^N\} \cup \{x_j^{(0)}\}_{j=1}^N \subset X$。

5. 参数空间为实球面

$$S^{M-1} = \{\theta \in \mathbb{R}^M : \ \|\theta\|_2 = 1\}, \qquad M = N.$$

对于一个小参数 $\delta > 0$，我们定义线性参数化

$$\mathcal{L}(\theta) := \mathcal{L}_{\mathrm{ref}} + \frac{\delta}{\sqrt{M}} \sum_{j=1}^{M} \theta_j G_j = \frac{\delta}{\sqrt{N}} \sum_{j=1}^{N} \theta_j G_j, \qquad \theta \in S^{M-1}.$$

我们取 μ_{sph} 在 S^{M-1} 上的旋转不变测度，并通过 $\theta \mapsto L(\theta)$ 将其向前推送，得到

$$\mu_{\mathcal{L}} := (\mathcal{L})_{\#}\mu_{\mathrm{sph}},$$

这定义了一个随机局域振幅阻尼林布拉德算符系综 $F := \{L(\theta) : \ \theta \in S^{M-1}\}$。

6. 在此模型中，自然地，我们将参考分布 Q 取为参考动力学（即 $L_{\mathrm{ref}} = 0$）下的测量分布：

$$Q(x) := \mathrm{Tr}(M_x \rho_{\mathrm{in}}) = \delta_{x,1^N}, \qquad x \in X.$$

备注 26. 在更一般的情形下，L_{ref} 可以是量子马尔可夫半群的任意 *GKSL* 生成元，例如局域振幅阻尼项加上局域哈密顿量；参考分布 Q 也可以选为系综平均$Q[\varphi] = \mathbb{E}_{\mathcal{L}\sim\mu_{\mathcal{L}}} P_{\mathcal{L}}[\varphi]$. 。在小噪声极限 $\delta \to 0$ 下，参考分布的不同选择只会改变高阶修正，不会影响一阶线性响应标度常数。本节将 $L_{\mathrm{ref}} = 0$ 设为纯粹形式，只为使 $a_{j,x}$ 能够显式计算。

引理 24（局域振幅阻尼耗散子对输入态的作用）。 在定义 27的设定下，对于每个 $j = 1$，.....，N，

$$G_j(\rho_{\mathrm{in}}) = \gamma\Big(\left|x_j^{(0)}\right\rangle\!\left\langle x_j^{(0)}\right| - \left|1^N\right\rangle\!\left\langle 1^N\right|\Big),$$

其中，$x_j^{(0)}$ 是第 j 位为0、其余位为1的比特串，而 $\left|1^N\right\rangle = |1 \ldots 1\rangle$。

证明。 我们首先考察单量子比特振幅阻尼耗散子$\mathcal{D}^{(-)}(\rho) := \gamma(\sigma^-\rho\sigma^+ - \frac{1}{2}\{\sigma^+\sigma^-, \rho\})$，其中 $\sigma^- = |0\rangle\langle 1|$，$\sigma^+ = |1\rangle\langle 0|$。对于单量子比特输入 $\rho = |1\rangle\langle 1|$，我们有

$$\begin{aligned}\sigma^-\rho\sigma^+ &= |0\rangle\langle 1|\,|1\rangle\langle 1|\,|1\rangle\langle 0| = |0\rangle\langle 0|,\\ \sigma^+\sigma^- &= |1\rangle\langle 1|,\\ \frac{1}{2}\{\sigma^+\sigma^-, \rho\} &= \frac{1}{2}(|1\rangle\langle 1|\,\rho + \rho|1\rangle\langle 1|) = |1\rangle\langle 1|.\end{aligned}$$

因此

$$\mathcal{D}^{(-)}(|1\rangle\langle 1|) = \gamma(|0\rangle\langle 0| - |1\rangle\langle 1|).$$

在多体系统上，$J_j^{(-)} = \sqrt{\gamma}\,\sigma_j^-$ 仅作用于第 j 个量子比特，而在其他所有量子比特上作用为恒等映射。记 $|1^N\rangle = |1\rangle \otimes \cdots \otimes |1\rangle$，则有

$$J_j^{(-)}|1^N\rangle = \sqrt{\gamma}\,|1\rangle \otimes \cdots \otimes |0\rangle_j \otimes \cdots \otimes |1\rangle = \sqrt{\gamma}\,\left|x_j^{(0)}\right\rangle,$$

因此

$$J_j^{(-)}\rho_{\mathrm{in}}J_j^{(-)\dagger} = \gamma\left|x_j^{(0)}\right\rangle\!\left\langle x_j^{(0)}\right|.$$

另一方面，

$$J_j^{(-)\dagger}J_j^{(-)} = \gamma\left(\mathbb{I}^{\otimes(j-1)} \otimes |1\rangle\langle 1|_j \otimes \mathbb{I}^{\otimes(N-j)}\right),$$

因此对于输入态 $\rho_{\mathrm{in}} = |1^N\rangle\langle 1^N|$，

$$\frac{1}{2}\{J_j^{(-)\dagger}J_j^{(-)}, \rho_{\mathrm{in}}\} = \gamma\,|1^N\rangle\langle 1^N|.$$

将这些代入 $G_j = \mathcal{D}_j^{(-)}$ 的定义中，得到

$$G_j(\rho_{\mathrm{in}}) = \gamma\left(\left|x_j^{(0)}\right\rangle\!\left\langle x_j^{(0)}\right| - |1^N\rangle\langle 1^N|\right),$$

正如所述。 ■

引理 25 （一阶线性响应系数的显式表达式 $a_{j,\,x}$）。 在定义 27 的设定下，令

$$\Lambda_t^{(\theta)} := e^{t\mathcal{L}(\theta)}, \qquad P_{\mathcal{L}(\theta)}(x) := \mathrm{Tr}\big(M_x\,\Lambda_t^{(\theta)}(\rho_{\mathrm{in}})\big).$$

在小噪声极限 $\delta \to 0$ 下，存在系数 $a_{j,\,x} \in \mathbb{R}$ 使得

$$P_{\mathcal{L}(\theta)}(x) = Q(x) + \frac{\delta}{\sqrt{M}}\sum_{j=1}^{M}\theta_j a_{j,x} + \mathcal{O}(\delta^2), \tag{9.1}$$

其中 $Q(x) = \delta_{x,\,1^N}$，且

$$a_{j,x} = t\gamma\big(\delta_{x,x_j^{(0)}} - \delta_{x,1^N}\big), \qquad j = 1,\dots,M, \quad x \in X, \tag{9.2}$$

其中 $M = N$。

证明。 由于$\mathcal{L}(\theta)$ 对 δ 呈线性依赖，我们写作

$$\mathcal{L}(\theta) = \frac{\delta}{\sqrt{M}}\sum_{j=1}^{M}\theta_j G_j, \qquad \mathcal{L}_{\mathrm{ref}} = 0.$$

将 $e^{t\mathcal{L}(\theta)}$ 在 $\delta=0$ 附近展开至一阶，得到

$$\Lambda_t^{(\theta)} = e^{t\mathcal{L}(\theta)} = \mathbb{I} + t\mathcal{L}(\theta) + \mathcal{O}(\delta^2) = \mathbb{I} + t\frac{\delta}{\sqrt{M}}\sum_{j=1}^{M}\theta_j G_j + \mathcal{O}(\delta^2).$$

作用于输入态 ρ_{in}，

$$\Lambda_t^{(\theta)}(\rho_{\text{in}}) = \rho_{\text{in}} + t\frac{\delta}{\sqrt{M}}\sum_{j=1}^{M}\theta_j G_j(\rho_{\text{in}}) + \mathcal{O}(\delta^2).$$

对于每个测量结果 $x\in X$，

$$\begin{aligned} P_{\mathcal{L}(\theta)}(x) &= \operatorname{Tr}\big(M_x\Lambda_t^{(\theta)}(\rho_{\text{in}})\big) \\ &= \operatorname{Tr}(M_x\rho_{\text{in}}) + t\frac{\delta}{\sqrt{M}}\sum_{j=1}^{M}\theta_j\operatorname{Tr}\big(M_x G_j(\rho_{\text{in}})\big) + \mathcal{O}(\delta^2). \end{aligned}$$

由于 $\rho_{\text{in}} = \left|1^N\right\rangle\!\left\langle 1^N\right|$ 和 $M_x = |x\rangle\langle x|$，

$$\operatorname{Tr}(M_x\rho_{\text{in}}) = \delta_{x,1^N} = Q(x).$$

利用引理 24，

$$\operatorname{Tr}\big(M_x G_j(\rho_{\text{in}})\big) = \gamma(\delta_{x,x_j^{(0)}} - \delta_{x,1^N}).$$

由此可得

$$P_{\mathcal{L}(\theta)}(x) = Q(x) + \frac{\delta}{\sqrt{M}}\sum_{j=1}^{M}\theta_j\big[t\gamma(\delta_{x,x_j^{(0)}} - \delta_{x,1^N})\big] + \mathcal{O}(\delta^2),$$

因此一阶系数为

$$a_{j,x} := t\gamma(\delta_{x,x_j^{(0)}} - \delta_{x,1^N}),$$

由此得到（9.1）和（9.2）。 ■

引理 26（一阶系数向量的范数与均值缩放 $a^{(x)}$）。 在前一个引理的设定下，为每个结果 $x\in X$ 关联一阶系数向量

$$a^{(x)} := (a_{1,x},\dots,a_{M,x})\in\mathbb{R}^M, \qquad \|a^{(x)}\|_2 := \Big(\sum_{j=1}^{M}a_{j,x}^2\Big)^{1/2}.$$

那么：

1. 对于全1 结果 $x=1^N$，

$$\|a^{(1^N)}\|_2 = \gamma t\sqrt{M}.$$

2. 对于每个 $j=1$、……、M，结果 $x_j^{(0)}$ 满足

$$\|a^{(x_j^{(0)})}\|_2 = \gamma t.$$

3. 对于所有其他结果（至少包含两个零的比特串），我们有 $\|a^{(x)}\|_2 = 0$。

4. 因此，平均范数满足

$$\frac{1}{M}\sum_{x\in X}\|a^{(x)}\|_2=\gamma t\Big(1+\frac{1}{\sqrt{M}}\Big)\xrightarrow[M\to\infty]{}\gamma t. \tag{9.3}$$

证明。 由（9.2），对于固定的 x 各分量为

$$a_{j,x}=t\gamma(\delta_{x,x_j^{(0)}}-\delta_{x,1^N}).$$

(1) 对于 $x=1^N$, $\delta_{x,\,x_j^{(0)}}=0$ 和 $\delta_{x,\,1^N}=1$，因此

$$a_{j,1^N}=-t\gamma,\qquad j=1,\dots,M.$$

因此

$$\|a^{(1^N)}\|_2=\Big(\sum_{j=1}^{M}(t\gamma)^2\Big)^{1/2}=\gamma t\sqrt{M}.$$

(2) 对于 $x=x_k^{(0)}$ （第 k 位为 0、其余位为 1 的比特串），

$$\delta_{x_k^{(0)},x_j^{(0)}}=\delta_{j,k},\qquad \delta_{x_k^{(0)},1^N}=0,$$

so

$$a_{j,x_k^{(0)}}=t\gamma(\delta_{j,k}-0)=\begin{cases}t\gamma, & j=k,\\ 0, & j\neq k.\end{cases}$$

Thus

$$\|a^{(x_k^{(0)})}\|_2=\big((t\gamma)^2+0+\cdots+0\big)^{1/2}=\gamma t.$$

(3) 对于任何其他 x （至少含有两个 0）， x 既不是 1^N，也不是任何 $x_j^{(0)}$，因此 $\delta_{x,\,x_j^{(0)}}=0=\delta_{x,\,1^N}$ 对所有 j均成立，由此 $a_{j,\,x}=0$ 且范数为零。

(4) 对所有 x求和时，只有 $x=1^N$ 和 M 个单比特翻转串 $x_j^{(0)}$ 有贡献，因此

$$\begin{aligned}\sum_{x\in X}\|a^{(x)}\|_2&=\|a^{(1^N)}\|_2+\sum_{j=1}^{M}\|a^{(x_j^{(0)})}\|_2+\sum_{\text{other }x}\|a^{(x)}\|_2\\&=\gamma t\sqrt{M}+M\gamma t.\end{aligned}$$

两边除以 M，得到

$$\begin{aligned}\frac{1}{M}\sum_{x\in X}\|a^{(x)}\|_2&=\frac{\gamma t\sqrt{M}+M\gamma t}{M}\\&=\gamma t\Big(1+\frac{1}{\sqrt{M}}\Big),\end{aligned}$$

当 $M\to\infty$ 时，其收敛到 γt 。 ■

定理 17 （随机局域振幅阻尼模型中的平均线性响应全变差距离）。 在定义 *27*、引理 *25* 和 *26*的设定下，定义

$$F_{\mathrm{TV}}(\theta):=d_{\mathrm{TV}}(P_{\mathcal{L}(\theta)},Q)=\frac{1}{2}\sum_{x\in X}\big|P_{\mathcal{L}(\theta)}(x)-Q(x)\big|,$$

and

$$m(\delta) := \mathbb{E}_{\theta\sim\mu_{\mathrm{sph}}}\big[F_{\mathrm{TV}}(\theta)\big].$$

那么在小噪声极限 $\delta \to 0$ 下，

$$m(\delta) = \delta\,\frac{\kappa_M}{2M}\sum_{x\in X}\|a^{(x)}\|_2 + \mathcal{O}(\delta^2), \tag{9.4}$$

其中 κ_M 与引理 *23* 及注释 *23*相同。利用引理*26* 我们特别得到

$$m(\delta) = \delta\,\frac{\kappa_M}{2}\,\gamma t\Big(1+\frac{1}{\sqrt{M}}\Big) + \mathcal{O}(\delta^2), \tag{9.5}$$

并且在 $M \to \infty$ 的极限下，

$$m(\delta) \xrightarrow[M\to\infty]{} \delta\,\gamma t\,\sqrt{\frac{1}{2\pi}} + \mathcal{O}(\delta^2). \tag{9.6}$$

换言之，在这个具体的随机局域振幅阻尼模型中，平均总变差距离的一阶线性响应标度常数为

$$m_l := \gamma t\sqrt{\frac{1}{2\pi}} > 0,$$

因此

$$m(\delta) = m_l\,\delta + \mathcal{O}(\delta^2) \quad (M\to\infty).$$

证明。 由引理 25,

$$P_{\mathcal{L}(\theta)}(x) - Q(x) = \frac{\delta}{\sqrt{M}}\sum_{j=1}^{M}\theta_j a_{j,x} + \mathcal{O}(\delta^2) = \frac{\delta}{\sqrt{M}}\,\langle\theta, a^{(x)}\rangle + \mathcal{O}(\delta^2),$$

其中 $a^{(x)} = (a_{1,\,x},\ \ldots\ldots,\ a_{M,\,x})$。因此，全变差距离可以写为

$$F_{\mathrm{TV}}(\theta) = \frac{1}{2}\sum_{x\in X}\big|P_{\mathcal{L}(\theta)}(x) - Q(x)\big| = \frac{\delta}{2\sqrt{M}}\sum_{x\in X}\big|\langle\theta, a^{(x)}\rangle\big| + \mathcal{O}(\delta^2).$$

对 $\theta\sim\mu_{\mathrm{sph}}$ 取期望，并运用引理23,

$$\mathbb{E}_\theta\big[|\langle\theta, a^{(x)}\rangle|\big] = \frac{\kappa_M}{\sqrt{M}}\,\|a^{(x)}\|_2.$$

因此

$$\begin{aligned} m(\delta) &= \mathbb{E}_\theta F_{\mathrm{TV}}(\theta) \\ &= \frac{\delta}{2\sqrt{M}}\sum_{x\in X}\mathbb{E}_\theta\big[|\langle\theta, a^{(x)}\rangle|\big] + \mathcal{O}(\delta^2) \\ &= \frac{\delta}{2\sqrt{M}}\sum_{x\in X}\frac{\kappa_M}{\sqrt{M}}\,\|a^{(x)}\|_2 + \mathcal{O}(\delta^2) \\ &= \delta\,\frac{\kappa_M}{2M}\sum_{x\in X}\|a^{(x)}\|_2 + \mathcal{O}(\delta^2), \end{aligned}$$

即（9.4）。

对于这个具体的模型，引理26 和（9.3）给出

$$\frac{1}{M}\sum_{x\in X}\|a^{(x)}\|_2 = \gamma t\Big(1+\frac{1}{\sqrt{M}}\Big),$$

so

$$\begin{aligned} m(\delta) &= \delta\,\frac{\kappa_M}{2M}\sum_{x\in X}\|a^{(x)}\|_2 + \mathcal{O}(\delta^2) \\ &= \delta\,\frac{\kappa_M}{2}\,\gamma t\Big(1+\frac{1}{\sqrt{M}}\Big) + \mathcal{O}(\delta^2), \end{aligned}$$

即9.5）。

利用$\kappa_M \to \sqrt{2/\pi}$（注23）和 $1+1/\sqrt{M}\to 1$，我们得到

$$\begin{aligned} m(\delta) &\xrightarrow[M\to\infty]{} \delta\,\frac{1}{2}\sqrt{\frac{2}{\pi}}\gamma t + \mathcal{O}(\delta^2) \\ &= \delta\,\gamma t\sqrt{\frac{1}{2\pi}} + \mathcal{O}(\delta^2), \end{aligned}$$

也就是说，一阶线性响应常数为 $m_l = \gamma t\sqrt{1/(2\pi)}$，正如所述。 ■

注 27 （物理解释与尺度总结）。 定理 *17* 表明，在这个随机局域振幅阻尼林布拉德模型中，尽管参数维数 $M = N$ 随系统规模增大，但在小噪声极限下，平均总变差距离的线性响应系数 $\frac{1}{M}\sum_x \|a^{(x)}\|_2$ 不会随M衰减，而是收敛到一个严格为正的常数 γt。将其乘以球面几何因子$\kappa_M/2$，即可得到宏观常数 $m_0 = \gamma t\sqrt{1/}$（2π）。这表明，在这类“局部 *Lindblad* 算子 +随机参数球面”模型中，只要噪声强度 δ 固定，平均总变差距离就不会随参数维数的增加而缩小。这支持了“开放系统波特–托马斯均值假设”中的建模预期，即 $m_0 > 0$ 不依赖于 M（或至少不会随 M衰减）。

B. 数值模拟：验证开放系统 Porter–Thomas 均值假设

在本小节中，我们对定义 27中的一维局域振幅阻尼模型进行数值模拟，以检验定理 17 并为假设 1提供数值支持。根据定理 17，在极限 $M\to\infty$ 下，我们有

$$m(\delta) := \mathbb{E}_{\theta\sim\mu_{\mathrm{sph}}} d_{\mathrm{TV}}\big(P_{\mathcal{L}(\theta)}, Q\big) = m_l\,\delta + \mathcal{O}(\delta^2), \qquad m_l = \gamma t\sqrt{\tfrac{1}{2\pi}},$$

其中， m_l 与参数维数 M无关。在数值计算中，我们设定 $\gamma = t = 1$，因此理论斜率为 $m_l = \sqrt{1/(2\pi)} \approx 0.399$。

数值模型与定理 17中的完全相同：系统是一个含 N 个量子比特的链，其希尔伯特空间维数为 $d = 2^N$，初态为 $\rho_{\mathrm{in}} = |1^N\rangle\langle 1^N|$，测量为全局计算基 POVM，参考分布为 $Q(x) = \delta_{x,\,1^N}$。在刘维尔表示中，对于每个局部耗散子 G_j，我们使用列优先向量化约定 $\mathrm{vec}(A\rho B^\dagger) = (B^{\mathsf{T}}\otimes A)\mathrm{vec}(\rho)$ 构造 $d^2\times d^2$ 超算子矩阵。给定 $\theta\in S^{M-1}$，我们构造

$$L(\theta) = \frac{\delta}{\sqrt{M}}\sum_{j=1}^{M}\theta_j G_j, \qquad \Lambda_t(\theta) = \exp\big(tL(\theta)\big),$$

然后从 $\mathrm{vec}(\rho_{t,\theta}) = \Lambda_t(\theta)\,\mathrm{vec}(\rho_{\mathrm{in}})$ 中得到 $\rho_{t,\theta}$。读取 $\rho_{t,\theta}$ 的对角线元素，即可得到输出分布 P_θ。对于每一对 (N,δ)，我们从球面 S^{M-1} 中独立采样 n_{samp} 个参数 $\theta^{(\ell)}$，

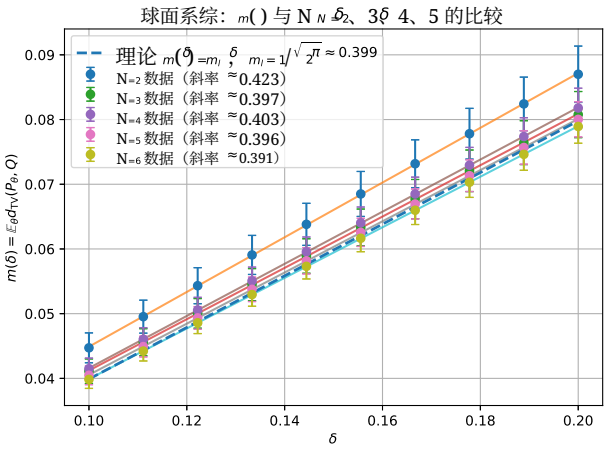

图 4. 在小噪声区间 $\delta \in [0.1, 0.2]$ 内，对于 $N = 2, \ldots, 6$，球形随机局域 Lindblad 模型中的平均全变差距离 $m(\delta;\, N) = \mathbb{E}_\theta d_{\mathrm{TV}}(P_\theta, Q)$。实心点表示蒙特卡洛数据，误差棒表示标准误。实线是各个 N 对应的线性拟合，虚线表示理论线性响应 $m(\delta) = m_l \delta$ with$m_l = \sqrt{1/(2\pi)} \approx 0.399$。

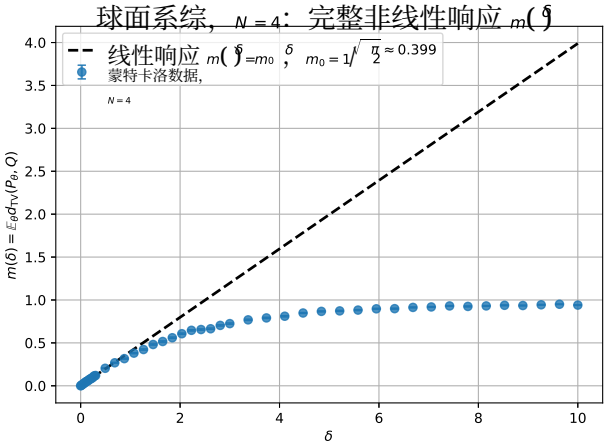

图 5. 在固定系统规模 $N = 4$ 下，球形随机局域 Lindblad 模型在较宽噪声范围 $\delta \in [0, 10]$ 内的平均全变差距离 $m(\delta;\, 4)$。实心点表示蒙特卡洛数据，误差棒表示标准误，虚线表示线性响应预测 $m(\delta) = m_l \delta$。在小噪声区内，两者吻合得非常好；而当 δ 增大时，曲线$m(\delta)$逐渐偏离直线并趋于饱和，展现了林德布拉德动力学的非线性响应。特别是，只要 $\delta > 0$, $m(\delta;\, 4)$ 始终严格为正且为 O(1) 量级。

并进行估计

$$\widehat{m}(\delta; N) = \frac{1}{n_{\mathrm{samp}}} \sum_{\ell=1}^{n_{\mathrm{samp}}} d_{\mathrm{TV}}\big(P_{\theta^{(\ell)}}, Q\big)$$

通过蒙特卡洛方法，其中 $M = N$。样本标准差 $\widehat{\sigma}(\delta;\, N)$ 得出标准误 $\widehat{\sigma}(\delta;\, N)/\sqrt{n_{\mathrm{samp}}}$，我们将其用作误差线。

图 4 展示了在 $\delta \in [0.1, 0.2]$线性响应区间内，$N = 2$取 3、4、5、6 时的数值结果。在此区间内，我们选取 10 个等间距的点，并在每个点用 $n_{\mathrm{samp}} = 200$ 个样本估计 $\widehat{m}(\delta;\, N)$。对于每个 N，我们对 $\widehat{m}(\delta;\, N)$ 进行线性拟合 $\approx m_{mc}^{(N)}\, \delta + b_N$. 拟合斜率 $m_{mc}^{(N)}$集中在 0.39–0.42 区间内；例如，$m_{mc}^{(2)} \approx 0.423$、$m_{mc}^{(4)} \approx 0.403$、$m_{mc}^{(6)} \approx 0.391$。这些结果与理论值$m_l \approx 0.399$ 一致，相对误差约为 5%–10%；而截距 b_N 远小于数据本身，数值上接近 0。随着 N 增大（在此模型中 $M = N$），拟合直线逐渐趋近于共同的理论直线 $m(\delta) = m_l \delta$，表明有限尺寸修正随 M增大而减小，这与定理 17 中的 $M \to \infty$ 极限一致。这直接验证了我们在第 IX A 节中的解析推导，并支持假设 1 中的物理解释，即“$m > 0$ 是一个与 M无关的常数，而不会随 M衰减”。

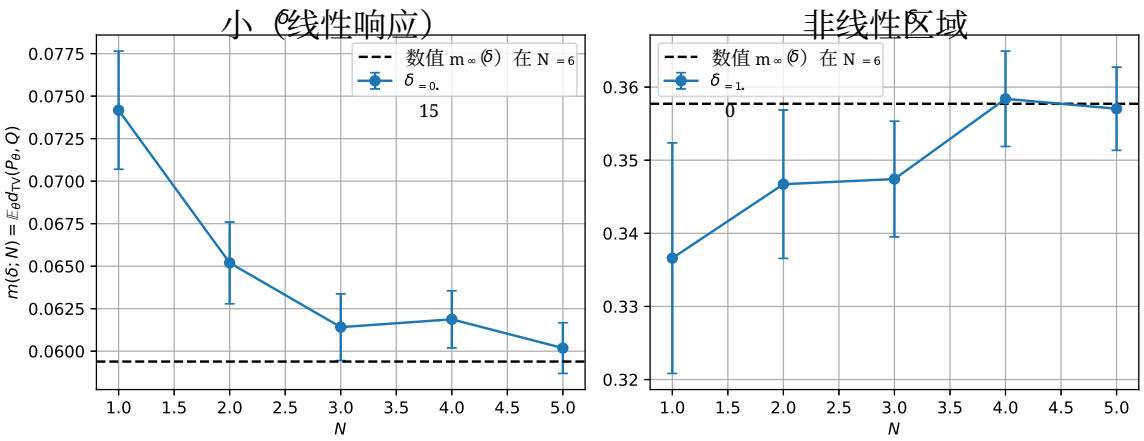

图 6. 球形随机局域 Lindblad 模型中，平均全变差距离 $m(\delta;\, N) \;=\; \mathbb{E}_\theta d_{\mathrm{TV}}(P_\theta,\;\; Q)$ 随量子比特数 N的变化。左图展示线性响应区域中的代表点 $\delta = 0.15$，右图展示非线性区间中的代表点 $\delta = 1.0$。实心圆点表示蒙特卡洛数据，误差棒表示标准误；虚线表示在 $N = 6$,

$\widehat{m}_\infty\ \delta\ \ = \widehat{m}\ \delta\ N = 6\qquad N\qquad\qquad 1\quad 5\ m\ \delta\ N$

( ) : (;) 处的数值参考值。随着从 增加到 ， (;) 在两种噪声强度下都迅速收敛到同一个宏观常数。

为了探究线性响应的失效以及强噪声下的行为，我们进一步固定 $N = 4$ ，并将噪声强度扩展至 $\delta \in [0, 10]$。我们在三个区间 $\delta \in [0.01, 0.3]$、 $[0.3, 3.0]$和$[3.0, 10.0]$ 采用非均匀步长（在较小的 δ处采样更密集）。在每个点，我们用 $n_{\mathrm{samp}} = 400$ 个样本估计 $\widehat{m}(\delta;\, 4)$。结果如图 5 所示。在小噪声区 $\delta \lesssim 0.2$，数值数据几乎完美地沿着直线 $m_l\delta$变化，再次验证了定理 17 给出的展开式 $m(\delta) \;= m_l\delta + \mathrm{O}(\delta^2)$。当 δ 增大到$O(1)$及以上时， $m(\delta)$仍单调增长，但明显低于线性外推，并在$\delta \sim 3$ 之后逐渐饱和至 O(1) 常数。这可以解释如下：一旦局域耗散强度足够大，系统几乎会在固定演化时间 t 内完全弛豫至一个基本不依赖于 θ 的稳态（在此模型中接近全零态）。在此区间内， P_θ 与参考分布 Q 之间的全变差距离受稳态自身结构的限制，不再随 δ线性增长，因此在大噪声区呈现出典型的非线性响应和饱和现象。

为了更直接地刻画系统参数增大时有限尺寸误差项 $\epsilon_{\mathrm{mean}} > 0$ 在假设 1 中的变化，我们进一步固定两种具有代表性的噪声强度：一种处于线性响应区域，$\delta = 0.15$，另一种处于非线性区间， $\delta = 1.0$。随后我们研究

$$m(\delta; N) := \mathbb{E}_\theta d_{\mathrm{TV}}\big(P_{\mathcal{L}(\theta)}, Q\big)$$

作为量子比特数量 N 的函数。在数值计算中，我们取 $N = 1$、2、3、4、5、6，并对每个 (δ, N) 使用 $n_{\mathrm{samp}} = 400$ 个样本估计 $\widehat{m}(\delta;\, N)$。对于固定的 δ，我们将最大系统规模 $N_{\max} = 6$ 下的值 $\widehat{m}(\delta;\, N_{\max})$ 视为“近似渐近值” $\widehat{m}_\infty(\delta)$，并且仅绘制 $N = 1$、.....、5 的数据。图 6 的左、右面板分别展示了 $\delta = 0.15$ （线性响应区域）和 $\delta = 1.0$ （非线性区间）的结果；水平虚线表示数值参考值 $\widehat{m}_\infty(\delta)$。

我们观察到，无论在小噪声区间还是非线性区间，随着 N 增大， $\widehat{m}(\delta;\, N)$ 都稳定地趋近于同一条水平虚线。对于 $\delta = 0.15$，当 N 从 1 增至 5 时，平均全变差距离从约 7×10^{-2} 降低，并趋近于 $\widehat{m}_\infty(0.15)$。对于 $\delta = 1.0$，非线性区间中的 $m(\delta;\, N)$ 略有上升，随后迅速饱和，并在 $N = 6$ 处趋近于参考值。对于给定的噪声强度 δ，平均全变差距离在有限尺寸下仅对 N 有较弱的依赖，并迅速收敛至一个与 N （因而也与 M）无关的常数，这与假设 1 中存在极限均值 $m_0(\delta)$ 的假设一致。

为量化有限尺寸偏差，我们将该模型中 ϵ_{mean} 假设1 中的误差项定义为如下数值代理量

$$\widehat{\epsilon}_{\mathrm{mean}}(\delta; N) := \big|\widehat{m}(\delta; N) - \widehat{m}_\infty(\delta)\big|, \qquad \widehat{m}_\infty(\delta) = \widehat{m}(\delta; N_{\max}),\ N_{\max} = 6,$$

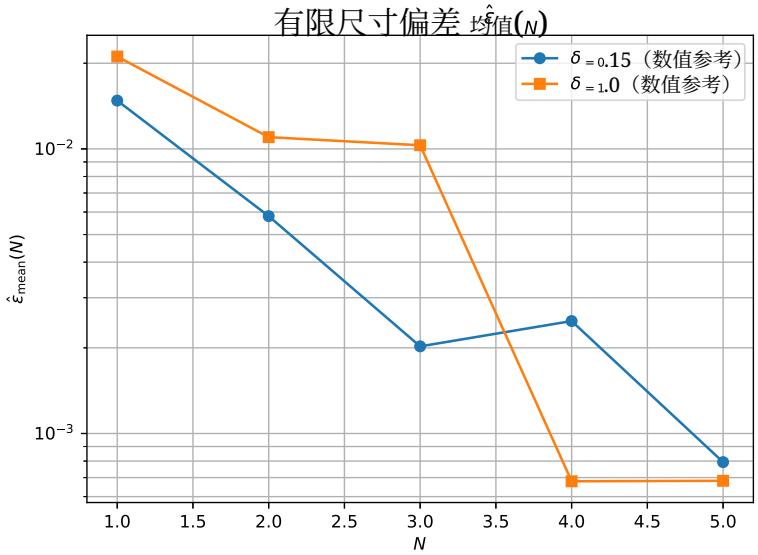

图 7. 有限尺寸偏差 $\widehat{\epsilon}_{\mathrm{mean}}(\delta;\ N) = |\widehat{m}(\delta;\ N) - \widehat{m}_{\infty}(\delta)|$ 作为量子比特数的函数 N，其中 $\widehat{m}_{\infty}(\delta)$ 取自 $N = 6$处的数值。蓝色圆圈和橙色方块分别对应于 $\delta = 0.15$ 线性响应区域中的情形，以及 $\delta = 1.0$ 非线性区间中的情形。纵轴采用对数尺度。两条曲线均呈现出明显趋向 0的趋势，表明该模型中平均全变差距离的有限尺寸修正迅速衰减，从而为假设 $\epsilon_{\mathrm{mean}} \to 0$ 中的条件提供了直接的数值证据 1。

并在图 $\widehat{\epsilon}_{\mathrm{mean}}$（$\delta$; N）中以半对数尺度绘制图像。7我们看到，对于 $\delta = 0.15$和 $\delta = 1.0$两者，$\widehat{\epsilon}_{\mathrm{mean}}$（$\delta$; N）均近似单调下降，从 10^{-2} 在 $N = 1$ 处的约 10^{-3} 下降至 $N = 5$处的或更小。这表明，在该局部 Lindblad 算子模型中，系统规模（量子比特数量 N 和参数维数 M）增大时，平均全变差距离的有限尺寸偏差 ϵ_{mean} 确实会迅速减小，从而为 $\epsilon_{\mathrm{mean}} \to 0$ 假设1中的条件提供了数值证据。

X. 随机林德布拉德算子构造的物理不可克隆函数：分布层面与基于层析的验证

本节将上述针对随机林德布拉德算子系综得到的 SQ/QPStat 学习困难性结果，转化为两个具体的密码协议。

物理不可克隆函数（PUF）最初被提出作为一种硬件原语，利用微观制造噪声实现认证和指纹识别等密码学任务 [CZZ17，DMAM17，PRTG02]。在经典情形下，PUF 通常由特定电路架构或光学介质实现；制造过程中产生的不可控缺陷会形成不可克隆的挑战—响应关系。然而，后续研究表明，这类经典 PUF 易受侧信道攻击和机器学习攻击：一旦观察到足够多的挑战—响应对，对手往往就能构建一个高效的经典模型，在统计层面复现 PUF 的行为 [RSS+10，GTFS16，TPI19，KG19]。为从原理上规避这类基于学习的攻击，人们提出了量子物理不可克隆函数的概念，利用量子态的不可克隆性和 Haar随机幺正演化，实现信息论安全认证 [ADDK21，PASA+21]。然而，现有的安全构造通常需要近似Haar随机幺正算符，还需要量子通信和量子存储器，因此在可预见的近期和中期平台上实现的成本极高 [ADDK21]。作为折中方案，人们提出了经典读出量子物理不可克隆函数（CR-QPUF），旨在保留量子物理不可克隆函数的部分安全性，同时仅依赖经典通信和存储 [PPS22，PASA+21]。

本节的目标是说明，针对随机林德布拉德系综的学习困难性结果可以转化为明确的 Lindblad-PUF 协议，其中 (i) 验证者和诚实证明者的成本仍为相关系统参数的多项式级，而 (ii) 任何以非可忽略概率通过验证的对手，都必须在 SQ 或 QPStat 意义下解决一个指数困难的学习问题。

我们将考虑两种验证范式：

(A) 通过 SQ 接口和庞大的测试函数族进行分布级验证。 在工厂（设置）阶段，制造商可以访问实现 Lindblad 通道 E_θ 后接固定测量 $\{M_x\}_{x\in X}$ 的设备样本，并利用这些样本访问，以较小的逐坐标误差学习完整的经典输出分布 $P_\theta(x) = \mathrm{Tr}(M_x E_\theta(\rho_{\mathrm{in}}))$，并将指纹 $\{P_\theta(x)\}_{x\in X}$ 作为经典秘密存储起来。然而，部署之后，物理设备只开放 SQ 接口 $\mathrm{Stat}_\tau(P_\theta)$：包括任何对手在内的外部用户不再能看到原始样本，只能获取测试函数 φ 的近似期望值 $P_\theta[\varphi]$： $X \to [-1,1]$。

公开挑战空间取为一个由 Hadamard 型测试函数构成的指数规模族 $\mathcal{F}_{\mathrm{Had}}$，定义在 X（定义 28）上，并由比特串 $\mathrm{BIT} \in \{0,1\}^L$ 进行索引。在每次认证会话中，验证者从 N_{chal} 中均匀随机抽取测试函数 $\mathcal{F}_{\mathrm{Had}}$，并检查统计查询预言机的回答是否与预先计算的概率指纹一致。拥有真实设备物理访问权限的诚实证明者只需进行多项式次数的统计查询调用即可通过这些测试，因此验证是高效的。

另一方面，由于挑战空间的大小为 $|\mathcal{F}_{\mathrm{Had}}| = 2^L$，任何试图预先计算并存储所有可能挑战对应答案的查表攻击，都需要在 L 中进行指数次数的统计查询。因而，我们的设计从构造上排除了这类非学习型攻击。此外，任何不依赖查表、但仍希望以不可忽略的概率正确回答随机子集中的 Hadamard 测试函数的对手，实际上都被迫在全变差距离意义下学习完整的输出分布。根据第 VIIC 节的统计查询困难性定理，这需要在 Lindblad 参数维数 M 上进行指数次数的统计查询，而验证者的成本在 $|X|$ 上仍为多项式级，并且与 M 无关。因此，我们将方案 A 视为一种真正积极的密码学构造：验证很容易，而成功的攻击在统计查询意义下具有指数级困难性。

(B) **通过扩展 QPStat 接口进行基于层析的验证。** 在通道层面，我们考虑一种扩展 QPStat 预言机（定义 31），并在算子空间和可观测量空间上构造层析基（引理 32）。在设置阶段，验证者使用 QPStat（或实验）层析 [BŻ17, NC10] 来估计一个层析完备族的期望值 $\mathrm{Tr}[G_k E_\theta(F_j)]$，，并将所得的层析指纹矩阵 $\mathcal{T}(E_\theta)$（定义 32）存储为经典秘密。在认证阶段，证明者必须逐项复现这些条目。根据引理 33，通过验证意味着证明者已在菱形距离意义下学得整个信道 E_θ，因此随机林德布拉德算子的 QPStat 困难性定理（定理 12，见第 VE 节）即可将其排除。

然而，当希尔伯特空间维数为 $D^2 \sim d^4$ 时，层析指纹包含 d 个条目，因此即使每个条目的精度为常数，验证者的初始化成本 q_{tom} 至少也会按 d 的固定多项式增长，最高可达 d^4 的量级。对于典型的局域 Lindbladian 模型，参数维数 M 至多为 d 的多项式，因此验证成本与信道本身的信息内容基本处于同一量级。从密码学视角来看，这属于常见的困境：验证“和”学习任务一样困难 [Gol04]，，因此我们主要将方案 B 视为信息论基准，而非实际高效的 Lindbladian-PUF。

我们首先介绍基于 SQ 的分布级林德布拉德物理不可克隆函数及其安全性定理，并将其视为本节主要的正面密码学构造。随后，我们介绍扩展 QPStat 模型和层析基，并以此为基础讨论基于层析的 Lindbladian-PUF 的 QPStat 安全性和验证成本。

A. 方案 A：基于输出分布的 Lindbladian-PUF

在本小节中，我们提出一种基于 SQ 接口和一族 Hadamard 型测试函数的 Lindblad-PUF 协议。在安全性分析中，我们不对对手 A 的内部攻击策略施加任何结构限制： A 可以是任意算法（可能是随机化的），只要在初始化阶段，其对外部设备的访问严格通过 SQ 接口 $\mathrm{Stat}_\tau(P_\theta)$ 进行，且查询总数不超过给定预算 q。在这种黑盒 SQ 攻击模型中，方案 A 的核心设计思路可概括如下：

1. 在制造阶段，供应商通过样本接口在实验室中高效地学习完整的输出分布 P_θ，并将其存储为秘密概率指纹。

2. 设备离开工厂后，物理设备仅向外界开放 SQ 接口 $\mathrm{Stat}_\tau(P_\theta)$。任何外部对手都无法看到单次测量结果，只能查询任意选定测试函数 φ 的近似期望值： $X \to [-1,1]$。

3. 在认证阶段，验证者从大小为 $|\mathcal{F}_{\mathrm{Had}}| = 2^L$ 的指数规模测试函数族中随机抽取若干个 Hadamard 型测试函数 $\varphi^{(r)}$，利用内部存储的概率指纹 $\{P_\theta(x)\}$ 计算目标值 u_r，并检查对手的模拟器在每一轮给出的响应与 u_r 的误差是否足够小。

这种设计在统计查询复杂度方面具有以下优势，从而保证了密钥的安全：

1. 诚实证明者只需多项式次调用 SQ 接口即可通过认证：在初始化阶段，样本复杂度由霍夫丁不等式控制，且按如下方式缩放：$\mathrm{poly}(n)$；在认证阶段，每轮只需向 $\mathrm{Stat}_\tau(P_\theta)$ 发起一次 SQ 查询即可（见备注 31及下文的完备性分析）。

2. 如果对手尝试查表攻击——即在攻击阶段，试图预先查询并存储 $P_\theta[\varphi_{\mathrm{BIT}}]$ 的近似值，覆盖尽可能多的挑战比特串 BIT——那么，由于哈达玛测试函数族的大小为 2^L，要覆盖大量挑战就必然需要对数量呈指数级增长的测试函数进行 SQ 查询。在我们的统计查询安全模型中，SQ 查询总数 q 被视为主要资源，因此当 $q = \mathrm{poly}(M)$ 时，这类查表策略不可行。

3. 更一般地说，无论对手采用查表、插值，还是任何其他学习型或非学习型策略，只要它在认证阶段以恒定的成功概率通过足够多次随机哈达玛测试，引理 30 和引理 31 就共同意味着，其模拟器 $w_{\theta,R}$ 必须在很大比例的挑战比特串 $P_\theta[\varphi_{\mathrm{BIT}}]$ 上达到极高的近似精度BIT。因此，在统计查询模型中，我们可以重构一个满足 $D_{\theta,R}$ 和$d_{\mathrm{TV}}(P_\theta,D_{\theta,R}) \le \varepsilon_{\mathrm{SQ}}$ 的近似分布。换言之，从信息论的角度来看，任何能够通过认证的对手，都等价于一个成功学习了 P_θ 的统计查询学习器，因此必然触发第 VIIC 节中针对随机林德布拉德算子确立的指数级平均情形统计查询下界（见定理 18）。

现在，我们将对测试函数族和协议进行形式化定义，然后陈述并证明安全性定理。

我们首先详细介绍 Hadamard 型测试函数族和 SQ 接口，并采用第 VIIC 节的统计查询模型记号11（另见定义 $P \in \mathcal{D}_X$）：对于一个定义在 X 上的分布以及容差 $\tau > 0$，统计查询预言机 $\mathrm{Stat}_\tau(P)$ 对任意查询函数 $\varphi\colon X \to [-1,1]$，返回一个实数 v，使得

$$|v - P[\varphi]| \le \tau.$$

在本小节中， X 是一个有限经典测量输出空间（例如，某种粗粒化分块投影测量所得到的结果组成的有限集$\{M_x\}_{x\in X}$；原则上，也可以将$X = \{0,1\}^n$ 取为一个 n量子比特系统的计算基测量结果，但我们稍后会解释为什么这并不理想）。为了构造一个指数规模的挑战空间，我们引入以下编码和测试函数。

定义 28（编码与哈达玛型测试函数族）。 设 X 为一个满足 $|X| = N$的有限集。选择$L \ge \lceil \text{对数}_2\, N \rceil$，并固定一个公开的单射编码

$$h : X \hookrightarrow \{0,1\}^L.$$

在 X 上实现的不同函数 $\varphi_{\mathrm{BIT}}(x) = (-1)^{\langle \mathrm{BIT},\ h(x)\rangle}$ 的数量等于 2^r，其中

$$r := \dim_{\mathbb{F}_2}\big(\mathrm{span}_{\mathbb{F}_2}(h(X))\big) = \mathrm{rank}_{\mathbb{F}_2}(H)$$

其中 H 是行由 $h(x)$ 构成的 $|X| \times L$ 矩阵，因此当且仅当 $r = L$ 时，才能达到完整的指数规模 2^L；否则，挑战族会缩减到规模 2^r [Rot06]。我们选择 h，使得 $|X| \times L$ 矩阵 H 的行空间满秩 $r = L$（只要 $|X| \geq L$，这总是可行的），从而在 X 上实现 $|\mathcal{F}_{Had}| = 2^L$ 个不同的测试函数。对于每个比特串 $BIT \in \{0,1\}^L$，定义测试函数

$$\varphi_{\mathrm{BIT}}(x) := (-1)^{\langle \mathrm{BIT}, h(x) \rangle}, \qquad x \in X, \tag{10.1}$$

其中 $\langle \mathrm{BIT}\ h(x) \rangle$ 表示模 2 的按位内积，即：

$$\langle \mathrm{BIT}, h(x) \rangle := \Big(\sum_{j=1}^{L} \mathrm{BIT}_j\, h(x)_j \Big) \bmod 2.$$

显然，对于所有 x，$\varphi_{\mathrm{BIT}}(x) \in \{-1,+1\} \subset [-1,1]$，因此 φ_{BIT} 是一个有效的 SQ 查询函数。

定义指数规模的测试函数族

$$\mathcal{F}_{\mathrm{Had}} := \{\varphi_{\mathrm{BIT}} :\ \mathrm{BIT} \in \{0,1\}^L\},$$

其大小为 $|\mathcal{F}_{\mathrm{Had}}| = 2^L$。

直观地说，$\mathcal{F}_{\mathrm{Had}}$ 是布尔超立方体 $\{0,1\}^L(X)$ 上的沃尔什–哈达玛基在 h上的限制。对于任意分布 $P \in \mathcal{D}_X$，测试值 $P[\varphi_{\mathrm{BIT}}]$ 可以视为P [O'D14]的哈达玛型傅里叶系数。

备注 28 (挑战空间的大小与构造的可行性)。一旦固定 h，挑战空间 $\mathcal{F}_{\mathrm{Had}}$ 的大小恰好为 2^L。在理论分析中，我们通常取 $L = \Theta(n)$，或将其视为独立的安全参数。验证者只需从这个指数规模的族中随机抽取 N_{chal} 个测试函数，即可进行 N_{chal} 轮认证，因此，任何旨在覆盖整个挑战空间的查表攻击都必须付出指数级的 SQ 查询成本。

现在我们解释为何引入希尔伯特空间的分块分解和粗粒化投影测量。在此方案中，我们关注随机林德布拉德演化后的经典输出分布。为避免每个单独比特串的概率都极小（呈指数级小）的极端情况，我们先在量子层面将希尔伯特空间粗粒化为若干块，然后对这些块进行投影测量，并将其作为 POVM 元素。

定义 29（正交分块分解与分块投影 POVM）。考虑一个含 n 个量子比特的系统，其希尔伯特空间为 $H \simeq (\mathbb{C}^2)^{\otimes n}$，维数为 $d = 2^n$。取一个有限指标集 X，并选取一族两两正交子空间

$$\mathcal{H} = \bigoplus_{x \in X} \mathcal{H}_x,$$

其中子空间 $H_x \subset H$ 两两正交。令 Π_x 为投影到 H_x上的正交投影算子，并定义 POVM 元素

$$M_x := \Pi_x, \qquad x \in X.$$

引理 27（分块投影 POVM 的算子范数与完备性）。在定义 29的设定下，有：

1. 对于每个 $x \in X$，Π_x 是一个正交投影算子：$\Pi_x^\dagger = \Pi_x$，$\Pi_x^2 = \Pi_x$.
2. 对于每个 $x \in X$，

$$0 \leq \Pi_x \leq I, \qquad \|\Pi_x\|_\infty = 1.$$

3. $\{M_x\}_{x \in X}$ 构成一个投影测量（POVM）：$\sum_{x \in X} M_x = I$，并且对所有 $x \neq y$，$M_x M_y = 0$。

证明。 根据正交分解 $\mathcal{H} = \bigoplus_{x\in X}\mathcal{H}_x$ 的标准性质，每个 Π_x 都是到 $\mathcal{H}_x$ 上的正交投影算子，因此 $\Pi_x^\dagger = \Pi_x$ 且 $\Pi_x^2 = \Pi_x$。

对于任意单位向量 $|\psi\rangle$，都有 $\|\Pi_x|\psi\rangle\| \le \||\psi\rangle\| = 1$，因此 $\|\Pi_x\|_\infty \le 1$。另一方面，若取任意归一化向量 $|\phi\rangle \in \mathcal{H}_x$，则 $\Pi_x|\phi\rangle = |\phi\rangle$，这意味着 $\|\Pi_x\|_\infty \ge 1$。综合可得 $\|\Pi_x\|_\infty = 1$以及 $0 \le \Pi_x \le I$。

由 $\mathcal{H}$ 的正交直和分解，任意向量 $|\psi\rangle \in\mathcal{H}$ 都可以唯一地写成 $|\psi\rangle = \sum_{x\in X}|\psi_x\rangle$，其中 $|\psi_x\rangle \in \mathcal{H}_x$。因此

$$\Big(\sum_{x\in X}\Pi_x\Big)|\psi\rangle = \sum_{x\in X}\Pi_x|\psi\rangle = \sum_{x\in X}|\psi_x\rangle = |\psi\rangle,$$

即 $\sum_{x\in X}\Pi_x = I$，并且对于 $x \ne y$，有 $\Pi_x\Pi_y = 0$。因此 $\{M_x\}_{x\in X}$ 构成一个 POVM。 ■

注释 29 （粗粒化测量与利普希茨界的保持）。 引理 27 告诉我们，即使每个测量算子 M_x 的秩可能非常高，其算子范数仍然满足 $\|M_x\|_\infty = 1$.因此，在我们之前对利普希茨常数的估计中，如果取 $O = M_x$ 仍有

$$\big|\mathrm{Tr}\big[M_x\,(E_\theta - E_{\theta'})(\rho)\big]\big| \le \|M_x\|_\infty\,\|(E_\theta - E_{\theta'})(\rho)\|_1 \le \|E_\theta - E_{\theta'}\|_{1\to 1},$$

因此 *Lips chitz* 结构不会因测量变得更加粗粒化或具有更高的秩而遭到破坏 k.

在具体设计中，我们还可以进一步选择 $\mathcal{H}$ 使其分解为仅有多项式数量的块，从而避免在近似最大混合态下每个 $P_\theta(x)$ 变得指数小的情况（这正是随机林布拉德算子在典型参数选择下的典型行为）。下面的简单引理阐释了这一思想。

引理 28 （粗粒化投影测量下的概率下界（在近似最大混合假设下））。 考虑一个 n-量子比特系统，其 $\mathcal{H} \simeq (\mathbb{C}^2)^{\otimes n}$ 维数为 $d = 2^n$，并取如下的正交分解，该分解见定义29:

$$\mathcal{H} = \bigoplus_{x\in X}\mathcal{H}_x.$$

假设存在一个多项式 $\kappa(n)$ 使得

$$|X| \le \kappa(n), \qquad \dim\mathcal{H}_x \ge \frac{d}{\kappa(n)} \quad \textit{for all } x \in X.$$

对于每个 θ，令 $\rho_\theta := E_\theta(\rho_{\mathrm{in}})$，并定义输出分布 $P_\theta(x) := \text{迹}\big(M_x\rho_\theta\big)$. 若存在一个常数$\varepsilon_{\mathrm{mix}} > 0$，使得在某个典型参数集上有

$$\big\|\rho_\theta - \tfrac{I}{d}\big\|_1 \le \varepsilon_{\mathrm{mix}},$$

那么对于该集合中的所有 θ 和所有 $x \in X$，

$$\big|P_\theta(x) - \tfrac{\dim\mathcal{H}_x}{d}\big| \le \varepsilon_{\mathrm{mix}}, \tag{10.2}$$

因此，若 $\varepsilon_{\mathrm{mix}} \le \frac{1}{2}\cdot\frac{\text{维数}\mathcal{H}_x}{d}$，

$$P_\theta(x) \;\ge\; \frac{\dim\mathcal{H}_x}{2d} \;\ge\; \frac{1}{2\kappa(n)}, \tag{10.3}$$

也就是说，每个粗粒化结果的概率都有下界 $1/$多项式(n)，并且不会像单比特串情形那样变得指数级小。

证明。 由于 $0 \le M_x \le I$ 和 $\|M_x\|_\infty \le 1$，我们有

$$\big|P_\theta(x) - \tfrac{\dim\mathcal{H}_x}{d}\big| = \big|\mathrm{Tr}\big[M_x(\rho_\theta - \tfrac{I}{d})\big]\big| \le \|M_x\|_\infty\,\big\|\rho_\theta - \tfrac{I}{d}\big\|_1 \le \varepsilon_{\mathrm{mix}}.$$

另一方面，$\mathrm{Tr}(M_x \frac{I}{d}) = $维数$\mathcal{H}_d{}^x$，因此

$$\left|P_\theta(x) - \tfrac{\dim \mathcal{H}_x}{d}\right| \le \varepsilon_{\mathrm{mix}}.$$

如果 $\varepsilon_{\mathrm{mix}} \le \frac{1}{2} \cdot$ 维数$\mathcal{H}_d{}^x$，则

$$P_\theta(x) \ge \tfrac{\dim \mathcal{H}_x}{d} - \varepsilon_{\mathrm{mix}} \ge \tfrac{1}{2} \cdot \tfrac{\dim \mathcal{H}_x}{d}.$$

利用假设 $\dim\mathcal{H}_x \ge d/\kappa(n)$，我们得到

$$P_\theta(x) \ge \frac{1}{2} \cdot \frac{d/\kappa(n)}{d} = \frac{1}{2\kappa(n)}.$$

这就得到了所需的多项式下界。 ■

注释 30 （为什么使用分块投影 POVM，而不是单比特串测量？）。 我们特意将希尔伯特空间分解为正交子空间 $H = \bigoplus_{x\in X} H_x$，并使用分块投影算子$M_x = \Pi_x$ 作为 *POVM* 元素，而不是直接在计算基 $\{|z\rangle\}_{z\in\{0,1\}^n}$ 中逐比特串进行测量，原因有以下几点：

1. 从统计学习和样本复杂度的角度来看，逐比特串进行测量会导致概率呈指数级变小，并使样本复杂度急剧增加。对于一个 n量子比特系统，在计算基测量下，一个典型量子态对每个比特串产生的概率量级为 2^{-n} 。在这种情况下，如果希望在全变差距离下准确学习完整分布，通常需要将每个坐标的分辨率控制在与 2^{-n}相当的水平，这对应于指数级小的容差 η。霍夫丁不等式（见注释 *31*）随后表明，样本复杂度 $T = \Theta\left(\eta^{-2}\log(|X|/\delta_{\mathrm{puf}})\right)$ 会变为指数级。换言之，协议的完备性将依赖于分辨指数级稀有的事件，而这对于任何基于采样的实际实现都是不可行的。

2. 粗粒化分块将概率提升至多项式尺度，使 *Hoeffding* 样本复杂度保持为多项式级。根据定义 *29*，我们将希尔伯特空间分解为子空间 H_x；引理 *28* 表明，对于典型参数，当随机林布拉德算子已将 ρ_θ 充分混合至最大混合态 I/d ，且每个分块都满足 $\dim H_x \ge d/\kappa(n)$，其中 $|X| \le \kappa(n)$ 时，粗粒化结果概率 $P_\theta(x) = \mathrm{Tr}(M_x\rho_\theta)$ 至少为 $1/\mathrm{poly}(n)$。在此设置下，我们可以将 *SQ* 容差τ 固定在常数尺度；选择 $\eta = \tau/|X|$后，*Hoeffding* 样本复杂度 $T = \Theta\left(\eta^{-2}\log(|X|/\delta_{\mathrm{puf}})\right)$仍为 $\mathrm{poly}(|X|) = \mathrm{poly}(n)$。因此，从信息论角度看，在初始化阶段学习概率指纹是可行的，并且我们避免了逐位串测量所导致的指数级样本复杂度。

3. 从复杂性理论视角来看，逐比特串测量对应于学习各个输出比特串的概率，而粗粒化分块测量则对应于估计相对简单的可观测量的期望值。这些问题处于不同的复杂度层级。在随机电路采样等场景中，对于典型的通用量子电路族，加性近似单个输出概率 $p(z) = \Pr[Z = z]$ 与 *#P* 计数问题紧密相关；在标准假设和预言机模型下，近似此类概率属于 *#P* 困难问题，而以全变差距离学习完整输出分布则被广泛认为是一个 *#P* 类型的任务，这一点也体现在随机电路采样的复杂性分析中 *[AA11*、*BFNV19*、*AAB+19]*。相比之下，我们的粗粒化概率

$$P_\theta(x) = \mathrm{Tr}(M_x\rho_\theta)$$

可视为相对简单且可高效实现的投影算符的期望值 M_x。这类期望值可以通过标准量子算法（如哈达玛测试或振幅估计）在有界误差量子多项式时间内近似 *[NC10]*。因此，在理想噪声模型中，学习粗粒化输出分布自然属于有界误差量子多项式时间，而不是“近似单个振幅”这一 *#P* 类问题。

接下来，我们假设 $\{M_x\}_{x\in X}$ 由一个固定的正交分块分解 $\mathcal{H} = \bigoplus_x \mathcal{H}_x$通过分块投影算子诱导，其中 $|X| \le \kappa(n) = \mathrm{poly}(n)$。

令 $\{E_\theta\}_{\theta\in\Theta}$ 为随机 Lindblad 通道族， $\rho_{\mathrm{in}} \in \mathsf{S}(\mathcal{H})$ 为固定输入态，$\{M_x\}_{x\in X}$为由正交分解 $\mathcal{H} = \bigoplus_x \mathcal{H}_x$ 诱导的分块投影测量，如上一小节所述。对于每个 θ，定义输出分布

$$P_\theta(x) := \mathrm{Tr}\big(M_x E_\theta(\rho_{\mathrm{in}})\big), \qquad x \in X.$$

定义 30 (带有 SQ 接口和哈达玛测试函数的 Lindblad-PUF 协议)。 固定统计查询容差参数 $\tau > 0$ 和认证轮次参数 $N_{\mathrm{chal}} \in \mathbb{N}$。验证者 V 与证明者P 之间的协议由两个阶段组成。

初始化阶段（在工厂内进行，具有样本访问权限）。

i. 在制造商实验室中， V 从 μ_Θ 中随机抽取一个参数 θ，从而获得对物理设备的样本级访问权限。在此阶段，制造商可以反复制备 ρ_{in}，通过 $E_\theta := E_\theta$ 使其演化，并使用 $\{M_x\}$进行测量，从而获得独立样本 X_1、X_2、……。

ii. 令 $\eta > 0$ 为指纹的目标逐点精度。验证者 V 运行设备 T 次，以获得独立样本 $X_1, \dots, X_T \in X$，并定义经验频率

$$\hat{P}_\theta(x) := \frac{1}{T}\sum_{t=1}^{T} \mathbf{1}\{X_t = x\} \quad \textit{for each } x \in X.$$

根据霍夫丁不等式（参见备注 *31*），选择

$$T = \Theta\big(\eta^{-2}\log(|X|/\delta_{\mathrm{puf}})\big)$$

可保证我们以至少 $1-\delta_{\mathrm{puf}}$ 的概率有

$$\big|\hat{P}_\theta(x) - P_\theta(x)\big| \le \eta \quad \forall x \in X.$$

在这一高概率事件成立的条件下， V 存储

$$\mathbf{p} := \{\hat{P}_\theta(x)\}_{x\in X}$$

作为设备的概率指纹，并将其保密。在下面的参数选择中，我们将设定

$$\eta := \frac{\tau}{|X|}, \tag{10.4}$$

因此 使用$\mathbf{p}$ 计算任意有界测试函数的期望值时，总误差至多为 τ.
th

iii. 初始化后，制造商会不可逆地禁用内部采样接口，仅保留外部 *SQ* 接口处于活动状态。在密码学模型中，我们将设备抽象为理想统计查询预言机$\mathrm{Stat}_\tau(P_\theta)$ （我们不关心其内部实现方式；它可以通过自身采样来实现该预言机）：对于任意外部查询函数 $\varphi : X \to [-1,1]$，它会返回 v，使得

$$|v - P_\theta[\varphi]| \le \tau.$$

随后，设备被售予最终用户。

认证阶段（使用 *SQ* 接口，限制查表攻击）。

i. 当 P 声称持有一台真实设备时（例如，设备需要维护，制造商受托派遣技术人员）， V 会启动认证。

ii. V首先确定公开编码 $h :\ X \to \{0,1\}^L$，从而确定定义*28*中的哈达玛测试函数族$\mathcal{F}_{\mathrm{Had}}$ 。

iii. 对于 $r = 1、2、\ldots、N_{\mathrm{chal}}$，重复执行以下挑战-响应过程：

A. V 从$\{0,1\}^L$中均匀采样一个比特串$\mathrm{BIT}^{(r)}$，并构造测试函数 $\varphi^{(r)} := \varphi_{\mathrm{BIT}^{(r)}}$。$V$ 使用内部存储的概率指纹$\mathbf{p}$计算

$$u_r := \sum_{x \in X} \varphi^{(r)}(x)\, \hat{P}_\theta(x),$$

它近似于真实的期望

$$P_\theta[\varphi^{(r)}] := \sum_{x \in X} \varphi^{(r)}(x)\, P_\theta(x).$$

由于对于所有 $x \in X$，我们有 $\big|\hat{}P_\theta(x) - P_\theta(x)\big| \le \eta$ 且 $|\varphi^{(r)}(x)| \le 1$，因此可得

$$\big|u_r - P_\theta[\varphi^{(r)}]\big| \le \sum_{x \in X} \big|\hat{P}_\theta(x) - P_\theta(x)\big| \le |X|\,\eta. \tag{10.5}$$

结合参数选择(10.4)，在初始化阶段的高概率事件下，我们有

$$\big|u_r - P_\theta[\varphi^{(r)}]\big| \le \tau.$$

B. V 将比特串$\mathrm{BIT}^{(r)}$ 发送给 P。

C. 诚实证明者 P 使用 $\varphi^{(r)}$ 作为查询函数，查询设备的统计查询接口，以计算$\mathrm{Stat}_\tau(P_\theta)$，并收到满足 $|v_r - P_\theta[\varphi^{(r)}]| \le \tau$的输出 v_r，随后将其返回给 V。

iv. V当且仅当对所有 $r = 1, \ldots, N_{\mathrm{chal}}$ 均成立时，才接受认证，

$$\big|v_r - u_r\big| \le 2\tau. \tag{10.6}$$

参数 2τ 源于三角不等式：其中一部分来自 u_r与 $P_\theta[\varphi^{(r)}]$ 之间的近似误差（见 (10.5) 和 (10.4)），另一部分来自 *SQ* 接口本身的容差 τ。

备注 31 (霍夫丁不等式与初始化阶段的样本复杂度)。 在初始化阶段，验证者 V重复运行设备 T次，获得独立样本 $X_1, \ldots, X_T \in X$，并定义

$$\hat{P}_\theta(x) := \frac{1}{T} \sum_{t=1}^{T} \mathbf{1}\{X_t = x\},$$

它是参数为 $P_\theta(x)$的伯努利随机变量的经验平均值。霍夫丁不等式指出，对任意 $\eta > 0$,

$$\Pr\Big(\big|\hat{P}_\theta(x) - P_\theta(x)\big| > \eta\Big) \le 2\exp(-2T\eta^2).$$

对所有 $x \in X$ 应用并集界可得

$$\Pr\Big(\exists x \in X :\ \big|\hat{P}_\theta(x) - P_\theta(x)\big| > \eta\Big) \le 2|X|\exp(-2T\eta^2).$$

因此，只要

$$T = \Theta\big(\eta^{-2}\log(|X|/\delta_{\mathrm{puf}})\big),$$

我们有

$$\Pr\Big(\big|\hat{P}_\theta(x) - P_\theta(x)\big| \le \eta\ \forall x \in X\Big) \ge 1 - \delta_{\mathrm{puf}}.$$

在此协议中，我们随后固定 $\eta = \tau/|X|$ *(*见 (10.4)*)*，使得使用指纹计算任意测试函数期望值时的总误差 $\mathbf{p}$ 不超过目标统计查询容差 τ。结合引理 *28*，我们可以将 $|X|$ 限制为至多 $\kappa(n)$ =poly(n)，因此上述 T 在 n 的多项式尺度上是可行的。

备注 32 （诚实证明者的完备性与效率）。 对于诚实证明者，设备可通过统计查询接口在内部访问 P_θ，且每次查询仅需 $\Theta(\tau^{-2})$ 个样本即可确保 $|v_r - P_\theta[\varphi^{(r)}]| \le \tau$。另一方面，在初始化阶段，指纹满足 $\left|\hat{}P_\theta(x) - P_\theta(x)\right| \le \eta$，其中 $\eta = \tau/|X|$，因此根据 (10.5) 可得

$$\left|u_r - P_\theta[\varphi^{(r)}]\right| \le |X|\eta = \tau.$$

因此，在每个挑战轮次中，

$$\left|v_r - u_r\right| \le \left|v_r - P_\theta[\varphi^{(r)}]\right| + \left|P_\theta[\varphi^{(r)}] - u_r\right| \le \tau + \tau = 2\tau,$$

因此，诚实证明者以高概率通过全部 N_{chal} 轮。验证者的主要开销为：在初始化阶段，设备需要进行 $T = \Theta\big(\eta^{-2}\log(|X|/\delta_{\text{puf}})\big)$ 次物理运行，其随 $\eta = \tau/|X|$ 增长为 $T = \text{poly}(|X|)$ =poly(n)；在认证阶段，每次挑战仅需 $O(|X|)$ 次经典操作，总开销为$N_{\text{chal}} \cdot \text{poly}(|X|)$。因此，该协议在量子比特数 n 的多项式规模下是可行的。

备注 33 （SQ 视角下的对手能力模型）。 在上述协议中，我们只允许对手在攻击阶段对设备的 *SQ* 接口 $\text{Stat}_\tau(P_\theta)$ 进行至多 q 次查询。此阶段结束后，假设设备已被取回或部署在可信环境中，而对手只能尝试构造一个模拟器，在认证阶段响应验证者的挑战。

因此，安全性分析中对手可用的接口与第 *VII C* 节 *SQ* 学习问题中学习器所用的接口完全相同：在每次查询中，对手只能指定 $\varphi: X \to [-1,1]$ 并获得一个近似的期望值；它既无法看到单个样本，也无法在认证阶段访问物理设备。

为了将“通过认证”这一事件转化为输出分布已被高精度学习的表述，我们需要针对哈达玛测试函数族的完备性引理。

引理 29 （哈达玛测试函数的帕塞瓦尔恒等式）。 将 X 嵌入 $\{0、1\}^L$，所用编码为 h，并定义

$$\chi_{\text{BIT}}(z) := (-1)^{\langle \text{BIT}, z\rangle}, \qquad z \in \{0,1\}^L.$$

对于任意两个分布 $P, Q \in \mathcal{D}_X$，定义它们在 $\{0,1\}^L$ 上的扩展为

$$\widetilde{P}(z) := \begin{cases} P(x), & z = h(x) \text{ for some } x \in X, \\ 0, & \text{otherwise}, \end{cases} \qquad \widetilde{Q} \text{ defined analogously.}$$

于是我们得到帕塞瓦尔型恒等映射

$$\frac{1}{2^L}\sum_{\text{BIT}\in\{0,1\}^L}\Big(P[\varphi_{\text{BIT}}] - Q[\varphi_{\text{BIT}}]\Big)^2 = \|\widetilde{P} - \widetilde{Q}\|_2^2 = \|P - Q\|_2^2. \tag{10.7}$$

证明。在布尔超立方体 $\{0,1\}^L$ 上，族 $\{\chi_{\text{BIT}}\}$ 关于内积 $f, g := 2^{-L}\sum_z f(z)g(z)$ 构成正交归一基（沃尔什–哈达玛基）。因此，对于任意函数 $f: \{0,1\}^L \to \mathbb{R}$，我们有帕塞瓦尔恒等式（傅里叶展开的一个基本事实；参见 [O'D14]）：

$$\frac{1}{2^L}\sum_{\text{BIT}}\Big(\sum_z \chi_{\text{BIT}}(z) f(z)\Big)^2 = \sum_z f(z)^2 = \|f\|_2^2.$$

~ ~取 $f := P - Q$。那么

$$\sum_{z} \chi_{\mathrm{BIT}}(z) f(z) = \sum_{x \in X} \chi_{\mathrm{BIT}}(h(x)) \big(P(x) - Q(x)\big) = \sum_{x \in X} \varphi_{\mathrm{BIT}}(x) \big(P(x) - Q(x)\big) = P[\varphi_{\mathrm{BIT}}] - Q[\varphi_{\mathrm{BIT}}],$$

因此

$$\frac{1}{2^L} \sum_{\mathrm{BIT} \in \{0,1\}^L} \Big(P[\varphi_{\mathrm{BIT}}] - Q[\varphi_{\mathrm{BIT}}]\Big)^2 = \sum_{z} f(z)^2 = \|\widetilde{P} - \widetilde{Q}\|_2^2.$$

另一方面，由于仅当存在某个 $x \in X$ 使得 $f(z) \neq 0$ 仅当 $z = h(x)$ 时，我们有

$$\|\widetilde{P} - \widetilde{Q}\|_2^2 = \sum_{z} f(z)^2 = \sum_{x \in X} \big(\widetilde{P}(h(x)) - \widetilde{Q}(h(x))\big)^2 = \sum_{x \in X} \big(P(x) - Q(x)\big)^2 = \|P - Q\|_2^2.$$

结合这两个恒等式即可得到该结论。 ■

引理 30（从多轮 Hadamard 认证成功到单轮预测准确率）。 固定一个参数 θ，并令 $P_\theta \in D_X$ 为相应的目标分布。假设对手在认证阶段的模拟器为

$$w : \{0,1\}^L \to \mathbb{R}, \qquad \mathrm{BIT} \mapsto w(\mathrm{BIT}),$$

且验证者的目标值为

$$u(\mathrm{BIT}) := \sum_{x \in X} \varphi_{\mathrm{BIT}}(x)\, \hat{P}_\theta(x),$$

ˆ其中指纹 P_θ 满足

$$\big|\hat{P}_\theta(x) - P_\theta(x)\big| \leq \eta_{\mathrm{fp}} \quad \forall x \in X.$$

因此，对于所有测试函数，我们有

$$\big|u(\mathrm{BIT}) - P_\theta[\varphi_{\mathrm{BIT}}]\big| \leq |X| \eta_{\mathrm{fp}}.$$

假设协议使用常数 $C_0 > 0$（在我们的协议中取 $C_0 = 2$），且接受条件为：在每一轮 $r = 1, \ldots, N_{\mathrm{chal}}$，

$$\big|w(\mathrm{BIT}^{(r)}) - u(\mathrm{BIT}^{(r)})\big| \leq C_0 \tau.$$

Let

$$\Delta_\theta(\mathrm{BIT}) := w(\mathrm{BIT}) - P_\theta[\varphi_{\mathrm{BIT}}],$$

并假设指纹参数满足

$$|X| \eta_{\mathrm{fp}} \leq \tau,$$

因此，事件“协议在本轮拒绝”等价于

$$\big|\Delta_\theta(\mathrm{BIT})\big| > (C_0 + 1)\tau \quad \Longrightarrow \quad \big|w(\mathrm{BIT}) - u(\mathrm{BIT})\big| > C_0 \tau.$$

如果在此接受规则下，通过全部 N_{chal} 轮次的概率满足

$$\Pr_{\mathrm{chal}}\big[\textit{all } N_{\mathrm{chal}} \textit{ rounds are accepted}\big] \;\geq\; \alpha_0,$$

其中 $\Pr_{\text{chal}}$ 仅对 $\text{BIT}^{(1)}$、…、$\text{BIT}^{(N_{\text{chal}})}$ 的独立一致抽样取平均（将 w 视为确定量），那么对于均匀随机的 $\text{BIT} \sim \text{Unif}(\{0,1\}^L)$，有

$$\Pr\Big(\big|\Delta_\theta(\text{BIT})\big| > (C_0+1)\tau\Big) \;\le\; \delta_{\text{Had}}, \qquad \delta_{\text{Had}} := 1 - \alpha_0^{1/N_{\text{chal}}}. \tag{10.8}$$

换言之，如果对手能够以至少α_0 的总体成功概率通过 N_{chal} 个随机挑战（其中 α_0 接近1），那么对于几乎所有挑战BIT，对手的预测 $w(\text{BIT})$ 都必须在误差$(C_0+1)\tau$以内逼近$P_\theta[\varphi_{\text{BIT}}]$。

证明。 令“坏”的挑战比特串集合为

$$B_\theta := \Big\{\text{BIT} :\; \big|\Delta_\theta(\text{BIT})\big| > (C_0+1)\tau\Big\}, \qquad p_\theta := \Pr_{\text{BIT}\sim\text{Unif}}[\text{BIT} \in B_\theta].$$

利用假设 $|X|\eta_{\text{fp}} \le \tau$ 和三角不等式，对于任意 BIT，我们得到：

$$\big|w(\text{BIT}) - u(\text{BIT})\big| \ge \big|\Delta_\theta(\text{BIT})\big| - \big|u(\text{BIT}) - P_\theta[\varphi_{\text{BIT}}]\big| > (C_0+1)\tau - \tau = C_0\tau.$$

因此，若某一轮的挑战比特串属于 B_θ，则该轮必然失败。因此，“所有 N_{chal} 轮均被接受”这一事件包含于“没有一个 N_{chal} 挑战比特串属于 B_θ”这一事件之中。由于不同轮次中的挑战比特串独立同分布，我们有

$$\Pr_{\text{chal}}[\text{all } N_{\text{chal}} \text{ rounds are accepted}] \;\le\; \Pr\big[\text{BIT}^{(1)},\dots,\text{BIT}^{(N_{\text{chal}})} \notin B_\theta\big] = (1-p_\theta)^{N_{\text{chal}}}.$$

根据假设 $\Pr_{\text{chal}}$[所有轮次均被接受] $\ge \alpha_0$，可得

$$(1-p_\theta)^{N_{\text{chal}}} \ge \alpha_0, \quad p_\theta \le 1 - \alpha_0^{1/N_{\text{chal}}} =: \delta_{\text{Had}}.$$

但是， p_θ 恰好等于$\Pr_{\text{BIT}}\big(|\Delta_\theta(\text{BIT})| > (C_0+1)\tau\big)$，因此得到（10.8）。 ■

引理 31 （根据哈达玛测试预测重构近似分布）。 设 X 为一个有限集， $P \in \mathcal{D}_X$ 为一个目标分布，并且 $\{\varphi_{\text{BIT}}\}_{\text{BIT}\in\{0,1\}^L}$ 为定义 28中的哈达玛测试函数族。设 $w:\ \{0,1\}^L \to \mathbb{R}$ 为任意函数（例如对手的模拟器的输出），并假设对于某个 $\kappa_* > 0$ 我们有

$$\mathbb{E}_{\text{BIT}\sim\text{Unif}}\Big[\big(w(\text{BIT}) - P[\varphi_{\text{BIT}}]\big)^2\Big] \;\le\; \kappa_*^2. \tag{10.9}$$

那么存在一个分布 $D \in \mathcal{D}_X$ 使得

$$d_{\text{TV}}(P, D) \;\le\; \sqrt{|X|}\,\kappa_*. \tag{10.10}$$

证明。 对于任意 $D \in \mathcal{D}_X$，考虑

$$G(D) \;:=\; \mathbb{E}_{\text{BIT}\sim\text{Unif}}\Big[\big(w(\text{BIT}) - D[\varphi_{\text{BIT}}]\big)^2\Big].$$

该映射

$$\mathcal{D}_X \ni D \;\mapsto\; \big(D[\varphi_{\text{BIT}}]\big)_{\text{BIT}\in\{0,1\}^L} \in \mathbb{R}^{2^L}$$

是连续的，并且 $\mathcal{D}_X$ 在 ℓ_2 拓扑下是紧致的。因此 $G(D)$ 在 $\mathcal{D}_X$上达到其最小值：存在$D^\star \in \mathcal{D}_X$ 使得

$$D^\star := \arg\min_{D\in\mathcal{D}_X} G(D).$$

在证明中，我们只需要 $D^\star$ 的存在性。若确实想要重构一个分布，则无需显式求解这个最小化问题。最直接的算法是应用逆沃尔什–哈达玛变换

，得到 w 一个向量，然后将该向量投影到概率单纯形上（投影过程可见 [WCP13]）。我们简要说明，这种构造过程所得的结果等价于取一个极小化元 $D^\star$；极小化元情形的推导见下文。令 $\tilde{p}$ 为通过逆变换得到的向量；根据引理29，有 $\mathbb{E}_{\mathrm{BIT}}\Big[\big(w_{\theta,\,R}(\mathrm{BIT}) - F_{P_\theta}(\mathrm{BIT})\big)^2\Big] = \big\|\tilde{p} - \tilde{P}_\theta\big\|_2^2 \le \kappa_{*\circ}^2$ 由于投影到凸集不会增大 ℓ_2 距离（$\|\Pi_C(a) - \Pi_C(b)\|_2 \le \|a-b\|_2$），若将投影后的分布记为 D_{pro}，则 $d_{\mathrm{TV}}(P_\theta,\ D_{\mathrm{pro}}) \le \frac{1}{2}\sqrt{|X|}\|P_\theta - D_{\mathrm{pro}}\|_2 \le \frac{1}{2}\sqrt{|X|}\kappa_{*\circ}$

现在回到极小化元 $D^\star$ 的情形。由于 P 也是一个候选分布，因此最小值不会大于在 P 处的取值，即

$$\mathbb{E}_{\mathrm{BIT}}\Big[\big(w(\mathrm{BIT}) - D^\star[\varphi_{\mathrm{BIT}}]\big)^2\Big] \;\le\; \mathbb{E}_{\mathrm{BIT}}\Big[\big(w(\mathrm{BIT}) - P[\varphi_{\mathrm{BIT}}]\big)^2\Big] \;\le\; \kappa_*^2, \tag{10.11}$$

其中最后一个不等式由假设（10.9）可得。

对于每个 $\mathrm{BIT} \in \{0,\ 1\}^L$，定义

$$\Delta(\mathrm{BIT}) \;:=\; D^\star[\varphi_{\mathrm{BIT}}] - P[\varphi_{\mathrm{BIT}}].$$

Let

$$a(\mathrm{BIT}) := D^\star[\varphi_{\mathrm{BIT}}] - w(\mathrm{BIT}), \qquad b(\mathrm{BIT}) := w(\mathrm{BIT}) - P[\varphi_{\mathrm{BIT}}],$$

于是对于每个 BIT，有

$$\Delta(\mathrm{BIT}) = a(\mathrm{BIT}) + b(\mathrm{BIT}).$$

对于任意实数 a，b，不等式 $(a+b)^2 \le 2a^2 + 2b^2$ 成立，因此对于每个 BIT，

$$\Delta(\mathrm{BIT})^2 \le 2\,a(\mathrm{BIT})^2 + 2\,b(\mathrm{BIT})^2.$$

对一致随机 BIT取期望，并利用（10.9）和（10.11），可得

$$\mathbb{E}_{\mathrm{BIT}}[\Delta(\mathrm{BIT})^2] \;\le\; 2\,\mathbb{E}_{\mathrm{BIT}}\big[a(\mathrm{BIT})^2\big] + 2\,\mathbb{E}_{\mathrm{BIT}}\big[b(\mathrm{BIT})^2\big] \;\le\; 4\kappa_*^2. \tag{10.12}$$

另一方面，将引理 29 应用于 P 和 $D^\star$，其中 $Q{:}\;= D^\star$，可得

$$\frac{1}{2^L}\sum_{\mathrm{BIT}\in\{0,1\}^L}\big(P[\varphi_{\mathrm{BIT}}] - D^\star[\varphi_{\mathrm{BIT}}]\big)^2 = \|\widetilde{P} - \widetilde{D}^\star\|_2^2 = \|P - D^\star\|_2^2.$$

左侧恰好为 $\mathbb{E}_{\mathrm{BIT}}[\Delta(\mathrm{BIT})^2]$,因此

$$\|P - D^\star\|_2^2 = \mathbb{E}_{\mathrm{BIT}}[\Delta(\mathrm{BIT})^2].$$

将此与（10.12）结合，得到

$$\|P - D^\star\|_2^2 \le 4\kappa_*^2, \qquad \text{and hence} \qquad \|P - D^\star\|_2 \le 2\kappa_*.$$

最后，由柯西–施瓦茨不等式，

$$d_{\mathrm{TV}}(P, D^\star) = \frac{1}{2}\|P - D^\star\|_1 \le \frac{1}{2}\sqrt{|X|}\,\|P - D^\star\|_2 \le \frac{1}{2}\sqrt{|X|}\cdot 2\kappa_* = \sqrt{|X|}\,\kappa_*.$$

令 $D := D^\star$ 即可完成证明。 ■

定理 18（具有 SQ 接口的 Hadamard 型 Lindbladian-PUF 的统计查询复杂度安全性）。考虑定义 *30*中的协议，它使用与第 *VIIC* 节统计查询困难性定理中相同的随机 *Lindblad* 算子系综。设 A 是任意一个（可能经过随机化的）对手，它在攻击阶段可以查询

设备的 *SQ* 接口 $\mathrm{Stat}_\tau(P_\theta)$ 至多 q 次（即最多进行 q 次统计查询），然后尝试构造一个模拟器（经典或量子），以回答认证阶段的所有挑战。

验证者在认证过程中执行 N_{chal} 轮相互独立的随机哈达玛测试。我们将N_{chal} 视为安全参数。根据标准的重复与放大论证，如果每轮的可靠性误差为常数，那么要将总体认证错误概率降至 δ_{auth}，只需取$N_{\mathrm{chal}} = \Theta(\log(1/\delta_{\mathrm{auth}}))$。下文中，我们直接使用记号 $\Theta(\log(1/\delta_{\mathrm{auth}}))$ 来强调这种缩放关系，而不固定常数。

假设存在常数 $\alpha > 1/2$ 和 $\beta > 0$，使得

$$\mu_\Theta\Big(\theta : \Pr_{\substack{\text{over adversary}\\ \text{and protocol randomness}}}\big[A \text{ is accepted in the authentication phase}\big] \geq \alpha\Big) \;\geq\; \beta.$$

那么，对于充分大的参数维数 M，存在常数 $c > 0$，使得

$$q \;\geq\; \exp(cM), \tag{10.13}$$

也就是说，就统计查询复杂度而言，对手必须发出指数多的统计查询，才能以不可忽略的成功概率攻破这一 *Lindbladian-PUF*协议。

证明。 为避免符号混淆，我们记

$$\alpha_{\mathrm{auth}} := \alpha, \qquad \beta_{\mathrm{auth}} := \beta$$

定理假设中出现的两个常数，它们分别描述认证成功概率以及“良好”参数的测度。它们是协议安全性的参数，稍后将与统计查询困难性定理中的 $(\alpha_{\mathrm{learn}}, \beta_{\mathrm{learn}})$ 联系起来。

步骤 *0*：为指纹确定“优良事件”。 在初始化阶段，制造商使用霍夫丁不等式（备注 31）选择足够大的样本量，使得指纹 $\hat{} \; P_\theta$ 满足

$$\big|\hat{P}_\theta(x) - P_\theta(x)\big| \leq \eta_{\mathrm{fp}} = \frac{\tau}{|X|} \quad \forall x \in X$$

其发生概率至少为 $1 - \delta_{\mathrm{puf}}$。下文中，我们始终在以此“优良事件”为条件的情况下进行讨论，并将δ_{puf} 计入总体认证错误概率 δ_{auth}；之后不再明确写出它。

在此优良事件下，对于所有哈达玛测试函数，我们都有

$$\big|u(\mathrm{BIT}) - P_\theta[\varphi_{\mathrm{BIT}}]\big| \leq \sum_{x\in X} |\varphi_{\mathrm{BIT}}(x)|\,\big|\hat{P}_\theta(x) - P_\theta(x)\big| \leq |X|\eta_{\mathrm{fp}} = \tau.$$

步骤 *1*：从较高的总体认证成功率得到单轮哈达玛预测的 L_2 界。定义“优良参数集”

$$\Theta_{\mathrm{good}} := \Big\{\theta : \Pr_{\substack{\text{over adversary}\\ \text{and protocol randomness}}}\big[A \text{ is accepted in the authentication phase}\big] \geq \alpha_{\mathrm{auth}}\Big\}.$$

根据定理假设，

$$\mu_\Theta(\Theta_{\mathrm{good}}) \;\geq\; \beta_{\mathrm{auth}}.$$

也就是说，对于至少 β_{auth} 比例的参数 θ，对手的总体成功概率——在其内部随机性、SQ 预言机的随机性以及认证挑战上进行测量——至少为 α_{auth}。

现在固定任意一个 $\theta \in \Theta_{\mathrm{good}}$。为区分攻击阶段的随机性与认证阶段的随机性，令

R =表示对手的内部随机数与攻击阶段 SQ 预言机响应的联合随机种子。

对于每个固定的 R，我们有：

1. 攻击阶段结束后，对手输出一个确定性模拟器

$$w_{\theta,R} : \{0,1\}^L \to \mathbb{R}, \qquad \mathrm{BIT} \mapsto w_{\theta,R}(\mathrm{BIT}).$$

2. 在认证阶段，唯一剩下的随机性在于该模拟器能否通过随机挑战比特串 $\mathrm{BIT}^{(1)}, \ldots, \mathrm{BIT}^{(N_{\mathrm{chal}})}$。

对于每个固定的 (θ, R)，定义

$$\mathrm{acc}_\theta(R) := \Pr_{\mathrm{chal}}\Big[\text{all } N_{\mathrm{chal}} \text{ rounds are accepted}\Big],$$

其中 $\Pr_{\mathrm{chal}}$ 仅对随机挑战比特串和验证者的随机性取平均。另一方面，定理假设中的整体认证成功概率可写为

$$\Pr_{\substack{\text{over adversary} \\ \text{and protocol randomness}}} \big[A \text{ is accepted in the authentication phase}\big] = \mathbb{E}_R\big[\mathrm{acc}_\theta(R)\big] \geq \alpha_{\mathrm{auth}} \qquad \forall\, \theta \in \Theta_{\mathrm{good}}.$$

为了将“均值至少为 α_{auth}”这一陈述转化为“对于大多数种子 R，接受概率不会太小”这一陈述，我们引入一个可自由选择的阈值。这里取

$$\alpha_0 := \frac{2\alpha_{\mathrm{auth}} - 1}{2},$$

因此，$1/2 < \alpha_{\mathrm{auth}} \leq 1$ 蕴含 $\alpha_0 \in (0, 1/2] \subset (0, 1)$。定义

$$G_\theta := \{R : \ \mathrm{acc}_\theta(R) \geq \alpha_0\}.$$

由于 $0 \leq \mathrm{acc}_\theta(R) \leq 1$，我们有

$$\alpha_{\mathrm{auth}} \leq \mathbb{E}_R[\mathrm{acc}_\theta(R)] \leq \Pr[R \in G_\theta] \cdot 1 + \Pr[R \notin G_\theta] \cdot \alpha_0.$$

因此

$$\begin{aligned} \Pr[R \in G_\theta] &\geq \frac{\alpha_{\mathrm{auth}} - \alpha_0}{1 - \alpha_0} \\ &= \frac{\alpha_{\mathrm{auth}} - \frac{2\alpha_{\mathrm{auth}} - 1}{2}}{1 - \frac{2\alpha_{\mathrm{auth}} - 1}{2}} \\ &= \frac{1}{3 - 2\alpha_{\mathrm{auth}}} \ =: p_0. \end{aligned}$$

由于 $\alpha_{\mathrm{auth}} > 1/2$，我们有 $3 - 2\alpha_{\mathrm{auth}} < 2$，因此

$$p_0 = \frac{1}{3 - 2\alpha_{\mathrm{auth}}} > \frac{1}{2}.$$

也就是说，对于每个固定的优良参数 $\theta \in \Theta_{\mathrm{good}}$，至少有 $p_0 > 1/2$ 比例的随机种子 R 满足 $\mathrm{acc}_\theta(R) \geq \alpha_0$。

现在固定这样一个 θ 和某个 $R \in G_\theta$。在这些条件下，模拟器 $w_{\theta,\, R}$ 是确定性的，并且其在 N_{chal} 个认证轮次中的总体成功概率至少为 α_0，即

$$\Pr_{\mathrm{chal}}\big[\text{all } N_{\mathrm{chal}} \text{ rounds are accepted}\big] = \mathrm{acc}_\theta(R) \geq \alpha_0.$$

由于我们事先没有限制对手输出的取值范围，因此可以采用一个简单的截断操作：如果 $w_{\theta,\, R}(\mathrm{BIT})$ 落在区间 $[-1, 1]$ 之外，验证者就可以将其截断至 $[-1, 1]$，然后再检查接受条件。这只会减小 $|w_{\theta,\, R}(\mathrm{BIT}) - u(\mathrm{BIT})|$，因此不会降低对手的接受概率。因此，不失一般性，我们可以假设

$$w_{\theta,R}(\mathrm{BIT}) \in [-1, 1] \quad \text{for all BIT}.$$

在良好指纹事件发生时，对于所有测试函数，我们都有 $|u(\mathrm{BIT}) - P_\theta[\varphi_{\mathrm{BIT}}]| \le \tau$。令

$$\Delta_\theta(\mathrm{BIT}) := w_{\theta,R}(\mathrm{BIT}) - P_\theta[\varphi_{\mathrm{BIT}}],$$

那么，每当 $|\Delta_\theta(\mathrm{BIT})| > (C_0+1)\tau$ 时，我们就有

$$\big|w_{\theta,R}(\mathrm{BIT}) - u(\mathrm{BIT})\big| \ge \big|\Delta_\theta(\mathrm{BIT})\big| - \big|u(\mathrm{BIT}) - P_\theta[\varphi_{\mathrm{BIT}}]\big| > (C_0+1)\tau - \tau = C_0\tau,$$

因此该轮必然失败。应用引理 30，对于均匀随机的 $\mathrm{BIT} \sim \mathrm{Unif}(\{0,1\}^L)$，

$$\Pr\Big(\big|\Delta_\theta(\mathrm{BIT})\big| > (C_0+1)\tau\Big) \le \delta_{\mathrm{Had}}, \qquad \delta_{\mathrm{Had}} := 1 - \alpha_0^{1/N_{\mathrm{chal}}}. \tag{10.14}$$

另一方面，由于 $w_{\theta,\,R}(\mathrm{BIT}) \in [-1,1]$ 且 $P_\theta[\varphi_{\mathrm{BIT}}] \in [-1,1]$，因此对于所有 BIT，我们有 $|\Delta_\theta(\mathrm{BIT})| \le 2$。将二阶矩拆分为“好”和“坏”事件，可得

$$\begin{aligned}
\mathbb{E}_{\mathrm{BIT}}\big[\Delta_\theta(\mathrm{BIT})^2\big] &= \mathbb{E}\big[\Delta_\theta^2 \mathbf{1}_{|\Delta_\theta| \le (C_0+1)\tau}\big] + \mathbb{E}\big[\Delta_\theta^2 \mathbf{1}_{|\Delta_\theta| > (C_0+1)\tau}\big] \qquad (10.15)\\
&\le (C_0+1)^2\tau^2 + 4\,\Pr\big(|\Delta_\theta| > (C_0+1)\tau\big)\\
&\le (C_0+1)^2\tau^2 + 4\,\delta_{\mathrm{Had}}\\
&=: \kappa_{\mathrm{Had}}^2. \qquad (10.16)
\end{aligned}$$

步骤 2：通过逆变换和投影进行重构；获得总变差近似。 对于每个固定的$(\theta,\ R)$，应用引理 31 ，其中

$$P := P_\theta, \qquad w := w_{\theta,R},$$

并在 (10.16) 中设定 $\kappa = \kappa_{\mathrm{Had}}$。该引理保证存在一个分布 $D_{\theta,\ R} \in \mathcal{D}_X$ ，使得

$$d_{\mathrm{TV}}(P_\theta, D_{\theta,R}) \le \frac{1}{2}\sqrt{|X|}\,\kappa_{\mathrm{Had}} =: \varepsilon_{\mathrm{SQ}}. \tag{10.17}$$

分布 $D_{\theta,\ R}$ 仅通过模拟器 $w_{\theta,\ R}$ 经由重构过程获得（见引理 31），且不需要额外的 SQ 查询。

如上所述，对于每个 $\theta \in \Theta_{\mathrm{good}}$， R 属于 G_θ 的概率至少为 p_0，其中

$$p_0 = \frac{1}{3 - 2\alpha_{\mathrm{auth}}} > \frac{1}{2}.$$

对于这些“良好种子”，等式（10.17）成立；对于 $R \notin G_\theta$ ，我们不作任何保证。因此，对于每个 $\theta \in \Theta_{\mathrm{good}}$，

$$\Pr_R\Big(d_{\mathrm{TV}}(P_\theta, D_{\theta,R}) \le \varepsilon_{\mathrm{SQ}}\Big) \ge p_0.$$

现在我们可以构造一个统计查询学习器 $\mathcal{L}^{\mathrm{SQ}}$。在可访问 $\mathsf{Stat}_\tau(P_\theta)$ 的情况下，$\mathcal{L}^{\mathrm{SQ}}$ 按如下方式进行：

1. 它将对手 A 作为子程序，并完整模拟攻击阶段。 A发出的每个 SQ 查询都会转发给 $\mathsf{Stat}_\tau(P_\theta)$，然后将响应返回给 A。攻击阶段结束时，$\mathcal{L}^{\mathrm{SQ}}$ 获得模拟器 $w_{\theta,\ R}$。

2. 使用引理 31 中的重构过程，$\mathcal{L}^{\mathrm{SQ}}$ 根据 $w_{\theta,\ R}$ 计算出 $D_{\theta,\ R}$ ，并输出 $D_{\theta,\ R}$。

在此过程中，$\mathcal{L}^{\mathrm{SQ}}$ 恰好调用 $\mathsf{Stat}_\tau(P_\theta)$ q 次，与对手在攻击阶段发出的 SQ 查询数量相同。重构步骤纯粹是经典后处理，不涉及额外的 SQ 查询。

因此，对于随机的 $\theta \sim \mu_\Theta$，

1. 对所有 $\theta \in \Theta_{\mathrm{good}}$，学习器（相对于其内部随机性 R）的成功概率至少为 $p_0 > 1/2$；

2. 对于 $\theta \notin \Theta_{\mathrm{good}}$，不作任何保证。

按照第 VIIC 节中对外层（参数）和内层（随机性）概率的记法，我们设定

$$\alpha_{\text{learn}} := p_0 = \frac{1}{3-2\alpha_{\text{auth}}} > \frac{1}{2}, \qquad \beta_{\text{learn}} := \beta_{\text{auth}},$$

使得

$$\mu_\Theta\Big(\theta : \Pr_{\text{over learner randomness}}\big[d_{\text{TV}}(P_\theta, D_{\theta,R}) \le \varepsilon_{\text{SQ}}\big] \ge \alpha_{\text{learn}}\Big) \ \ge \ \beta_{\text{learn}}.$$

这恰好是随机林德布拉德算子平均情形 SQ 困难性定理所要求的 $(\alpha_{\text{learn}}, \beta_{\text{learn}})$ 结构，并且我们已确保 $\alpha_{\text{learn}} > 1/2$。

步骤 *3*：调用随机林德布拉德算子的 *SQ* 困难性下界。第 VIIC 节中的 SQ 困难性定理指出，对于由随机林德布拉德算子系综诱导的分布族 $\{P_\theta\}$，如果存在一个 SQ 学习算法，其使用至多 q 次查询，且准确率参数为常数 ε_{SQ}，并以如上所述的参数 $(\alpha_{\text{learn}}, \beta_{\text{learn}})$ 成功，那么对于充分大的参数维数 M，必有

$$q \ \ge \ \exp(cM)$$

对于某个常数 $c > 0$，它仅取决于 $(\varepsilon_{\text{SQ}}, \alpha_{\text{learn}}, \beta_{\text{learn}})$，且与 M 无关。

根据步骤 2，我们构造了这样一个 SQ 学习算法 $\mathcal{L}^{\text{SQ}}$，其查询复杂度恰好等于对手在攻击阶段使用的 SQ 查询数量 q。因此，同一下界也适用于对手：如果存在一个对手能够达到定理中的参数 $(\alpha_{\text{auth}}, \beta_{\text{auth}})$，那么必然有

$$q \ \ge \ \exp(cM).$$

这与对手仅使用 $q = \text{poly}(M)$ SQ 查询即可通过认证且成功概率不可忽略的假设相矛盾。因此，当 M 足够大时，任何仅进行多项式次 SQ 查询的对手都无法攻破定义 30 中参数为 (α, β) 的协议，正如该定理所述。定理得证。 ■

注 34 （关于 α_{auth} 与 α_{learn}之间的关系）。 在上述归约中，认证参数$(\alpha_{\text{auth}}, \beta_{\text{auth}})$ 定义为

$$\mu_\Theta\Big(\theta : \Pr_{\substack{\textit{over adversary}\\ \textit{and protocol randomness}}}\big[A \textit{ is accepted in the authentication phase}\big] \ge \alpha_{\text{auth}}\Big) \ \ge \ \beta_{\text{auth}},$$

w而在统计查询困难性定理中，参数 $(\alpha_{\text{learn}}, \beta_{\text{learn}})$ 指的是学习成功 *s:*

$$\mu_\Theta\Big(\theta : \Pr_{\textit{over learner randomness}}\big[d_{\text{TV}}(P_\theta, D_{\theta,R}) \le \varepsilon_{\text{SQ}}\big] \ge \alpha_{\text{learn}}\Big) \ \ge \ \beta_{\text{learn}}.$$

它们之间的联系通过自由选择的中间阈值 α_0 建立：对于固定的优良参数 $\theta \in \Theta_{\text{good}}$，我们知道 $\mathbb{E}_R[\text{acc}_\theta(R)] \ge \alpha_{\text{auth}}$。对于任意选择的 $\alpha_0 \in (0, 2\alpha_{\text{auth}} - 1)$，我们可以使用

$$\Pr[R \in G_\theta] \ge \frac{\alpha_{\text{auth}} - \alpha_0}{1 - \alpha_0}$$

从而得到 α_{learn} 的不同取值。在本文中，我们选择

$$\alpha_0 := \frac{2\alpha_{\text{auth}} - 1}{2},$$

由此得到

$$\alpha_{\text{learn}} := \Pr_R\big[\textit{learning succeeds}\big] \ge \Pr[R \in G_\theta] = \frac{1}{3-2\alpha_{\text{auth}}} > \frac{1}{2},$$

严格满足统计查询困难性定理的要求 $\alpha_{\text{learn}} > 1/2$。我们看到，这一选择仅利用了

事实 $\alpha_{\text{auth}} > 1/2$，且不依赖对手 A 的任何内部细节。选择 α_0 的自由度本质上是一个松弛参数，使我们能够在统计查询框架中方便地将认证成功概率映射为学习成功概率。

备注 35（对手模型的完全一般性及排除查表攻击）。在定理 18中，我们不对对手 A的内部结构施加任何限制：A 可以是复杂度和内存资源均不受限制的任意经典或量子算法。唯一的约束是，在攻击阶段，对 *SQ* 接口 $\mathrm{Stat}_\tau(P_\theta)$ 的查询次数不超过 q。因此，就统计查询复杂度而言，该安全性结论是信息论意义上的：只要 $q = \mathrm{poly}(M)$，无论 A 如何计算、存储数据，或是否使用量子存储器，都无法利用定理中的 (α, β) 参数进行伪造。

B. 扩展的 QPStat 模型与层析基

现在我们转向信道级验证方案。为了在有限维线性代数框架内更方便地使用 QPStat 接口，我们先作一个温和的形式扩展，然后在算子空间上构造层析基及其对应的层析指纹。

定义 31（扩展 QPStat 预言机）。设 $E : B(H) \to B(H)$ 是作用于有限维希尔伯特空间 $H \simeq \mathbb{C}^d$上的完全正迹保持信道。其扩展 *QPStat* 预言机记为 QPStat_E，输入一个三元组

$$(\sigma, O, \tau),$$

其中 $\sigma \in B(H)$ 是厄米的，且具有 $\|\sigma\|_1 \le 1$；$O \in B(H)$ 是厄米的，且具有 $\|O\|_\infty \le 1$；$\tau > 0$ 是一个容差参数。该预言机输出一个实数 α，满足

$$\left|\alpha - \mathrm{Tr}[O\, E(\sigma)]\right| \le \tau. \tag{10.18}$$

QPStat 学习算法至多可以自适应地调用该预言机 q 次；我们称其使用了 q 次 *QPStat* 查询，精度为 τ。

备注 36。在第 VE节中，我们在物理态 $\rho \in \mathsf{S}(\mathcal{H})$ 上定义了 *QPStat* 预言机。然而，在引理 16、5 和定理 12的证明中，所使用的唯一性质是 $\|\rho\|_1 \le 1$ 和 $\|O\|_\infty \le 1$，以及 *CPTP* 映射的迹范数收缩性和一些标准范数不等式；我们从未使用正性$\rho \ge 0$。因此，如果将 ρ 替换为任意厄米算子 σ，且满足 $\|\sigma\|_1 \le 1$，这些结果仍然成立。定义 31只是将这一扩展形式化。

现在我们 在算子空间 $\mathcal{B}(\mathcal{H})$ 和可观测量空间上构造显式的层析基。

引理 32(关于 算子空间上的层析基**)**。设 $\mathcal{H} \simeq \mathbb{C}^d$ 且 $D := d^2$。存在有限个族 *es*

$$\{F_j\}_{j=1}^{D} \subset \mathcal{B}(\mathcal{H}), \qquad \{G_k\}_{k=1}^{D} \subset \mathcal{B}(\mathcal{H}),$$

使得：

1. 每个 F_j 和 G_k 都是厄米的。
2. $\{F_j\}_{j=1}^{D}$ 构成厄米算子空间 $B_{\mathrm{Herm}}(H)$的实线性基；$\{G_k\}_{k=1}^{D}$同理。
3. 存在常数 $C_1, C_\infty > 0$（仅取决于 d），使得

$$\|F_j\|_1 \le C_1, \qquad \|G_k\|_\infty \le C_\infty \quad \textit{for all } j, k.$$

证明。取$\{H_\mu\}_{\mu=1}^{D}$ 为厄米算子的希尔伯特–施密特正交归一基，例如当 $d = 2^N$ 时取归一化泡利基，一般情况下取广义盖尔-曼基。由于厄米算子空间的实维数为 D，这样的基总是存在的。

设 $F_j := \gamma_1^{-1} H_j$ 和 $G_k := \gamma_\infty^{-1} H_k$，其中 γ_1，$\gamma_\infty > 0$ 选取为满足

$$\|H_j\|_1 \le \gamma_1, \qquad \|H_k\|_\infty \le \gamma_\infty \quad \text{for all } j,k.$$

由于有限维空间中只有有限多个基元素，定义 γ_1 和 γ_∞ 的最大值存在且有限。族$\{F_j\}$ 和$\{G_k\}$ 仍然是厄米算子空间的基，并且

$$\|F_j\|_1 = \gamma_1^{-1}\|H_j\|_1 \le 1, \qquad \|G_k\|_\infty = \gamma_\infty^{-1}\|H_k\|_\infty \le 1.$$

取 $C_1 := 1$ 和 $C_\infty := 1$ 即可得到所需的界。 ■

对于任意线性映射（超算子） $T : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$，我们使用上述基定义其层析指纹。

定义 32（层析指纹映射）。 设 $\{F_j\}_{j=1}^{D}$ 和 $\{G_k\}_{k=1}^{D}$ 如引理 *32*所述。定义线性映射

$$\mathcal{T} : \mathrm{End}(\mathcal{B}(\mathcal{H})) \longrightarrow \mathbb{R}^{D\times D}$$

by

$$\big[\mathcal{T}(T)\big]_{k,j} := \mathrm{Tr}\big[G_k\, T(F_j)\big], \qquad 1 \le k,j \le D. \tag{10.19}$$

对于 *CPTP* 信道 E，我们称 $\mathcal{T}(E)$ 为其层析指纹矩阵。

引理 33（单射性与范数等价）。 定义 $\mathcal{T}$ 中的映射 *32* 是实线性单射。因此，

$$\|T\|_{\mathrm{tom}} := \max_{1\le k,j\le D} \big|\big[\mathcal{T}(T)\big]_{k,j}\big| \tag{10.20}$$

*de*在有限维实向量空间End($\mathcal{B}(H)$上定义一个范数（层析范数）).

此外，由于有限维向量空间上的任意两个范数都等价，因此存在常数$C_\diamond > 0$ （仅取决于 d 和所选基），使得对于所有线性映射 T:$\mathcal{B}(H) \to \mathcal{B}(H)$，

$$\|T\|_\diamond \;\le\; C_\diamond \, \|T\|_{\mathrm{tom}}. \tag{10.21}$$

证明。 我们先证明单射性。若$\mathcal{T}(T) = 0$，则对于所有 j,k，$\mathrm{Tr}[G_k\, T(F_j)] = 0$。对于任意厄米算子$X \in \mathcal{B}_{\mathrm{Herm}}(\mathcal{H})$，可将其写为$X = \sum_j a_j F_j$，其中 $a_j \in \mathbb{R}$，因此

$$T(X) = \sum_j a_j T(F_j).$$

对于任意厄米算子 $Y \in \mathcal{B}_{\mathrm{Herm}}(\mathcal{H})$，写作 $Y = \sum_k b_k G_k$。于是

$$\mathrm{Tr}[Y\, T(X)] = \sum_{j,k} a_j b_k \,\mathrm{Tr}[G_k\, T(F_j)] = 0.$$

由于厄米算子张成$\mathcal{B}(\mathcal{H})$，且希尔伯特–施密特内积是非退化的，我们必有$T(X) = 0$ 对于所有 X，因此 $T = 0$。由此$\mathcal{T}$是单射，且 $\|\cdot\|_{\mathrm{tom}}$ 是一个范数。

范数等价是一个标准事实：如果 V 是一个有限维实向量空间，且 $\|\cdot\|_a, \|\cdot\|_b$ 是两个范数，那么存在常数 $C > 0$，使得 $\|v\|_a \le C\|v\|_b$ 对所有 $v \in V$ 都成立。这里我们取 $V = \mathrm{End}(\mathcal{B}(\mathcal{H}))$,$\|\cdot\|_a = \|\cdot\|_\diamond$（菱形范数），以及 $\|\cdot\|_b = \|\cdot\|_{\mathrm{tom}}$。根据范数等价，存在一个常数 $C_\diamond > 0$，它仅取决于维数和所选基，使得

$$\|T\|_\diamond \le C_\diamond \, \|T\|_{\mathrm{tom}}$$

对于所有 T。 ■

注释 37。 上述证明仅使用了线性泛函族 $T \mapsto \text{迹}[G_k T\ (F_j)\ ]$ 张成 $\mathrm{End}(\boldsymbol{B}\ (\boldsymbol{H})$ 的对偶空间这一事实；我们从未使用 T 的任何完全正性或保迹性质。因此，该不等式对任意线性映射均成立。

此外，由于 $\{G_k\}$ 张成了厄米算子空间，对于任意给定的实数组 $\{a_{k,\ j}\}_{k,\ j}$ 以及每个固定的 j，线性映射 $X \mapsto($迹$[G_k X])_k$ 从 $\boldsymbol{B}(\boldsymbol{H})$ 到 $\mathbb{R}^D$ 是一个同构。因此存在唯一的 X_j，使得迹$[G_k X_j] = a_{k,\ j}$ 对所有 k均成立。定义 $T(F_j)$ $:= X_j$，并将其线性扩展到 $\boldsymbol{B}(\boldsymbol{H})$ 的全体元素上，可得到线性映射 T，满足 $\boldsymbol{T}\ (T)\ = \{a_{k,\ j}\}$。这表明 $\boldsymbol{T}$ 实际上是一个双射。

引理 34 (关于 $C_\diamond$ 的粗略维数依赖上界**)**。 设 $\boldsymbol{H} \simeq \mathbb{C}^d$，且设 $D = d^2$。固定一个希尔伯特–施密特正交归一基 $\{H_\mu\}_{\mu=1}^{D} \subset \boldsymbol{B}_{\mathrm{Herm}}(\boldsymbol{H})$，并定义规范层析范数

$$\|T\|_{\mathrm{tom,can}} := \max_{1\le \mu,\nu\le D} \big|\mathrm{Tr}\big[H_\mu\, T(H_\nu)\big]\big|.$$

T因此存在一个普适常数 $c_0 > 0$，使得对于所有线性映射 T： $\boldsymbol{B}(\boldsymbol{H}) \to \boldsymbol{B}(\boldsymbol{H})$，

$$\|T\|_\diamond \ \le\ C_\diamond(d)\, \|T\|_{\mathrm{tom,can}}, \qquad C_\diamond(d)\ \le\ c_0\, d^{7/2}. \tag{10.22}$$

特别地， $C_\diamond(d)$ 关于 d至多呈多项式增长。

证明。 我们首先将 T 诱导的 $1 \to 1$ 范数上界为$\|T\|_{\mathrm{tom,can}}$。 根据对偶性,

$$\begin{aligned} \|T\|_{1\to 1} &= \sup_{\|X\|_1\le 1} \|T(X)\|_1 \\ &= \sup_{\|X\|_1\le 1,\ \|Y\|_\infty\le 1} \big|\mathrm{Tr}[Y\, T(X)]\big|. \end{aligned}$$

将 X 和 Y 按正交归一基展开:

$$X = \sum_\nu x_\nu H_\nu, \qquad Y = \sum_\mu y_\mu H_\mu, \qquad x_\nu = \mathrm{Tr}[H_\nu X],\ y_\mu = \mathrm{Tr}[H_\mu Y].$$

Then

$$T(X) = \sum_\nu x_\nu T(H_\nu), \qquad \mathrm{Tr}[YT(X)] = \sum_{\mu,\nu} x_\nu y_\mu\, \mathrm{Tr}[H_\mu T(H_\nu)].$$

因此

$$\big|\mathrm{Tr}[YT(X)]\big| \le \Big(\sum_\nu |x_\nu|\Big)\Big(\sum_\mu |y_\mu|\Big)\|T\|_{\mathrm{tom,can}}.$$

现在我们来界定系数和。由于$\{H_\nu\}$ 是正交归一的,

$$\sum_\nu |x_\nu|^2 = \|X\|_2^2 \le \|X\|_1^2.$$

因此，对于 $\|X\|_1 \le 1$,

$$\sum_\nu |x_\nu| \le \sqrt{D}\,\Big(\sum_\nu |x_\nu|^2\Big)^{1/2} \le \sqrt{D}\,\|X\|_1 \le \sqrt{D} = d.$$

对于 Y，同样有

$$\sum_\mu |y_\mu|^2 = \|Y\|_2^2 \le d\,\|Y\|_\infty^2 \le d,$$

由此，对于 $\|Y\|_\infty \le 1$,

$$\sum_\mu |y_\mu| \le \sqrt{D}\,\|Y\|_2 \le \sqrt{D}\,\sqrt{d} = d^{3/2}.$$

综合这些估计，

$$\big|\mathrm{Tr}[YT(X)]\big| \le d^{5/2}\,\|T\|_{\mathrm{tom,can}},$$

因此

$$\|T\|_{1\to 1} \le d^{5/2}\,\|T\|_{\mathrm{tom,can}}. \tag{10.23}$$

另一方面，对于映射 $T\colon M_d \to M_d$，一个标准结论是

$$\|T\|_\diamond = \sup_{k\ge 1} \|T\otimes \mathrm{id}_k\|_{1\to 1} \le d\,\|T\|_{1\to 1}.$$

将其与（10.23）结合可得

$$\|T\|_\diamond \le d\cdot d^{5/2}\,\|T\|_{\mathrm{tom,can}} = d^{7/2}\,\|T\|_{\mathrm{tom,can}}.$$

将数值常数吸收到 c_0 中，即可得到所声称的界。 ■

注 *38*（与引理 *33* 中层析范数 $\|\cdot\|_{\mathrm{tom}}$ 的关系）。在引理 *32* 和定义 *32* 中，我们允许一般的厄米基 $\{F_j\}$、$\{G_k\}$，其中 $\|F_j\|_1 \le C_1$ 和 $\|G_k\|_\infty \le C_\infty$，并定义 $\|T\|_{\mathrm{tom}} := \max_{j,k} |迹[G_k T(F_j)]|$。。由于任意两个基之间都存在可逆线性坐标变换，且基元素只有有限个，因此范数 $\|\cdot\|_{\mathrm{tom}}$ 和 $\|\cdot\|_{\mathrm{tom,can}}$ 等价，等价常数至多依赖于 d 的多项式。因此，引理 *33* 中的抽象常数 $C_\diamond$ 可以选取为使得

$$C_\diamond(d) \;\le\; \mathrm{poly}(d),$$

例如，调整常数后，$C_\diamond(d) \le c_0 d^{7/2}$。特别是，$C_\diamond$ 的增长速度始终不超过希尔伯特空间维数的某个固定多项式。

使用形式为 (F_j, G_k) 且输出 迹$[G_k E(F_j)]$, 的 QPStat 查询，可以近似层析指纹 $\mathcal{T}(E)$的所有元素。根据引理 33，这可以一致地控制信道之间的菱形范数距离。

C. 方案 B：基于层析的 Lindbladian-PUF

现在，我们定义一种信道级别的 Lindbladian-PUF 协议：验证者将随机 Lindblad 通道的层析指纹作为经典秘密存储，并在认证阶段要求证明者逐项复现该指纹。这迫使对手以菱形距离学习该信道。

定义 33 (基于层析的 Lindbladian-PUF 协议)。 设 (Θ, d, μ_Θ) 是定义 *26*中的一个随机 *Lindbladian* 参数系综。每个参数 $\theta \in \Theta$ 指定一个 *Lindblad* 生成元 $\mathcal{L}(\theta)$，并在固定时间 $t > 0$下指定一个完全正迹保持信道

$$E_\theta := e^{t\mathcal{L}(\theta)}.$$

令 $\{F_j\}$ 和 $\{G_k\}$ 为引理 *32*中的层析基，并令 $\mathcal{T}(E_\theta) \in \mathbb{R}^{D\times D}$ $(D = d^2)$ 为相应的层析指纹。

固定容差参数 $\tau > 0$ 和整数 $N \ge 1$。验证者 V 与证明者 P 之间的基于层析的 *Lindbladian-PUF* 协议定义如下：

1. 设置。

(a) V 样本 θ 来自 μ_Θ，并获得对实现 E_θ 的设备的一次性物理访问权限。

(b) 对每一对$(j,k) \in [D]\times[D]$, V在输入(F_j, G_k, τ)时调用$\mathrm{QPStat}^{E_\theta}$，并得到一个近似值

$$y_{k,j} \approx \mathrm{Tr}[G_k E_\theta(F_j)],$$

满足$\left|y_{k,\ j} - 迹[G_k E_\theta(F_j)]\right| \le \tau$。（等价地，在一种更接近实验的实现中，$V$可以反复制备 F_j、测量 G_k，并取经验平均值；每个表项需要进行 $O(1/\tau^2)$ 次物理操作。）

(c) V将整个表$\mathbf{y} = \{y_{k,j}\}_{k,j}$ 作为经典秘密保存，然后将物理设备交给证明者。

2. 认证。

(a) 当 P 声称持有真实设备时，V 发起挑战—响应认证。

(b) 对于每一对$(k,j) \in [D]\times[D]$（按某种预定顺序），V发送索引(k,j)作为挑战。持有真实设备的诚实证明者 E_θ 可以通过 *QPStat* 查询或实验运行来估计迹$[G_k E_\theta(F_j)]$，使误差不超过 τ，并返回一个值 $y'_{k,j}$。

(c) V 当且仅当接受

$$\left|y'_{k,j} - y_{k,j}\right| \le 2\tau \quad \textit{for all } k,j. \tag{10.24}$$

备注 39 (完备性)。如果证明者持有真实信道 E_θ，并使用精度为 τ 的 *QPStat* 查询来回答每个挑战，那么根据三角不等式，

$$\left|y'_{k,j} - y_{k,j}\right| \le \left|y'_{k,j} - \mathrm{Tr}[G_k E_\theta(F_j)]\right| + \left|\mathrm{Tr}[G_k E_\theta(F_j)] - y_{k,j}\right| \le 2\tau$$

对所有 k,j 均成立。因此，诚实证明者总会被接受。

现在我们陈述一个关于 QPStat 查询复杂度安全性的结果。原则上，任何未持有真实设备却通过基于层析的验证的对手，都必定已经学会了菱形距离意义下的 Lindblad 通道，因此可由第 12 节 VE中的定理加以排除。

定理 19 (基于层析的 Lindbladian-PUF 的 QPStat 查询复杂度安全性)。考虑定义*33*中的基于层析的 *Lindbladian-PUF* 协议，其底层随机林布拉德算子系综与定理*12*中的相同。设 A 是一个任意的（可能经过随机化的）对手，它在认证之前可以与$\mathrm{QPStat}^{E_\theta}$ 交互，使用至多 q 次精度为 τ的 *QPStat* 查询。在设置阶段，验证者还需要额外 $q_{\mathrm{tom}} = D^2$ 次（或 $O(D^2)$次）*QPStat* 查询来生成层析指纹；此成本仅取决于输出空间维数 d，而不取决于参数维数 M。

如果存在常数 $\alpha > 1/2$ 和 $\beta > 0$，使得

$$\mu_\Theta\Big(\theta : \Pr_{\textit{internal randomness of the adversary}}\big[A \textit{ is accepted in the protocol}\big] \ge \alpha\Big) \ \ge\ \beta, \tag{10.25}$$

那么，对于足够大的参数维数 M，存在与 M 无关的常数 $c > 0$ 和 $c' > 0$，使得

$$q + q_{\mathrm{tom}} \ \ge\ \exp(c(\mathrm{poly}(d))M). \tag{10.26}$$

由于验证者的初始化成本仅随输出维度多项式增长（事实上 $q_{tom} = D^2 = d^4$），而 *QPStat* 下界则按$\exp(c\ \mathrm{poly}(d)M)$增长；当 M（因此 d）足够大时，该下界渐近地超过 d 中的任何固定多项式。因此，与指数级困难项相比，层析成本可以忽略不计，而 q仍必须随 M呈指数级增长。特别地，对于充分大的 M，任何仅使用 $q = \mathrm{poly}(M)$ 个 *QPStat* 查询的对手，都无法以不可忽略的成功概率攻破基于层析的 *Lindbladian-PUF*。

证明。 假设存在一个如上所述的成功对手 A。我们利用它构造一个针对 Lindblad 通道系综的 QPStat 学习算法$\mathcal{L}_{\text{learn}}$ ，然后推导所需查询次数的下界。

我们首先利用成功的对手构造一个近似的层析指纹。对于固定的 $\theta \in \Theta$，定义优良参数集

$$\Theta_{\text{good}} := \Big\{\theta : \ \Pr\big[A \text{ is accepted}\big] \geq \alpha\Big\},$$

根据假设，其中 $\mu_\Theta(\Theta_{\text{good}}) \geq \beta$。在获得 QPStat$_{E_\theta}$ 的访问权限后，$\mathcal{L}_{\text{learn}}$ 模拟整个 Lindbladian-PUF 协议（包括设置阶段）：

i. 在模拟设置阶段，$\mathcal{L}_{\text{learn}}$ 调用 QPStat$_{E_\theta}$ ，并遵循定义 33中验证者 V'的策略，生成表 $\mathbf{y} = \{y_{k,\ j}\}$，将其作为内部秘密保留（不向 A 揭示），并充当预言机与 A 之间的中间媒介，将 A 所需调用的结果传送给 A，同时向 A 提供协议中公开的参数（例如基 $\{34\}F_j\}$，$\{41\}G_k\}$、容差 τ 以及挑战索引集）。

ii. 在模拟认证阶段，$\mathcal{L}_{\text{learn}}$ 按预先确定的顺序向 A 发送挑战索引（$k,\ j$），并记录 A'的答复 $y'_{k,\ j}$。

根据构造，这种模拟交互的分布与 V 和 A之间真实协议的分布完全相同。因此，对于任意 $\theta \in \Theta_{\text{good}}$,

$$\Pr\Big[\big|y'_{k,j} - y_{k,j}\big| \leq 2\tau \ \forall k, j\Big] \ \geq \ \alpha. \tag{10.27}$$

在此事件中，对于所有 $k,\ j$,

$$\big|y'_{k,j} - \mathrm{Tr}[G_k E_\theta(F_j)]\big| \leq \big|y'_{k,j} - y_{k,j}\big| + \big|y_{k,j} - \mathrm{Tr}[G_k E_\theta(F_j)]\big| \leq 3\tau. \tag{10.28}$$

现在我们构造一个线性映射 E，其层析指纹满足 $[\mathcal{T}(E)]_{k,\ j} = y'_{k,\ j}$。对于每个固定的 j，考虑线性同构

$$\Phi : \mathcal{B}(\mathcal{H}) \to \mathbb{R}^D, \quad X \mapsto \big(\mathrm{Tr}[G_k X]\big)_{k=1}^{D}.$$

由于 $\{G_k\}$ 构成一个厄米基， Φ 是双射。因此，对于每个 j，都存在唯一的算子 X_j，使得 迹 $[G_k X_j] = y'_{k,\ j}$ 对所有 k 都成立。在基 $\{F_j\}$ 上定义 E，令 $E(F_j) := X_j$，并将其线性扩展到 B(H) 上的所有元素；由此得到一个线性映射 E，满足 $[\mathrm{T}\,(E)]_{k,\ j} = y'_{k,\ j}$。根据引理 33 中 T 的单射性， E 是唯一确定的。我们不要求 E 是完全正迹保持的；它只是一个假设通道。

在上述成功事件发生时，

$$\Big|\big[\mathcal{T}(\widehat{E} - E_\theta)\big]_{k,j}\Big| = \big|y'_{k,j} - \mathrm{Tr}[G_k E_\theta(F_j)]\big| \leq 3\tau \quad \text{for all } k, j,$$

so

$$\| \widehat{E} - E_\theta \|_{\text{tom}} \leq 3\tau. \tag{10.29}$$

根据引理 33，我们可得

$$\| \widehat{E} - E_\theta \|_\diamond \ \leq \ C_\diamond \| \widehat{E} - E_\theta \|_{\text{tom}} \ \leq \ 3C_\diamond \tau. \tag{10.30}$$

因此，在认证成功的事件中， E 与 E_θ之间的菱形距离为 $\varepsilon := 3C_\diamond \tau$。

现在我们 将上述过程视为针对信道族$\mathcal{L}_{\text{learn}}$ 的 QPStat 学习算法 }:

i. $\mathcal{L}_{\text{learn}}$ 可以访问 QPStat$_{E_\theta}$ ，并在内部模拟 V 与 A之间的完整协议。

ii. 它输出上述构造的假设映射 E。

对于任意 $\theta \in \Theta_{\text{good}}$，以至少 α 的概率（关于算法的内部随机性），我们有

$$d_\diamond(\widehat{E}, E_\theta) := \| \widehat{E} - E_\theta \|_\diamond \leq 3C_\diamond \tau =: \varepsilon.$$

此外，$\mathcal{L}_{\text{learn}}$ 使用的 QPStat 查询总数为

$$q_{\text{tot}} = q_{\text{tom}} + q,$$

其中，q_{tom} 是模拟设置阶段生成$\mathbf{y}$ 所需的查询次数，仅取决于 d和 τ，而不取决于 M；q 是对手 A 自身使用的查询次数。

此时，我们恰好处于定理 12所述的设置中。学习器 $\mathcal{L}_{\text{learn}}$ 至多使用 q_{tot} 次 QPStat 查询，并且在 μ_Θ-测度至少为 β的参数子集上，以至少 $\varepsilon = 3C_\diamond\tau$ 的成功概率达到菱形距离 α。根据定理 12，存在一个常数 $c > 0$，与 M 无关，使得当 M充分大时，

$$q_{\text{tot}} \geq \exp(c(\text{poly}(d))M). \tag{10.31}$$

■

备注 40 （验证成本）。如此强大的验证能力伴随着信息论成本。层析指纹 $T(E_\theta)$ 包含 $D^2 \sim d^4$ 个条目，因此，即使每个条目只需达到常数精度，验证者的初始化成本 q_{tom} 也至少会像 d^4那样多项式增长。在大多数量子多体模型中，参数维数 M 至多关于 d呈多项式增长，因此验证成本与信道本身的信息内容处于同一数量级，这使得很难将其视为可高效验证的密码协议。这与分布级方案形成鲜明对比；在该方案中，$|X|$ 可以取为多项式，而参数维数 M 可以远大于 $\log|X|$。

备注 41 （为什么经典影子无法取代基于层析的验证）。一个自然的问题是，经典影子技术（结合经典压缩的随机测量）能否取代完整层析，从而在维持信道级安全性的同时，将验证成本控制在多项式范围内。从信息论视角来看，一般而言这是不可能的。

经典影子协议的基本思想 *[HKP20a]* 是对待研究对象（量子态或信道）施加一组固定的随机测量，并通过简单的经典后处理将每个测量结果压缩成一个简短的经典影子字符串。对于量子态学习，这些影子足以以高概率预测大量可观测量的期望值，但其核心实现的是一种低维线性投影：

$$\Phi_{\text{sh}} : \text{End}(\mathcal{B}(\mathcal{H})) \longrightarrow \mathbb{R}^K,$$

其中 K 至多与样本数量和每次测量的比特数成正比，并且在多项式采样下远小于信道空间维数 d^4。换言之，经典阴影模型是一种有意进行有损压缩的学习方法，旨在近似大量期望值，而非区分所有信道。

从线性代数的角度来看，任何目标维数为 $K \ll d^4$ 的线性映射 Φ_{sh} 必然具有非平凡核：存在 $T \neq 0$，使得 $\Phi_{\text{sh}}(T) = 0$。这意味着存在不同的信道$E \neq E'$，满足 $\Phi_{\text{sh}}(E) = \Phi_{\text{sh}}(E')$，因此经典影子指纹无法在菱形范数下区分它们。所以，本小节中基于层析的验证特意使用了一个层析指纹映射 $T : \text{End}(B(H) \to \mathbb{R}^{D\times D}$，该映射是单射的，因此通过验证在信息论上等价于控制菱形范数。代价是需要长度为 $D^2 \sim d^4$ 的指纹，以及相应数量级的验证成本；这是经典影子无法避免的根本性成本。分布级 *Lindblad* 物理不可克隆函数则采取了不同的路径：它只关注一维输出信道 $E_\theta \mapsto P_\theta$，而在这个约化空间中，我们既能证明统计查询困难性（指数级查询复杂度），又能将验证成本控制在关于 $|X|$ 的多项式规模，从而获得真正可高效验证的密码协议。

[AA11]Scott Aaronson 和 Alex Arkhipov。《线性光学的计算复杂性》。载于《第四十三届 ACM计算理论研讨会论文集》，第333–342页，2011年。72[AAAB+25] Dmitry A Abanin、Rajeev Acharya、Laleh Aghababaie-Beni、Georg Aigeldinger、Ashok Ajoy、Ross Alcaraz、Igor Aleiner、Trond I Andersen、Markus Ansmann、Frank Arute等。《量子遍历动力学边缘的相长干涉》。arXiv预印本 arXiv:2506.10191，2025年。2[AAB+19] Frank Arute、Kunal Arya、Ryan Babbush、Dave Bacon、Joseph C Bardin、Rami Barends、Rupak Biswas、Sergio Boixo、Fernando GSL Brandao、David A Buell等。《使用可编程超导处理器实现量子霸权》。Nature，574(7779):505–510，2019年。2, 27, 72[Aar18a] Scott Aaronson。《量子态的影子层析》。载于《第50届 ACM SIGACT 计算理论研讨会论文集》（STOC 2018）。ACM，2018年，arXiv：1711.01053。2[Aar18b] Scott Aaronson。《量子态的影子层析》。载于STOC，第325–338页，2018年。3[ABC+24] Chris Akers、Adam Bouland、Lijie Chen、Tamara Kohler、Tony Metger和Umesh Vazirani。《全息伪纠缠与 AdS/CFT 字典的复杂度》。arXiv预印本 arXiv:2411.04978，2024年。2[ABGL25] Prabhanjan Ananth、John Bostanci、Aditya Gulati和Yao-Ting Lin。《Haar 随机预言机模型中的伪随机酉矩阵》。载于《年度国际密码学会议》，第301–333页。施普林格，2025年。2[AC16] Scott Aaronson和Lijie Chen。《量子霸权实验的复杂性理论基础》。arXiv预印本 arXiv:1612.05903，2016年。2, 9[ACH+18] Scott Aaronson、Xinyi Chen、Elad Hazan、Satyen Kale和Ashwin Nayak。《量子态的在线学习》。载于《神经信息处理系统进展》，第31卷，2018年，arXiv：1802.09025。2[ACQ22] Dorit Aharonov、Jordan Cotler和Xiao-Liang Qi。《量子算法测量》。《自然·通讯》，13(1):58，2022年。2[ADDK21] Myrto Arapinis、Mahshid Delavar、Mina Doosti和Elham Kashefi。《量子物理不可克隆函数：可能性与不可能性》。《Quantum》，5:475，2021年。67[AdW17] Srinivasan Arunachalam和Ronald de Wolf。《特邀专栏：量子学习理论综述》。《ACM SIGACT News》，48(2):41–67，2017年。2[AdW18a] Srinivasan Arunachalam和Ronald de Wolf。《学习算法的最优量子样本复杂度》。《机器学习研究期刊》，19(1):1–36，2018年。2[ADW18b] Srinivasan Arunachalam和Ronald De Wolf。《学习算法的最优量子样本复杂度》。《机器学习研究期刊》，19(71):1–36，2018年。2[AEH+22] Chris Akers、Netta Engelhardt、Daniel Harlow、Geoff Penington和Shreya Vardhan。《非等距编码与复杂度中的黑洞内部》。arXiv预印本 arXiv:2207.06536，2022年。2[AGY20] Srinivasan Arunachalam、Alex B Grilo和Henry Yuen。《量子统计查询学习》。arXiv:2002.08240，2020年。2[AHS24] Srinivasan Arunachalam、Vojtech Havlicek和Louis Schatzki。《纠缠与统计数据在学习中的作用》。载于《神经信息处理系统进展》，36:55064–55076，2024年。2[Bao25] Ruicheng Bao。《量子弛豫中的初态典型性》。arXiv预印本 arXiv:2511.01709，2025年。3[BCD+09] Alessandro Bisio、Giulio Chiribella、Giacomo Mauro D'Ariano、Stefano Facchini和Paolo Perinotti。《最优量子层析》。《电气电子工程师学会量子电子学精选主题期刊》，15(6):1646–1660，2009年。3[BCHJ+21] Fernando GSL Brandão、Wissam Chemissany、Nicholas Hunter-Jones、Richard Kueng和John Preskill。《量子复杂性增长模型》。《PRX Quantum》，2(3):030316，2021年。24[BCMS19] Colin D Bruzewicz、John Chiaverini、Robert McConnell和Jeremy M Sage。《囚禁离子量子计算：进展与挑战》。《应用物理评论》，6(2)，2019年。27[BFNV19] Adam Bouland、Bill Fefferman、Chinmay Nirkhe和Umesh Vazirani。《量子随机电路采样的复杂度与验证》。《自然·物理》，15(2):159，2019年。2, 72[BGP+20] Eyal Bairey、Chu Guo、Dario Poletti、Netanel H Lindner和Itai Arad。《从稳态学习开放量子系统的动力学》。《新物理学杂志》，22(3):032001，2020年。3[BGS84] Oriol Bohigas、Marie-Joya Giannoni和Charles Schmit。《混沌量子谱的表征与能级涨落定律的普适性》。《物理评论快报》，52(1):1，1984年。2[Bha13] Rajendra Bhatia。《矩阵分析》，第169卷。施普林格科学与商业媒体，2013年。15[BHH16]Fernando GSL Brandao、Aram W Harrow和Michał Horodecki。《局域随机量子电路是近似多项式设计》。《数学物理通讯》，346(2):397–434，2016年。2, 4, 31, 32[BIS+18] Sergio Boixo、Sergei V Isakov、Vadim N Smelyanskiy、Ryan Babbush、Nan Ding、Zhang Jiang、Michael J Bremner、John M Martinis和Hartmut Neven。《近期设备中的量子霸权表征》。《自然·物理》，14(6):595–600，2018年。2, 47[BJ95] Nader H. Bshouty和Jeffrey C. Jackson。《在均匀分布下使用量子示例学习 DNF》

预言机。《第八届计算学习理论年会论文集》，COLT'95，第118–127页。美国计算机协会，1995年。2[BMS+11] Julio T Barreiro、Markus Müller、Philipp Schindler、Daniel Nigg、Thomas Monz、Michael Chwalla、Markus Hennrich、Christian F Roos、Peter Zoller和Rainer Blatt。采用囚禁离子的开放系统量子模拟器。《自然》，470(7335):486–491，2011年。3[BS19] Zvika Brakerski和Omri Shmueli。具有二元相位的（伪）随机量子态。见《密码学理论会议》，第229–250页。施普林格，2019年。2[BŻ17] Ingemar Bengtsson和Karol Życzkowski。《量子态几何：量子纠缠导论》。剑桥大学出版社，2017年。68[CBB+24] Chi-Fang Chen、Adam Bouland、Fernando GSL Brandão、Jordan Docter、Patrick Hayden和Michelle Xu。由置换构造的高效酉设计与伪随机酉矩阵。arXiv预印本 arXiv:2404.16751，2024年。2[CCHL21] Sitan Chen、Jordan Cotler、Hsin-Yuan Huang和Jerry Li。使用量子存储器学习与不使用量子存储器学习之间的指数级分离。见《2021 IEEE 第62届计算机科学基础年会》（FOCS），第574–585页。IEEE，2021年。2[CCHL23] Sitan Chen、Jordan Cotler、Hsin-Yuan Huang和Jerry Li。含噪声中等规模量子的复杂度。《自然·通讯》，14(1):6001，2023年。2[CL21] Kai-Min Chung和Han-Hsuan Lin。在PAC模型中学习量子信道的样本高效算法与近似态判别问题。见《第16届量子计算、通信与密码学理论会议》（TQC 2021），第3:1–3:22页。达格施图尔城堡—莱布尼茨信息学中心，2021年。3[CLL+22] Andrew M Childs、Tongyang Li、Jin-Peng Liu、Chunhao Wang和Ruizhe Zhang。用于采样对数凹分布和估计归一化常数的量子算法。《神经信息处理系统进展》，35:23205–23217，2022年。3[CRJ+22] Malcolm Carroll、Sami Rosenblatt、Petar Jurcevic、Isaac Lauer和Abhinav Kandala。超导量子比特弛豫时间的动力学。《npj量子信息》，8(1):132，2022年。27[CSBH25] Laura Cui、Thomas Schuster、Fernando Brandão和Hsin-Yuan Huang。近最优深度下的酉设计。arXiv预印本 arXiv:2507.06216，2025年。2[CW20] Jordan Cotler和Frank Wilczek。量子重叠层析。《物理评论快报》，124(10):100401，2020年。2[CZZ17] Chip-Hong Chang、Yue Zheng和Le Zhang。回顾与展望：物理不可克隆函数发展的十五年。《IEEE电路与系统杂志》，17(3):32–62，2017年。67[Dan05]Christoph Dankert。随机量子态和算子的高效模拟。arXiv预印本 quant-ph/0512217，2005年。2[DCEL09]Christoph Dankert、Richard Cleve、Joseph Emerson和Etera Livine。精确与近似酉2-设计及其在保真度估计中的应用。《物理评论 A》，80(1):012304，2009年。2[Deu91] J. M. Deutsch。封闭系统中的量子统计力学。《物理评论 A》，43:2046，1991年。2[DLT+19] Sergey Denisov、Tetyana Laptyeva、Wojciech Tarnowski、Dariusz Chruściński和Karol Życzkowski。随机林德布拉德算符的普适谱。《物理评论快报》，123(14):140403，2019年。3，27[DMAM17] Mahshid Delavar、Sattar Mirzakuchaki、Mohammad Hassan Ameri和Javad Mohajeri。高级计量基础设施（AMI）中基于物理不可克隆函数的安全通信解决方案。《国际通信系统杂志》，30(9):e3195，2017年。67[DMK+08] Sebastian Diehl、A Micheli、Adrian Kantian、B Kraus、HP Büchler和Peter Zoller。采用冷原子的受驱动开放量子系统中的量子态与相。《自然·物理》，4(11):878–883，2008年。3[EAŻ05] Joseph Emerson、Robert Alicki和Karol Życzkowski。利用随机酉算子进行可扩展噪声估计。《光学杂志 B：量子与半经典光学》，7(10):S347，2005年。2[EFH+23] Andreas Elben、Steven T Flammia、Hsin-Yuan Huang、Richard Kueng、John Preskill、Benoît Vermersch和Peter Zoller。随机测量工具箱。《自然综述：物理》，5(1):9–24，2023年。2[EN00] Klaus-Jochen Engel和Rainer Nagel。线性演化方程的单参数半群。施普林格，2000年。23[EWS+03] Joseph Emerson、Yaakov S Weinstein、Marcos Saraceno、Seth Lloyd和David G Cory。用于量子信息处理的伪随机酉算子。《科学》，302(5653):2098–2100，2003年。2[Fel17] Vitaly Feldman。统计查询复杂度的一般刻画。见《学习理论会议》，第785–830页。机器学习研究论文集，2017年。6, 18, 20, 48[GAE07] David Gross、Koenraad Audenaert和Jens Eisert。均匀分布的酉算子：论酉设计的结构。《数学物理学杂志》，48(5)，2007年。2[GHH+25] Lorenzo Grevink、Jonas Haferkamp、Markus Heinrich、Jonas Helsen、Marcel Hinsche、Thomas Schuster和Zoltán Zimborás。能否拼接？论超越酉群的短深度设计。arXiv预印本 arXiv:2506.23925，2025年。2[GKKT20] M Guţă、Jonas Kahn、Richard Kueng和Joel A Tropp。具有最优误差界的快速量子态层析。

《物理学杂志 A：数学与理论》，53(20):204001，2020年。2[Gol04] Oded Goldreich。《密码学基础》，第2卷。剑桥大学出版社，剑桥，2004年。68[GTFS16] Fatemeh Ganji、Shahin Tajik、Fabian Fäßler和Jean-Pierre Seifert。针对无数学模型的物理不可克隆函数的强机器学习攻击。见《国际密码硬件与嵌入式系统会议》，第391–411页。施普林格，2016年。67[Haf22] Jonas Haferkamp。随机量子电路在给定深度下是近似酉 t-设计。《Quantum》，6:795，2022年。2, 4, 31, 32[HBC+22] Hsin-Yuan Huang、Michael Broughton、Jordan Cotler、Sitan Chen、Jerry Li、Masoud Mohseni、Hartmut Neven、Ryan Babbush、Richard Kueng、John Preskill和Jarrod R. McClean。通过实验学习中的量子优势。《科学》，376(6598):1182–1186，2022年。2[HE23] Dominik Hangleiter和Jens Eisert。量子随机采样的计算优势。《现代物理学评论》，95(3):035001，2023年。47[HHJ+15] Jeongwan Haah、Aram W. Harrow、Zhengfeng Ji、Xiaodi Wu和Nengkun Yu。量子态的样本最优层析。2015年，arXiv:1508.01797。2[HIN+23] Marcel Hinsche、Marios Ioannou、Alexander Nietner、Jonas Haferkamp、Yihui Quek、Dominik Hangleiter、J-P Seifert、Jens Eisert和Ryan Sweke。一个 t 门即可使分布学习变得困难。《物理评论快报》，130(24):240602，2023年。2[HKKU20] Ryusuke Hamazaki、Kohei Kawabata、Naoto Kura和Masahito Ueda。非厄米随机矩阵的普适类。《物理评论研究》，2(2):023286，2020年。32[HKOT23] Jeongwan Haah、Robin Kothari、Ryan O’Donnell和Ewin Tang。菱形距离下酉信道的查询最优估计。见《2023 IEEE 第64届计算机科学基础年会》（FOCS），第363–390页。IEEE，2023年。3[HKP20a] Hsin-Yuan Huang、Richard Kueng和John Preskill。从极少量测量中预测量子系统的诸多性质。《自然·物理》，16(10):1050–1057，2020年。2, 89[HKP20b] Hsin-Yuan Huang、Richard Kueng和John Preskill。从极少量测量中预测量子系统的诸多性质。《自然·物理》，16(10):1050–1057，2020年6月。2[HKP21] Hsin-Yuan Huang、Richard Kueng和John Preskill。机器学习中量子优势的信息论界。《物理评论快报》，126(19):190505，2021年。2[HP07] Patrick Hayden和John Preskill。黑洞作为镜子：随机子系统中的量子信息。《高能物理学杂志》，2007(09):120，2007年。2[HTFS23] Hsin-Yuan Huang、Yu Tong、Di Fang和Yuan Su。以海森堡极限标度学习多体哈密顿量。《物理评论快报》，130(20):200403，2023年。2[JLS18] Zhengfeng Ji、Yi-Kai Liu和Fang Song。伪随机量子态。见《密码学进展——CRYPTO 2018：第38届密码学年会，美国加利福尼亚州圣巴巴拉，2018年8月19–23日，论文集，第III部分38》，第126–152页。施普林格，2018年。2[Kam23] Alex Kamenev。非平衡系统场论。剑桥大学出版社，2023年。54[Kat13] Tosio Kato。线性算子的微扰理论，第132卷。施普林格科学与商业媒体，2013年。24[KBD+08] Barbara Kraus、Hans P Büchler、Sebastian Diehl、Adrian Kantian、Andrea Micheli和Peter Zoller。通过量子马尔可夫过程制备纠缠态。《物理评论 A——原子、分子与光学物理》，78(4):042307，2008年。3[Kea98] Michael Kearns。利用统计查询进行高效抗噪学习。《美国计算机学会会刊》，45(6):983–1006，1998年。2[KG19] Mahmoud Khalafalla和Catherine Gebotys。物理不可克隆函数的深度攻击：利用深度学习技术增强建模攻击，以破解双仲裁器物理不可克隆函数。见《2019年欧洲设计、自动化与测试会议暨展览》（DATE），第204–209页。IEEE，2019年。67[KHM19] Ivan M Khaymovich、Masudul Haque和Paul A McClarty。本征态热化、随机矩阵理论与巨兽。《物理评论快报》，122(7):070601，2019年。32[KLR+08] Emanuel Knill、Dietrich Leibfried、Rolf Reichle、Joe Britton、R Brad Blakestad、John D Jost、Chris Langer、Roee Ozeri、Signe Seidelin和David J Wineland。量子门的随机基准测试。《物理评论 A》，77(1):012307，2008年。2[KTP20] Isaac Kim、Eugene Tang和John Preskill。辐射中的幽灵：黑洞内部的鲁棒编码。《高能物理学杂志》，2020(6):1–65，2020年。2[Kub57] Ryogo Kubo。不可逆过程的统计力学理论。I. 一般理论及其在磁学和传导问题中的简单应用。《日本物理学会志》，12(6):570–586，1957年。52[LDNT25] Guglielmo Lami、Jacopo De Nardis和Xhek Turkeshi。随机张量网络的反集中与态设计。《物理评论快报》，134(1):010401，2025年。2[Led01] Michel Ledoux。测度集中现象。第89号。美国数学学会，2001年。24, 25, 31, 32, 34

[LL24] Nicholas LaRacuente 和 Felix Leditzky。浅层低通信电路生成的近似酉 k 设计。arXiv 预印本 arXiv:2407.07876，2024 年。2[LP61] Günter Lumer 和 Ralph S Phillips。巴拿赫空间中的耗散算子。1961 年。18[Meh04] Madan Lal Mehta。随机矩阵，第 142 卷。Elsevier，2004 年。32[Mel24] Antonio Anna Mele。量子信息中的哈尔测度工具导论：初学者教程。《Quantum》，8:1340，2024 年。4, 31, 32[MH25] Fermi Ma 和 Hsin-Yuan Huang。如何构造随机酉矩阵。载于《第57届ACM计算理论研讨会论文集》，第806–809页，2025年。2[MHB+04] Sebastian Müller、Stefan Heusler、Petr Braun、Fritz Haake 和 Alexander Altland。量子混沌中普适性的半经典基础。《物理评论快报》，93(1):014103，2004 年。2[Mon17a] Ashley Montanaro。通过 Bell 采样学习稳定子态。arXiv:1707.04012，2017 年。3[Mon17b] Cécile Monthus。具有边界驱动和体退相干的耗散随机量子自旋链：非平衡稳态中的磁化与电流统计。《统计力学杂志：理论与实验》，2017(4):043302，2017 年。27[MPSY24] Tony Metger、Alexander Poremba、Makrand Sinha 和 Henry Yuen。线性深度 t-设计与伪随机酉矩阵的简单构造。arXiv 预印本 arXiv:2404.12647，2024 年。2[MRL08] Masoud Mohseni、Ali T Rezakhani 和 Daniel A Lidar。量子过程层析：不同策略的资源分析。《物理评论 A》，77(3):032322，2008 年。3[MVM+23] Alexis Morvan、B Villalonga、X Mi、S Mandra、A Bengtsson、PV Klimov、Z Chen、S Hong、C Erickson、IK Drozdov 等。随机电路采样中的相变。arXiv 预印本 arXiv:2304.11119，2023 年。2[NC10] Michael A Nielsen 和 Isaac L Chuang。量子计算与量子信息。剑桥大学出版社，2010 年。68, 72[NH95] Igor Najfeld 和 Timothy F Havel。矩阵指数的导数及其计算。《应用数学进展》，16(3):321–375，1995 年。24[NHKW16] Yoshifumi Nakata、Christoph Hirche、Masato Koashi 和 Andreas Winter。具有近似时间无关哈密顿动力学的高效酉设计。arXiv 预印本 arXiv:1609.07021，2016 年。2[Nie23] Alexander Nietner。统一（量子）统计算法与参数化（量子）算法。arXiv 预印本 arXiv:2310.17716，2023 年。2[NIS+23] Alexander Nietner、Marios Ioannou、Ryan Sweke、Richard Kueng、Jens Eisert、Marcel Hinsche 和 Jonas Haferkamp。学习量子电路输出分布的平均情形复杂度。arXiv 预印本 arXiv:2305.05765，2023 年。2[NIS+25] Alexander Nietner、Marios Ioannou、Ryan Sweke、Richard Kueng、Jens Eisert、Marcel Hinsche 和 Jonas Haferkamp。学习量子电路输出分布的平均情形复杂度。《Quantum》，9:1883，2025 年。4, 6, 18, 20, 21, 22, 32, 47, 48[NO14] Yoshifumi Nakata 和 Tobias J Osborne。随机量子多体系统的热态。《物理评论 A》，90(5):050304，2014 年。32[O'D14] Ryan O'Donnell。布尔函数分析。剑桥大学出版社，2014 年。70, 75[PASA+21]Koustubh Phalak、Abdullah Ash-Saki、Mahabubul Alam、Rasit Onur Topaloglu 和 Swaroop Ghosh。用于量子计算安全与可信性的量子物理不可克隆函数。《电气电子工程师学会电路与系统新兴和精选主题期刊》，11(2):333–342，2021 年。67[PPS22] Niklas Pirnay、Anna Pappa 和 Jean-Pierre Seifert。基于单量子比特门学习经典读出量子物理不可克隆函数。《量子机器智能》，4(2):14，2022 年。67[PRTG02] Ravikanth Pappu、Ben Recht、Jason Taylor 和 Neil Gershenfeld。物理单向函数。《科学》，297(5589):2026–2030，2002 年。67[RDO08] Marcos Rigol、Vanja Dunjko 和 Maxim Olshanii。一般孤立量子系统的热化及其机制。《自然》，452(7189):854–858，2008 年。2[RH12] Angel Rivas 和 Susana F Huelga。开放量子系统，第 10 卷。施普林格，2012 年。17, 18[Rot06] Ron Roth。编码理论导论。剑桥大学出版社，2006 年。70[RSS+10] Ulrich Rührmair、Frank Sehnke、Jan Sölter、Gideon Dror、Srinivas Devadas 和 Jürgen Schmidhuber。针对物理不可克隆函数的建模攻击。载于《第17届ACM计算机与通信安全会议论文集》，第237–249页，2010年。67[SHH25] Thomas Schuster、Jonas Haferkamp 和 Hsin-Yuan Huang。极低深度中的随机酉矩阵。《科学》，389(6755):92–96，2025 年。2[SHU21] Shoki Sugimoto、Ryusuke Hamazaki 和 Masahito Ueda。基于局部随机矩阵理论检验本征态热化假说。《物理评论快报》，126(12):120602，2021 年。32[SKYH25] Thomas Schuster、Dominik Kufel、Norman Y Yao 和 Hsin-Yuan Huang。识别物质相的困难性。即将出版，2025 年。2[SML+25] Thomas Schuster、Fermi Ma、Alex Lombardi、Fernando Brandão 和 Hsin-Yuan Huang。强随机

酉矩阵与快速扰乱。arXiv 预印本 arXiv:2509.26310，2025 年。2[TCDŻ23] Wojciech Tarnowski、Dariusz Chruściński、Sergey Denisov 和 Karol Życzkowski。满足细致平衡的随机林德布拉德算符。《开放系统与信息动力学》，30(02):2350007，2023 年。3[TPI19] Lars Tebelmann、Michael Pehl 和 Vincent Immler。Tero PUF 的侧信道分析。载于《国际建设性侧信道分析与安全设计研讨会》，第43–60页。施普林格，2019 年。67[Val84] Leslie G Valiant。可学习性理论。《美国计算机协会通讯》，27(11):1134–1142，1984 年。2[VWIC09] Frank Verstraete、Michael M Wolf 和 J Ignacio Cirac。由耗散驱动的量子计算与量子态工程。《自然 · 物理》，5(9):633–636，2009 年。3[WAG+25] Stewart Wallace、Yoann Altmann、Brian D Gerardot、Erik M Gauger 和 Cristian Bonato。从实验数据中学习马尔可夫开放量子系统的动力学。《物理评论研究》，7(3):033217，2025 年。3[Wat04] John Watrous。关于由 Schatten 范数诱导的超算子范数的笔记。arXiv 预印本 quant-ph/0411077，2004 年。15[Wat18] John Watrous。量子信息理论。剑桥大学出版社，2018 年。15[WCP13] Weiran Wang 和 Miguel A Carreira-Perpinn。投影到概率单纯形：一种高效算法及其简明证明与应用。arXiv 预印本 arXiv:1309.1541，2013 年。78[WD24] Chirag Wadhwa 和 Mina Doosti。基于统计数据的浅层量子电路耐噪可学习性与量子伪随机性的代价。arXiv 预印本 arXiv:2405.12085，2024 年。21, 22[Wig67] Eugene P Wigner。物理学中的随机矩阵。《SIAM评论》，9(1):1–23，1967 年。2[WKPT22] Yue Wu、Shimon Kolkowitz、Shruti Puri 和 Jeff D Thompson。碱土里德伯原子阵列中用于容错量子计算的擦除转换。《自然·通讯》，13(1):4657，2022 年。27[WL24] Ke Wang 和 Xiantao Li。开放量子系统的仿真辅助学习。《Quantum》，8:1407，2024 年。3[WPS+17] Jianwei Wang、Stefano Paesani、Raffaele Santagati、Sebastian Knauer、Antonio A. Gentile、Nathan Wiebe、Maurangelo Petruzzella、Jeremy L. O'Brien、John G. Rarity、Anthony Laing 和 Mark G. Thompson。实验量子哈密顿量学习。《自然·物理》，13(6):551–555，2017 年。2[YE25] Lisa Yang 和 Netta Engelhardt。学习黑洞及其他混沌系统的（伪）随机动力学的复杂度。《高能物理学杂志》，2025(3):1–65，2025 年。2[Yos12] Kôsaku Yosida。泛函分析，第 123 卷。施普林格科学与商业媒体，2012 年。22, 23[ZRM21] Andrew Zhao、Nicholas C Rubin 和 Akimasa Miyake。通过经典影子实现费米子部分层析。《物理评论快报》，127(11):110504，2021 年。2