arXiv:2303.01188v2 [quant-ph] 1 Jul 2023

非相干策略下的量子信道认证

Omar Fawzi[1], Nicolas Flammarion[2],Aurélien Garivier[3], 和 Aadil Oufkir[1]

[1]里昂大学、Inria、里昂高等师范学院、里昂第一大学、
LIP，里昂，法国[2] 洛桑联邦理工学院，洛桑，瑞士[3]里昂大学、
里昂高等师范学院、UMPA UMR 5669，里昂，法国

2023年7月4日

摘要

在量子信道认证问题中，我们可以将一个量子过程作为黑盒访问，并希望判断该过程是否符合某个预先定义的规范，或者是否与该规范相差 ε。我们的目标是在尽量减少黑盒使用次数的同时完成这一任务。本文关注信道认证两个重要极端情形下的最优非相干策略。第一种情形是预先定义的规范为酉信道，例如量子电路中的一个门。在这种情况下，我们证明，要测试黑盒是否由维数为 d 的固定酉算子描述，或者在迹范数下与其相差 ε-远，需要使用黑盒 $\Theta(d/\varepsilon^2)$ 次。我们考虑的第二种设置是，预先定义的规范为输入维度为 d_{in}、输出维度为 d_{out} 的完全退极化信道。在这种情况下，我们证明，在非自适应设置中，需要且只需使用 $\tilde{\Theta}(d_{\text{in}}^2 d_{\text{out}}^{1.5}/\varepsilon^2)$ 次该量子信道，便可验证它是否等于该去极化信道，或者在菱形范数下与其相差 ε-远。最后，我们证明，在自适应设置下，该问题的下界为 $\Omega(d_{\text{in}}^2 d_{\text{out}}/\varepsilon^2)$。请注意，特殊情形 $d_{\text{in}} = 1$ 对应于广为研究的量子态认证问题。

1 引言

我们研究量子信道认证问题，其任务是验证我们能够通过黑盒访问的量子过程是否按预期运行。量子理论中的有效过程由量子信道建模。输入维度为 d_{in}、输出维度为 d_{out} 的量子信道是一个满足某些正性和归一化条件的线性映射 $\mathbb{C}^{d_{\text{in}}\times d_{\text{in}}} \to \mathbb{C}^{d_{\text{out}}\times d_{\text{out}}}$（详情见第 2 节）。给定已知量子信道 $\mathcal{N}_0$ 的完整描述，以及未知量子信道 $\mathcal{N}$ 的 N 个副本，且该未知量子信道与 $\mathcal{N}_0$ 的距离可能为 $\mathcal{N}_0$ 或 ε，在每一步 $1 \le t \le N$，我们可以选择一个输入量子态，将其送入未知过程 $\mathcal{N}$，然后测量输出量子态。收集到足够多的经典观测值后，我们的目标是以高概率判断量子信道 $\mathcal{N}$ 属于哪种情况，同时尽量减少 N。我们也将这个问题称为对量子信道 $\mathcal{N}_0$ 进行恒等性检验。

这项测试任务之所以重要，有诸多原因。首先，量子计算的基本构件是酉门。因此，了解验证一个未知量子信道是否按指定实现了某个给定门所需的复杂度十分重要。其次，量子信道认证是量子态认证的自然推广。事实上，如果这些量子通道是恒定的量子态，那么对它们进行测试就等同于测试这些量子态。乍看之下，利用 Choi–Jamiołkowski 同构，似乎可以通过将量子态认证算法应用于相应的 Choi 态来实现量子信道认证。然而，至少有两个原因使这种做法行不通：第一，在不允许使用辅助系统的模型中

无法轻易从实现该量子信道的黑盒制备 Choi 态；第二，量子通道的自然距离概念并不等同于 Choi 态之间的迹距离。最后，量子过程层析，即以菱形范数完整学习一个量子信道的问题，代价高昂 [Surawy-Stepney 等，2022，Oufkir， 2023], 我们希望认证所需的副本数能少于完整层析所需的数量。

本文聚焦于两个极端情形： $\mathcal{N}_0(\rho) = \mathcal{N}_U(\rho) = U\rho U^\dagger$是酉信道，其中 U是酉矩阵；而 $\mathcal{N}_0(\rho) = \mathcal{D}(\rho) = \mathrm{Tr}(\rho)\frac{\mathbb{I}}{d_{\mathrm{out}}}$ 是完全退极化信道。

贡献。我们提出了一种非相干无辅助系统测试算法，用于在迹距离下检验恒等信道与固定酉信道 $\mathcal{N}_U$ 是否相同，所使用的测量次数为 $\mathcal{O}(d/\varepsilon^2)$（其中 $d_{\mathrm{in}} = d_{\mathrm{out}} = d$）。该测试器选择一个随机输入态，并使用经酉矩阵 U共轭的相应正算子值测度进行测量。该结果陈述于定理 3.1 中。关于 Choi 态的 1-范数与量子信道菱形范数之间关系的标准不等式，仅能给出上界 $\mathcal{O}(d^2/\varepsilon^2)$。我们通过证明纠缠保真度与到恒等信道的迹距离之间的新不等式，在维数依赖方面取得了二次改进（引理 A.3）。此外，我们还建立了在迹距离下检验恒等信道与固定酉信道是否相同的匹配下界 $\Omega(d/\varepsilon^2)$。即使采用辅助系统辅助策略，该下界仍然成立。为此，我们构造了一个精心选择的信道分布，该分布中的信道与恒等信道相距 ε。经过足够多次测量后，两个假设下的观测值应当是可区分的，即（Kullback–Leibler）KL 散度为 $\Omega(1)$。然而，我们可以证明，对于所选的这一信道分布，无论先前观测值如何，任意自适应测试器在一次测量后至多只能将 KL 散度增加 $\mathcal{O}(\varepsilon^2/d)$。该下界陈述并证明于定理B.1 中。

关于完全退极化信道 $\mathcal{D}(\rho) = \mathrm{Tr}(\rho)\frac{\mathbb{I}}{d_{\mathrm{out}}}$的认证，我们提出一种无辅助量子比特的非相干策略，以使用 $\mathcal{O}(d_{\mathrm{in}}^2 d_{\mathrm{out}}^{1.5}/\varepsilon^2)$ 次测量来区分 $\mathcal{N} = \mathcal{D}$ 与 $\mathcal{N}$ 是否与其相距 ε（菱形距离）（见定理 4.4）。为此，我们说明如何将该认证问题归约为最大混合态的认证（混合性测试） $\frac{\mathbb{I}}{d_{\mathrm{out}}}$。我们随机选择输入态 $|\phi\rangle\langle\phi|$，并比较输出态 $\mathcal{N}(|\phi\rangle\langle\phi|)$ 与最大混合态$\frac{\mathbb{I}}{d_{\mathrm{out}}}$之间的 2-范数。我们证明，以至少 $\Omega(1)$ 的概率，有 $Y = \|\mathcal{N}(|\phi\rangle\langle\phi|) - \mathbb{I}/d_{\mathrm{out}}\|_2^2 \geq \varepsilon^2/(4d_{\mathrm{out}}d_{\mathrm{in}}^2)$。该不等式足以得到所需的复杂度，但证明它仍需一些工作。首先，我们利用 Weingarten演算证明一个类似的期望不等式。然后，我们仔细控制随机变量 Y 的方差，使得该上界取决于问题的实际难度，主要取决于 Y 的期望以及 $\mathcal{N}$ 与 $\mathcal{D}$ 之间的菱形距离。接下来，我们利用 Paley-Zygmund 不等式得到反集中不等式。

另一方面，我们证明了使用非自适应策略进行恒等信道到去极化信道测试的下界为 $\Omega\left(d_{\mathrm{in}}^2 d_{\mathrm{out}}^{1.5}/(\log(d_{\mathrm{in}}d_{\mathrm{out}}/\varepsilon)^2\varepsilon^2)\right)$（定理 4.5）。为此，我们构造了一种随机量子信道：除随机选取的某个输入态的一个邻域外，其输出态在 1-范数意义下几乎都与最大混合态 $\frac{\mathbb{I}}{d_{\mathrm{out}}}$相距 $\mathcal{O}(\varepsilon/d_{\mathrm{in}})$，而该邻域内的输出与 $\frac{\mathbb{I}}{d_{\mathrm{out}}}$ 相距 ε。随后，我们采用 Le Cam 方法 [LeCam， 1973] 与 [Bubeck 等人， 2020] 的方法类似，但有所不同。首先，我们需要对检验算法选取的输入态与最佳输入态的重叠度都很小这一事件进行条件化。这种条件化是我们得到额外对数因子下界的主要原因。其次，通过使用高斯元素构成的随机矩阵，而非 Haar 分布酉矩阵来构造，我们可以运用超收缩性 [Aubrun 和 Szarek，2017，命题 5.48]：只要对二阶矩给出上界，就能控制所有矩。在特殊情形 $d_{\mathrm{in}} = 1$下，这就得到了 [Bubeck 等人， 2020] 的一个结果，同时大幅简化了他们的分析。此外，采用相同的构造，我们还证明了自适应策略的下界为 $\Omega(d_{\mathrm{in}}^2 d_{\mathrm{out}}/\varepsilon^2)$（定理 4.6）。在这一证明中，我们使用 Kullback–Leibler散度，而非全变差距离。表 1 汇总了这些结果。

相关工作。对酉信道进行恒等性检验，可以看作是对离散分布 [Valiant and Valiant、量子态 [Chen et al., 的常见恒等性检验问题的一种推广，

恒等性检验至 $\mathcal{N}_0$	下界 辅助量子比特辅助	上界 无辅助量子比特
$\mathcal{N}_0 = \mathcal{N}_U$ 迹距离下的自适应策略 d_{Tr}	$\Omega\left(\frac{d}{\varepsilon^2}\right)$，定理 3.1	$\mathcal{O}\left(\frac{d}{\varepsilon^2}\right)$，定理 3.1
$\mathcal{N}_0 = \mathcal{N}_U$ 菱形距离下的自适应策略 $d_\diamond$	$\Omega\left(\frac{d}{\varepsilon^2}\right)$，定理 3.1	$\mathcal{O}\left(\frac{d}{\varepsilon^4}\right)$，定理 3.1
$\mathcal{N}_0 = \mathcal{D}$ 非自适应策略	$\Omega\left(\frac{d_{\mathrm{in}}^2 d_{\mathrm{out}}^{1.5}}{d_{\mathrm{in}} d_{\mathrm{out}}/\varepsilon^{\log(\mathcal{O})^2\varepsilon^2}}\right)$，定理 4.5	$\mathcal{O}\left(\frac{d_{\mathrm{in}}^2 d_{\mathrm{out}}^{1.5}}{\varepsilon^2}\right)$，定理 4.4
$\mathcal{N}_0 = \mathcal{D}$ 自适应策略	$\Omega\left(\frac{d_{\mathrm{in}}^2 d_{\mathrm{out}}+d_{\mathrm{out}}^{1.5}}{\varepsilon^2}\right)$，定理 4.6	$\mathcal{O}\left(\frac{d_{\mathrm{in}}^2 d_{\mathrm{out}}^{1.5}}{\varepsilon^2}\right)$，定理 4.4

表 1：使用非相干策略，在菱形距离和迹距离下对量子通道进行恒等性检验的下界和上界。 $\mathcal{N}_U$是幺正量子信道 $\mathcal{N}_U(\rho) = U\rho U^\dagger$， $\mathcal{D}$是去极化信道 $\mathcal{D}(\rho) = \mathrm{Tr}(\rho)\frac{\mathbb{I}}{d_{\mathrm{out}}}$。我们提出的算法（上界）是无辅助量子比特的，而下界即使对于辅助系统算法也成立。

2022a]。然而，在最坏情形下，对恒等信道进行恒等性检验需要 $\Omega(d/\varepsilon^2)$ 次测量；相比之下，对秩一量子态或狄拉克分布进行恒等性检验，只需 $\mathcal{O}(1/\varepsilon^2)$ 次测量/样本。此外，在对酉信道进行恒等性检验问题的定义中，我们并不要求待检验的未知量子信道是酉信道。在后一种设定下，如果允许使用辅助系统，就很容易设计出高效的检验方法。其他关于酉信道性质的检验方法也见 [Wang, 2011]。关于酉信道检验方法的其他示例，还可参阅综述 [Montanaro and de Wolf, 2013] 。由于酉信道的 Choi 秩为 1，而去极化信道的 Choi 秩为 $d_{\mathrm{in}}d_{\mathrm{out}}$，本研究是迈向实例最优量子信道认证的第一步，类似于经典情形 [Valiant and Valiant, 2016] 或量子态情形 [Chen et al., 2022a]。另一方面，对完全退极化信道进行恒等性检验，是对分布恒等性检验 [Diakonikolas et al., 2017] 以及态混合性检验 [Bubeck et al., 2020, Chen et al., 2022b]的推广。特别地，如果输入维度为 $d_{\mathrm{in}} = 1$，这些量子信道就是常量信道，该问题便归结为对维度为 d_{out}的量子态进行混合性检验。在这种情况下，我们得到 [Bubeck et al., 2020, Chen et al., 2022b]的最优复杂度。

另一项值得关注的工作是 [Chen 等人，2022c] 对幺正性进行估计。在这项工作中，研究表明，无辅助量子比特的非自适应策略可以使用 $\mathcal{O}(d^{0.5}/\varepsilon^2)$ 次测量，将 $\mathrm{Tr}(\mathcal{J}_{\mathcal{N}}^2)$ 估计到 ε 以内，其中 $\mathcal{J}_{\mathcal{N}}$ 是量子信道 $\mathcal{N}$ 的 Choi 态。特别是，这种估计可用于区分满足 $\mathrm{Tr}(\mathcal{J}_{\mathcal{N}}^2) = 1$ 的 $\mathcal{N} = \mathcal{N}_U$ 与满足 $\mathrm{Tr}(\mathcal{J}_{\mathcal{N}}^2) = 1/d^2$ 的 $\mathcal{N} = \mathcal{D}$。对于自适应策略， [Chen 等人，2022c] 给出了相匹配的下界（以 d 计），改进了此前 [Chen 等人，2022d] 给出的下界。这种复杂度似乎与我们的结果相矛盾，但事实并非如此。实际上，这类检验无法用于检验某个固定酉信道是否为恒等信道；例如，我们可以有两个在菱形距离上相差 ε 的酉信道。最后，我们注意到，针对量子态的检验问题也曾在相干策略或纠缠策略这一类情形下得到研究，在这种情形中，可以使用任意纠缠测量：例如， [Bˇadescu 等人， 2019] 研究了这一设定下的状态认证。本文聚焦于非相干策略，在这种策略中，不允许对量子信道的不同次调用使用纠缠输入，也不允许使用纠缠测量。

2 预备知识

我们考虑输入维度为 d_{in} 、输出维度为 d_{out}的量子信道。我们采用狄拉克符号：列向量记作 $|\phi\rangle$ ，其伴随记作 $\langle\phi| = |\phi\rangle^\dagger$。按照这种记号， $\langle\phi|\psi\rangle$ 是

向量 ϕ 和 ψ 的点积；对于单位向量 $|\phi\rangle \in \mathsf{S}^d$，$|\phi\rangle\langle\phi|$ 是投影到 ϕ张成的空间上的投影算符。标准基 $\{e_i\}_{i\in[d]}$ 记作 $\{|i\rangle\}_{i\in[d]} := \{|e_i\rangle\}_{i\in[d]}$。量子态是迹为 1 的半正定厄米矩阵。两个量子态之间的保真度定义为 $\mathrm{F}(\rho,\sigma) = \left(\text{迹}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right)^2$。保真度是对称的；若量子态 ρ或 σ 为秩一，则有更简洁的表达式：$\mathrm{F}(\rho,|\phi\rangle\langle\phi|) = \langle\phi|\rho|\phi\rangle$。一个 $(d_{\text{in}}, d_{\text{out}})$ 维量子信道是形如 $\mathcal{N}(\rho) = \sum_k A_k \rho A_k^\dagger$ 的映射 $\mathcal{N}: \mathbb{C}^{d_{\text{in}}\times d_{\text{in}}} \to \mathbb{C}^{d_{\text{out}}\times d_{\text{out}}}$（Kraus 分解），其中 Kraus 算子 $\{A_k\}_k$ 满足 $\sum_k A_k^\dagger A_k = \mathbb{I}$。例如，恒等映射 $\mathrm{id}_d(\rho) = \rho$ 可由 Kraus 算子 $\{\mathbb{I}_d\}$ 表示，而完全退极化信道 $\mathcal{D}(\rho) = \text{迹}(\rho)\,\mathrm{I}/d_{\text{out}}$ 可由 Kraus 算子 $\left\{\frac{1}{\sqrt{d_{\text{out}}}}|i\rangle\langle j|\right\}_{j\in[d_{\text{in}}],i\in[d_{\text{out}}]}$表示。给定酉矩阵 U，相应的酉信道 $\mathcal{N}_U(\rho) = U\rho U^\dagger$可由 Kraus 算子 $\{U\}$表示。我们用 $\mathrm{Haar}(d)$表示酉 $d\times d$ 矩阵紧群上的 Haar 概率测度。Haar 随机向量是 Haar 分布酉矩阵的任意列向量。

我们将两个量子信道 $\mathcal{N}$和 $\mathcal{M}$ 之间的迹距离定义为它们之差的迹范数：$d_{\mathrm{Tr}}(\mathcal{N},\mathcal{M}) := \max_\rho \|(\mathcal{N}-\mathcal{M})(\rho)\|_1$，其中最大化范围为所有量子态，而矩阵 M的 Schatten-p范数定义为 $\|M\|_p^p = \text{迹}\left(\sqrt{M^\dagger M}^p\right)$。在某些情况下，允许引入辅助系统并在其上施加恒等映射会有所帮助。此时，我们得到菱形距离，其形式化定义为 $d_\diamond(\mathcal{N},\mathcal{M}) := \max_\rho \|\mathrm{id}_d \otimes (\mathcal{N}-\mathcal{M})(\rho)\|_1$，其中最大化范围为所有量子态 $\rho \in \mathbb{C}^{d\times d}\otimes\mathbb{C}^{d_{\text{in}}\times d_{\text{in}}}$。请注意，根据施密特分解，我们总可以假设 $d = d_{\text{in}}$。迹距离/菱形距离可视为最坏情形距离，而我们可以用相应 Choi 态之间的 Schatten 2-范数定义平均情形距离。我们将量子信道 $\mathcal{N}$ 的 Choi 态定义为 $\mathcal{J}_\mathcal{N} = \mathrm{id}\otimes\mathcal{N}(|\Psi\rangle\langle\Psi|)$，其中 $|\Psi\rangle = \frac{1}{\sqrt{d_{\text{in}}}}\sum_{i=1}^{d_{\text{in}}}|i\rangle\otimes|i\rangle$ 为最大纠缠态。映射 $\mathcal{J}: \mathcal{N}\mapsto \mathrm{id}\otimes\mathcal{N}(|\Psi\rangle\langle\Psi|)$ 是一个同构，称为 Choi–Jamiołkowski 同构 [Choi，1975年，Jamiołkowski, 1972]。请注意，对于任意量子信道 $\mathcal{N}$，$\mathcal{J}_\mathcal{N}$均为半正定，并满足迹$_2(\mathcal{J}_\mathcal{N}) = \frac{\mathbb{I}}{d_{\text{in}}}$。此外，任何满足这些条件的 $\mathcal{K}$都称为 Choi 态，并且我们可以构造一个量子信道 $\mathcal{N}$，使得 $\mathcal{J}_\mathcal{N} = \mathcal{K}$。

我们考虑对固定量子信道进行恒等性检验的问题。给定一个固定量子信道 $\mathcal{N}_0$ 和精度参数 $\varepsilon > 0$，目标是以至少 $2/3$ 的概率检验未知量子信道 $\mathcal{N}$ 是否恰好为 $\mathcal{N}_0$，或与其相距 ε，即：

$$H_0 : \mathcal{N} = \mathcal{N}_0 \qquad \text{vs.} \qquad H_1 : \mathrm{dist}(\mathcal{N},\mathcal{N}_0) \geq \varepsilon$$

其中 $\mathrm{dist} \in \{d_\diamond, d_{\mathrm{Tr}}\}$。$H_0$ 称为零假设，而 H_1 称为备择假设。如果算法 $\mathcal{A}$ 在该问题上是 $1/3$-正确的，则当 H_0 成立时，它以至多 $1/3$ 的概率输出 H_1；当 H_1 成立时，它以至多 $1/3$ 的概率输出 H_0。如果 $0 < \mathrm{dist}(\mathcal{N},\mathcal{N}_0) < \varepsilon$，算法 $\mathcal{A}$ 可以输出任意假设。该检验的自然评价指标是菱形距离（分别为迹距离），因为在允许使用辅助系统（分别是不允许使用辅助系统）的情况下，它刻画了区分两个量子信道所需的最小错误概率 [Watrous, 2018]。

检验算法只能通过测量输出态，从未知量子信道 $\mathcal{N}$ 中提取经典信息。本文仅考虑非相干策略。也就是说，检验算法在每一步只能使用一个信道副本。换言之，对于一个 $(d_{\text{in}}, d_{\text{out}})$ 维量子信道，检验算法只能使用 d_{in} 维输入态和 d_{out} 维测量装置。具体而言，d 维测量由一个包含有限个元素的正算子值测度（POVM）定义：它是作用于希尔伯特空间 $\mathbb{C}^d$ 上的一组半正定矩阵 $\mathcal{M} = \{M_x\}_{x\in\mathcal{X}}$，并满足 $\sum_{x\in\mathcal{X}} M_x = \mathbb{I}$。POVM$\mathcal{M}$ 中的每个元素 M_x 都与测量结果 $x\in\mathcal{X}$ 相关联。元组 $\{\text{迹}(\rho M_x)\}_{x\in\mathcal{X}}$ 非负且总和为 1，因此定义了一个概率。玻恩规则 [Born, 1926] 指出，对量子态 ρ 使用 POVM $\mathcal{M}$ 进行测量时，输出 x 的概率恰好为迹(ρM_x)。根据是否允许使用辅助系统，我们将非相干策略分为两类。

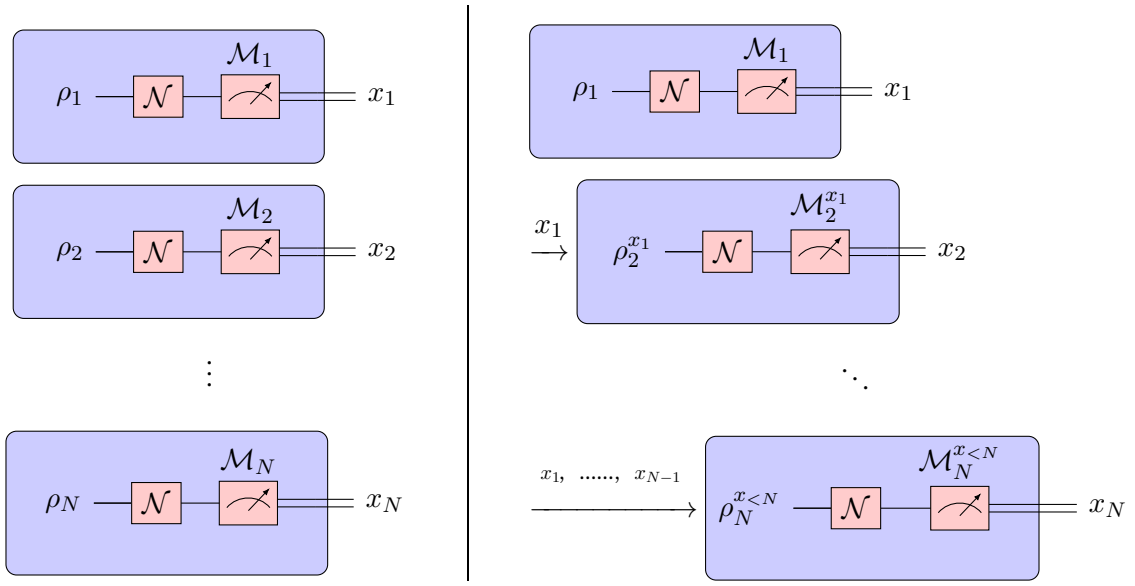

图1：用于检验量子信道恒等性的无辅助量子比特非相干非自适应（左）和自适应（右）策略示意图。随后，使用经典算法处理观测值（x_1、……、x_N），以回答 H_0 或 H_1。

• 无辅助系统策略。在每一步 t，学习者会选择一个 $d_{\text{输入}}$维量子态 ρ_t，以及一个 $d_{\text{输出}}$维测量装置 $\mathcal{M}_t = \{M_x^t\}_{x\in\mathcal{X}_t}$。因此，它以概率迹$(\mathcal{N}(\rho_t)M_{x_t}^t)$ 观测到测量结果 $x_t \in \mathcal{X}_t$。如果量子态 ρ_t 和测量装置 $\mathcal{M}_t$ 的选择可以依赖于先前的观测值 $(x_1, \ldots, x_{t-1})$，则该策略称为自适应策略；否则称为非自适应策略（示意见图 1）。

• 辅助系统辅助策略。在每一步 t，学习者会选择一个输入 $d_{\text{辅助量子比特}} \times d_{\text{输入}}$维状态$\rho_t \in \mathbb{C}^{d_{\text{辅助量子比特}}\times d_{\text{辅助量子比特}}} \otimes \mathbb{C}^{d_{\text{输入}}\times d_{\text{输入}}}$（对于任意给定的 $d_{\text{辅助量子比特}}$）以及一个 $d_{\text{辅助量子比特}} \times d_{\text{输出}}$维测量装置$\mathcal{M}_t = \{M_x^t\}_{x\in\mathcal{X}_t}$。因此，它以概率 $\text{Tr}(\text{id}_{d_{\text{辅助量子比特}}}\otimes\mathcal{N}(\rho_t)M_{x_t}^t)$ 观测到测量结果 $x_t \in \mathcal{X}_t$。如果状态 ρ_t 和测量装置 $\mathcal{M}_t$ 的选择可以取决于先前的观测值（x_1、……、x_{t-1}），则该策略称为自适应策略；否则称为非自适应策略（示意见图2）。

注意，我们可以将无辅助系统策略视为一种特殊的辅助系统策略，其中 d_{anc} =1。不过事实证明，在某些问题中，辅助系统辅助策略优于无辅助系统策略，例如 [Chen 等，2022e,d]。然而，在本文中，我们证明，对于检验一个固定酉信道或去极化信道是否为恒等信道，无辅助系统策略足以达到最优复杂度。

3 对酉信道进行恒等性检验

本节中，我们关注在菱形距离和迹距离下，对固定酉信道进行恒等性检验的问题。给定一个固定酉矩阵 U 和一个精度参数 $\varepsilon > 0$，目标是区分以下假设：

$$H_0 : \mathcal{N} = \mathcal{N}_U = U \cdot U^\dagger \quad \text{vs.} \quad H_1 : \text{dist}(\mathcal{N}, \mathcal{N}_U) \geq \varepsilon$$

至少以概率 $2/3$ 满足距离 dist $\in \{d_\diamond, d_{\text{Tr}}\}$。由于我们考虑的是酉信道，输入和输出维度应当相等 $d_{\text{in}} = d_{\text{out}} = d$。

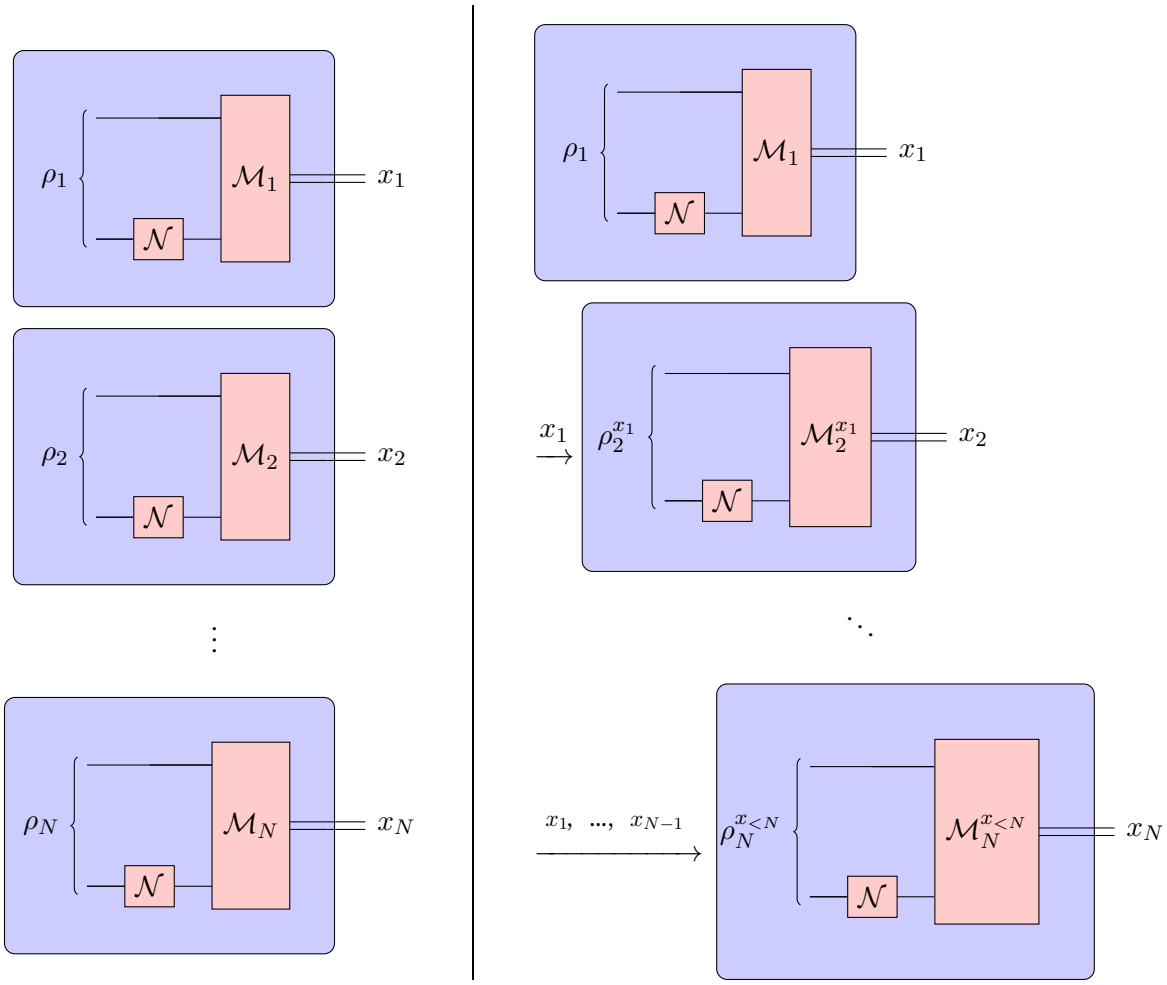

图2：用于检验量子信道恒等性的辅助量子比特辅助非自适应不相干策略（左）和自适应策略（右）示意图。随后，使用经典算法处理观测值（$x_1, \ldots, x_N$），以判断 H_0 还是 H_1。

化简为情形 $U = \mathbb{I}$。已知酉信道 $\mathcal{N}_U$ 等价于已知 U。因此，我们可以通过用 U 对测量装置进行共轭，将每个从恒等映射到 $\mathcal{N}_U$ 的恒等性检验化简为对 $\mathcal{N}_{\mathbb{I}} = \mathrm{id}_d$ 的恒等性检验。这是可行的，因为迹距离／菱形距离具有酉不变性：$\mathrm{dist}(\mathcal{N}, \mathcal{N}_U) = \mathrm{dist}(U^\dagger \mathcal{N} U, \mathrm{id})$，且对所有 ρ 和 M，$\mathrm{Tr}(U^\dagger \mathcal{N}(\rho) U M) = \mathrm{Tr}(\mathcal{N}(\rho) U M U^\dagger)$。从现在起，我们只考虑情形 $U = \mathbb{I}$，并将这个特定的对 $\mathcal{N}_{\mathbb{I}} = \mathrm{id}_d$ 的检验问题简称为“恒等信道到恒等信道测试”。

鉴于菱形距离和迹距离的性质，在备择假设下，量子信道 $\mathcal{N}$ 除了某个状态的一个邻域外，可能与恒等信道相同。此外，学习者并不知道该状态。当算法允许使用辅助系统时，可以将最大纠缠态 $|\Psi\rangle\langle\Psi|$ 作为输入，从而制备该量子信道 $\mathcal{N}$ 的 Choi 态 $\mathcal{J}_{\mathcal{N}}$（它基本上包含了关于该量子信道的一切信息）。在零假设 H_0 下，Choi 态恰好为 $\mathcal{J}_{\mathrm{id}} = \mathrm{id} \otimes \mathrm{id}(|\Psi\rangle\langle\Psi|) = |\Psi\rangle\langle\Psi|$；而在备择假设 H_1 下，Choi 态 $\mathcal{J}_{\mathcal{N}}$ 与 $|\Psi\rangle\langle\Psi|$ 的保真度满足：

$$\mathrm{Tr}(\mathrm{id} \otimes \mathcal{N}(|\Psi\rangle\langle\Psi|)\,|\Psi\rangle\langle\Psi|) = \mathrm{F}(\mathcal{J}_{\mathcal{N}}, |\Psi\rangle\langle\Psi|) \leq 1 - \frac{1}{4}\,\|\mathcal{J}_{\mathcal{N}} - \mathcal{J}_{\mathrm{id}}\|_1^2 \leq 1 - \frac{d_\diamond(\mathcal{N}, \mathrm{id})^2}{4d^2}$$

其中我们使用了 Fuchs–van de Graaf 不等式 [Fuchs 和 Van De Graaf，1999]，以及一个标准不等式，该不等式将两个量子通道之间的菱形范数与其对应 Choi

态之间的迹范数联系起来：$\|\mathcal{J}_{\mathcal{N}} - \mathcal{J}_{\mathcal{M}}\|_1 \geq {}^{d_\diamond(\mathcal{N},\mathcal{M})}\, d$（例如，Jenˇcová 和 Plávala [2016]）。因此，使用正算子值测度$\mathcal{M}_\Psi = \{|\Psi\rangle\langle\Psi|, \mathbb{I} - |\Psi\rangle\langle\Psi|\}$ 的测量可以区分这两种情况。然而，如果测试者不允许使用辅助系统，就既无法制备 Choi 态 $\mathcal{J}_{\mathcal{N}}$，也无法使用正算子值测度$\mathcal{M}_\Psi$进行测量。相反，我们使用一个随机的 d 维秩 1 输入态。事实上，这种选择很自然，因为输入态 $|\phi\rangle\langle\phi|$ 与输出态 $\mathcal{N}(|\phi\rangle\langle\phi|)$ 之间的期望保真度可以很容易地与 Choi 态之间的保真度联系起来：$\mathrm{E}_{|\phi\rangle\sim\mathrm{Haar}}\,[\mathrm{F}(\mathcal{N}(|\phi\rangle\langle\phi|),\ |\phi\rangle\langle\phi|)] = {}^{1+d}\,\mathrm{F}(\mathcal{J}_{\mathcal{N}},|\Psi\rangle\langle\Psi|)\,{}^{1+d}$（证明见引理 A.1）。这个引理广为人知，因为它联系了平均保真度 $\mathrm{E}_{|\phi\rangle\sim\mathrm{Haar}}\,[\mathrm{F}(\mathcal{N}(|\phi\rangle\langle\phi|),\ |\phi\rangle\langle\phi|)]$与纠缠保真度 $\mathrm{F}(\mathcal{J}_{\mathcal{N}},|\Psi\rangle\langle\Psi|)$。若使用测量装置 $\mathcal{M}_\phi = \{|\phi\rangle\langle\phi|, \mathbb{I} - |\phi\rangle\langle\phi|\}$进行测量，则在 H_0 下错误概率为 0，而在 H_1 下错误概率为 $\mathrm{E}_{|\phi\rangle\sim\mathrm{Haar}}[\langle\phi|\mathcal{N}(|\phi\rangle\langle\phi|)\ |\phi\rangle] = \mathrm{E}_{|\phi\rangle\sim\mathrm{Haar}}[\mathrm{F}(\mathcal{N}(|\phi\rangle\langle\phi|),\ |\phi\rangle\langle\phi|)]$。该算法详见算法 1。

算法 1：在菱形距离/迹距离下进行恒等信道到恒等信道测试

$N = \mathcal{O}(d/\varepsilon^4)$（在迹距离下测试时，替换为 $N = \mathcal{O}(d/\varepsilon^2)$）。

对于 $k = 1$： N 执行

在 S^d 中采样一个 Haar 随机向量 ϕ_k。

使用正算子值测度 $\{|\phi_k\rangle\langle\phi_k|, \mathbb{I} - |\phi_k\rangle\langle\phi_k|\}$ 测量输出态 $\mathcal{N}(|\phi_k\rangle\langle\phi_k|)$。

观察 $X_k \sim$ 伯努利分布$(1 - \langle\phi_k|\mathcal{N}(|\phi_k\rangle\langle\phi_k|)\ |\phi_k\rangle)$。

结束循环

如果 $\exists k$： ${}^{X_k} = 1$则返回 $\mathcal{N}$ 与 id 的距离为 ε；否则返回 $\mathcal{N} = \mathrm{id}$。

利用众所周知的引理A.1和我们的引理A.3，可以给出 H_1 下错误概率的上界：

$$\mathbb{E}_{|\phi\rangle\sim\mathrm{Haar}}\,[\mathrm{F}(\mathcal{N}(|\phi\rangle\langle\phi|),|\phi\rangle\langle\phi|)] = \frac{1 + d\,\mathrm{F}(\mathcal{J}_{\mathcal{N}},|\Psi\rangle\langle\Psi|)}{1+d} \leq 1 - \frac{d_{\mathrm{Tr}}(\mathcal{N},\mathrm{id})^2}{4(d+1)} \leq 1 - \frac{d_\diamond(\mathcal{N},\mathrm{id})^4}{16(d+1)}.$$

注意，标准不等式 $\|\mathcal{J}_{\mathcal{N}} - \mathcal{J}_{\mathcal{M}}\|_1 \geq {}^{d_\diamond(\mathcal{N},\ \mathcal{M})}\, d$意味着：$\mathrm{E}_\phi\,[\mathrm{F}(\mathcal{N}(|\phi\rangle\langle\phi|)\ |\phi\rangle\langle\phi|)] \leq 1 - {}^{d_\diamond\left(\mathcal{N},\ \frac{}{4d,d+1}\right)^2}$, $\mathrm{id})()$，其对菱形距离的依赖更优，但对维度 d的依赖更差。这个简单的引理（引理A.3）描述了其中一个量子信道为酉矩阵时纠缠保真度与迹距离/菱形距离之间的关系，或许本身也值得关注。要获得一个 $1/3$ 正确的算法，只需在迹距离的情况下重复所述过程，使用 $N = \mathcal{O}(d/\varepsilon^2)$个 $|\phi\rangle\langle\phi|$ 副本；在菱形距离的情况下则使用$N = \mathcal{O}(d/\varepsilon^4)$个 $|\phi\rangle\langle\phi|$ 副本。事实上，例如对于迹距离， H_1 下的错误概率可按如下方式控制：

$$\begin{aligned}\mathbb{P}_{H_1}(\text{error}) = \mathbb{P}_{H_1}(\forall k \in [N] : X_k = 0) &= \prod_{k=1}^{N} \mathbb{P}_{H_1}(X_k = 0) \\ &\leq \left(1 - \frac{\varepsilon^2}{4(d+1)}\right)^N \leq \exp\left(-\frac{\varepsilon^2 N}{4(d+1)}\right) \leq \frac{1}{3}\end{aligned}$$

对于 $N = 4\log(3)(d+1)/\varepsilon^2 = \mathcal{O}(d/\varepsilon^2)$ [1]。类似的证明表明， $\mathcal{O}(d/\varepsilon^4)$ 个副本足以进行菱形距离测试。至此，算法 1 的正确性得证。附录 B 中证明了匹配的下界 $N = \Omega\left(\frac{d}{\varepsilon^2}\right)$。为此，我们构造了一个与恒等信道在迹距离/菱形距离上相距 ε 的随机量子信道，但对于大多数输入态而言，它看起来与恒等信道相似。然后，我们利用 KL 散度比较两个假设下的观测值。有趣的是，类似的经典问题——恒等映射到恒等映射测试——其复杂度为 $\Theta(d/\varepsilon)$。因此，对于这项任务，当

[1]本文中的所有对数均以 e 为底，信息量以“奈特”为单位。

转向量子情形时，对维度 d 的依赖保持不变，而对精度参数 ε 的依赖则从 ε 变为 ε^2。事实上，获得正确的 ε^2 依赖关系是这个下界证明的主要难点。这需要一种经过精心选择的构造，其灵感来自 Audenaert 的量子偏斜散度 [, 2014] 并结合使用 Weingarten演算进行的精细分析。我们在下面的定理中总结本节的主要结果。

定理 3.1. 存在一种非相干无辅助系统算法，仅使用 $N = \mathcal{O}\left(\frac{d}{\varepsilon^2}\right)$ 次测量，即可通过迹距离检验恒等信道到恒等信道。此外，该算法也能仅使用 $N = \mathcal{O}\left(\frac{d}{\varepsilon^4}\right)$ 次测量，通过菱形距离解决恒等到恒等测试问题。另一方面，任何非相干自适应辅助系统策略，在最坏情况下都需要满足 $N = \Omega\left(\frac{d}{\varepsilon^2}\right)$ 的测量次数，才能以至少 $2/3$ 的概率区分 $\mathcal{N} = \mathrm{id}$ 与 $d_\diamond(\mathcal{N}, \mathrm{id}) > \varepsilon$（或 $d_{\mathrm{Tr}}(\mathcal{N}, \mathrm{id}) > \varepsilon$）。

4 恒等信道与去极化信道的检验

本节转而研究通过菱形距离检验恒等信道与完全退极化信道的问题。给定精度参数 $\varepsilon > 0$ 和未知量子信道 $\mathcal{N}$，我们希望以至多 $1/3$ 的错误概率检验 H_0：$\mathcal{N} = \mathcal{D}$ 还是 H_1：$d_\diamond(\mathcal{N}, \mathcal{D}) \geq \varepsilon$。若 $\mathcal{N} = \mathcal{D}$，测试者应以至少 $2/3$ 的概率给出零假设 H_0；而若 $d_\diamond(\mathcal{N}, \mathcal{D}) \geq \varepsilon$，测试者应以至少 $2/3$ 的概率给出备择假设 H_1。备择条件意味着

$$d_\diamond(\mathcal{N}, \mathcal{D}) \geq \varepsilon \iff \exists\, |\phi\rangle \in \mathbf{S}^{d_{\mathrm{in}} \times d_{\mathrm{in}}} : \left\| \mathrm{id}_{d_{\mathrm{in}}} \otimes \mathcal{N}(|\phi\rangle\langle\phi|) - \mathrm{id}_{d_{\mathrm{in}}} \otimes \mathcal{D}(|\phi\rangle\langle\phi|) \right\|_1 \geq \varepsilon.$$

这个不等式给出了 Choi 态之间 1-范数的下界：$\|\mathcal{J}_\mathcal{N} - \mathcal{J}_\mathcal{D}\|_1 \geq \frac{\varepsilon}{d_{\mathrm{in}}}$。最简单的想法是利用这个不等式，将量子通道检验问题化归为量子态检验。事实上，这种从量子通道到量子态的化归已用于量子过程层析[Surawy-Stepney 等人, 2022] 以及影子过程层析 [Kunjummen 等人, 2021]。去极化信道 $\mathcal{D}$ 的 Choi 态为$\mathcal{J}_\mathcal{D} = \frac{1}{d_{\mathrm{in}}} \sum_{i,\, j=1}^{d_{\mathrm{in}}} |i\rangle\langle j| \otimes \mathrm{Tr}(|i\rangle\langle j|) \frac{\mathbb{I}}{d_{\mathrm{out}}} = \frac{\mathbb{I}_{d_{\mathrm{in}}} \otimes \mathbb{I}_{d_{\mathrm{out}}}}{d_{\mathrm{in}} d_{\mathrm{out}}} = \frac{\mathbb{I}_{d_{\mathrm{in}} d_{\mathrm{out}}}}{d_{\mathrm{in}} d_{\mathrm{out}}}$，因此应用前述不等式，对于与去极化信道相差 $\mathcal{N}$ ε的量子信道$\mathcal{D}$，可得：$\left\| \mathcal{J}_\mathcal{N} - \frac{\mathbb{I}}{d_{\mathrm{in}} d_{\mathrm{out}}} \right\|_1 \geq \frac{\varepsilon}{d_{\mathrm{in}}}$.然后，我们可以应用量子态混合性测试[Bubeck 等人, 2020]的化归，设计一种辅助系统策略，所需测量次数为 $\mathcal{O}\left(\frac{d_{\mathrm{in}}^{1.5} d_{\mathrm{out}}^{1.5}}{\varepsilon / d_{\mathrm{in}}()^2}\right) = \mathcal{O}\left(\frac{d_{\mathrm{in}}^{3.5} d_{\mathrm{out}}^{1.5}}{\varepsilon^2}\right)$，因为量子态 $\mathcal{J}_\mathcal{N}$和$\frac{\mathbb{I}}{d_{\mathrm{in}} d_{\mathrm{out}}}$的维数为 $d_{\mathrm{in}} d_{\mathrm{out}}$，且精度参数为$\frac{\varepsilon}{d_{\mathrm{in}}}$。然而，这种方法有两个问题。首先，我们必须能够使用辅助系统来制备 Choi 态$\mathcal{J}_\mathcal{N}$，这是一项额外资源。其次，复杂度 $\mathcal{O}\left(\frac{d_{\mathrm{in}}^{3.5} d_{\mathrm{out}}^{1.5}}{\varepsilon^2}\right)$并非最优，正如我们稍后将看到的那样。如果尝试在 2-范数下化归为量子态恒等性测试（附录 E），可以得到稍好一些但仍非最优的界，而且仍需要使用辅助系统。

受恒等到恒等测试问题（第 3 节）的启发，当我们不知道某个最优输入态时，就将其选为随机态。设 $|\phi\rangle$ 是一个 Haar 随机向量。如果输入态为 $|\phi\rangle\langle\phi|$，则在 H_0 下的输出态为 $\mathcal{D}(|\phi\rangle\langle\phi|) = \frac{\mathbb{I}}{d_{\mathrm{out}}}$，而在 H_1 下的输出态为 $\mathcal{N}(|\phi\rangle\langle\phi|)$。因此，自然会问 $\mathcal{N}(|\phi\rangle\langle\phi|)$ 与 $\frac{\mathbb{I}}{d_{\mathrm{out}}}$ 之间的距离是多少。请注意，通常计算 2-范数的期望比计算 1-范数的期望容易得多。为此，我们先计算 $\mathcal{N}(|\phi\rangle\langle\phi|)$ 与 $\frac{\mathbb{I}}{d_{\mathrm{out}}}$ 之间 2-范数的期望（证明见引理 C.2）。

引理 4.1。设 $\mathcal{M} = \mathcal{N} - \mathcal{D}$ 和 $\mathcal{J}_\mathcal{M} = \mathrm{id} \otimes \mathcal{M}(|\Psi\rangle\langle\Psi|)$。我们有：

$$\mathbb{E}_{|\phi\rangle \sim \mathrm{Haar}} \left(\|\mathcal{M}(|\phi\rangle\langle\phi|)\|_2^2 \right) = \frac{\|\mathcal{M}(\mathbb{I})\|_2^2 + d_{\mathrm{in}}^2 \|\mathcal{J}_\mathcal{M}\|_2^2}{d_{\mathrm{in}}(d_{\mathrm{in}} + 1)} \geq \frac{d_{\mathrm{in}}}{d_{\mathrm{in}} + 1} \|\mathcal{J}_\mathcal{M}\|_2^2 .$$

现在我们需要将量子信道 $\mathcal{N}$ 的 Choi 态与去极化量子信道 $\|\mathcal{J}_{\mathcal{N}}-\mathcal{J}_{\mathcal{D}}\|_2$ 的 Choi 态之间的 2-范数，与它们之间的菱形距离 $d_\diamond(\mathcal{N},\mathcal{D})$ 联系起来。这由下面的引理给出，其证明见附录 C.1：

引理4.2。设 $\mathcal{N}_1$ 和 $\mathcal{N}_2$ 是两个（d_{in}， d_{out}）-量子信道。我们有：

$$\|\mathcal{J}_{\mathcal{N}_1}-\mathcal{J}_{\mathcal{N}_2}\|_2 \geq \frac{d_\diamond(\mathcal{N}_1,\mathcal{N}_2)}{d_{\text{in}}\sqrt{d_{\text{out}}}}.$$

设 $\mathcal{N}$ 是满足 $d_\diamond(\mathcal{N},\ \mathcal{D})\geq\varepsilon$ 且 $X=\left\|\mathcal{N}(|\phi\rangle\langle\phi|)-\frac{\mathbb{I}}{d_{\text{out}}}\right\|_2^2$ 的量子信道，根据引理4.1、4.2，我们得到：

$$\mathbb{E}(X)=\mathbb{E}_{|\phi\rangle\sim\text{Haar}}\left(\left\|\mathcal{N}(|\phi\rangle\langle\phi|)-\frac{\mathbb{I}}{d_{\text{out}}}\right\|_2^2\right)\geq\frac{d_{\text{in}}}{d_{\text{in}}+1}\left\|\mathcal{J}_{\mathcal{N}}-\frac{\mathbb{I}}{d_{\text{in}}d_{\text{out}}}\right\|_2^2\geq\frac{\varepsilon^2}{2d_{\text{in}}^2d_{\text{out}}}. \tag{1}$$

如果我们能够证明 X 以恒定概率大于 Ω(E（X）)，那么我们就可以将问题约化为通常的 2-范数量子态恒等性检验（附录 E 中的量子态认证），并使用 $\mathcal{O}\left(\frac{\sqrt{d_{\text{out}}}}{\varepsilon/d_{\text{in}}\sqrt{d_{\text{out}}}()^2}\right)=\mathcal{O}\left(\frac{d_{\text{in}}^2d_{\text{out}}^{1.5}}{\varepsilon^2}\right)$ 次测量得到一种非相干无辅助系统算法。事实证明，建立这一点是证明中技术性最强的部分，以下定理对此进行了总结。

定理4.3。设 $|\phi\rangle$ 是 S^d 中的 Haar 分布向量（或任意 4-设计）。设 $X=\left\|\mathcal{N}(|\phi\rangle\langle\phi|)-\frac{\mathbb{I}}{d_{\text{out}}}\right\|_2^2$。我们有：

$$\text{Var}(X)=\mathcal{O}\left([\mathbb{E}(X)]^2\right).$$

这个定理是本文中技术性最强的部分，我们相信采用类似的方法可以将其推广到任意两个量子信道之差。此外，将这个不等式与 Paley-Zygmund 不等式结合使用，足以完成我们的归约：对于恒等信道到去极化信道测试，只需重复我们的测试 $\mathcal{O}(1)$ 次，即可将错误概率降至 $1/3$。

证明概要。我们首先观察到 $\text{Var}(X)=\text{Var}\left(\text{Tr}[(\mathcal{N}(|\phi\rangle\langle\phi|))^2]\right)$。然后利用 Weingarten演算（引理 F.1、F.3），可以计算出期望

$$\mathbb{E}\left(\left(\text{Tr}[(\mathcal{N}(|\phi\rangle\langle\phi|))^2]\right)^2\right)=\frac{1}{d_{\text{in}}(d_{\text{in}}+1)(d_{\text{in}}+2)(d_{\text{in}}+3)}\sum_{\alpha\in\mathfrak{S}_4}F(\alpha)$$

其中，对于 $\alpha\in\mathfrak{S}_4$，$F(\alpha)=\sum_{i,j,k,l,k',l'}\text{Tr}_\alpha(A_{l'}^\dagger|j\rangle\langle i|A_k,A_k^\dagger A_l,A_l^\dagger|i\rangle\langle j|A_{k'},A_{k'}^\dagger A_{l'})$，且 $\text{Tr}_\alpha(M_1,\ldots,M_n)=\Pi_j\text{Tr}(\Pi_{i\in C_j}M_i)$，其中 $\alpha=\Pi_jC_j$和 C_j是循环。令 $m=\left\|\mathcal{N}(\mathbb{I})-\frac{d_{\text{in}}}{d_{\text{out}}}\mathbb{I}\right\|_2$和 $\eta=d_{\text{in}}\left\|\mathcal{J}_{\mathcal{N}}-\frac{\mathbb{I}}{d_{\text{in}}d_{\text{out}}}\right\|_2$。接下来，我们给出函数 F的上界，如表 2 所示。这是证明中最困难的一步，需要对许多 $F(\alpha)'s$进行细致分析。我们反复使用的一个特别有用的技巧称为复制技巧：若 $\mathsf{F}=\sum_{i,j=1}^d(|i\rangle\otimes|j\rangle)(\langle j|\otimes\langle i|)$ 是翻转算子，则对所有 $A,B\in\mathbb{C}^{d\times d}$，有：$\text{Tr}((A\otimes B)\mathsf{F})=\text{Tr}(AB)$，类似地，$\text{Tr}(A\otimes B)=\text{Tr}(A)\text{Tr}(B)$。此外，我们还经常需要使用另一个技巧，即利用部分转置使半正定矩阵 $M^\dagger M=\sum_{k,l}A_k^\dagger A_l\otimes A_k^\top\bar{A}_l$和 $MM^\dagger=\sum_{k,l}A_kA_l^\dagger\otimes\bar{A}_kA_l^\top$出现，其中 $M=\sum_kA_k\otimes A_k$ 由量子信道 $\mathcal{N}$的 Kraus 算子 $\{A_k\}_k$ 定义。此外，我们可以证明近似关系 $\left\|M^\dagger M-\frac{d_{\text{in}}}{d_{\text{out}}}|\Psi\rangle\langle\Psi|\right\|_1\leq 5\eta^2$，其中$|\Psi\rangle=\frac{1}{\sqrt{d_{\text{in}}}}\sum_{i=1}^{d_{\text{in}}}|i\rangle\otimes|i\rangle$ 是最大纠缠态（见引理 C.6）。这一结果用于 $\alpha=$ (142) 和 (24)。一种应用

排列 α	$F(\alpha)$ 的上界	参考文献
(13)	$\left(\frac{d_{\text{in}}}{d_{\text{out}}}+\eta^2\right)^2$	
id, (132), (314), (24)(13)	$\frac{d_{\text{in}}/d_{\text{out}}+\eta^2}{d_{\text{out}}}+\frac{\eta^2}{d_{\text{out}}}+5\eta^4$	(引理 C.8)
(312), (134)	$\left(\frac{d_{\text{in}}^2}{d_{\text{out}}}+m^2\right)\left(\frac{d_{\text{in}}}{d_{\text{out}}}+\eta^2\right)$	
(1234)	$\left(\frac{d_{\text{in}}^2}{d_{\text{out}}}+m^2\right)^2$	
(24), (1432)	$\frac{d_{\text{in}}^2}{d_{\text{out}}^2}+\frac{2m^2}{d_{\text{out}}}+25\eta^4$	(引理 C.9)
(142), (243)	$\frac{d_{\text{in}}/d_{\text{out}}+\eta^2}{d_{\text{out}}}+\frac{\eta^2}{d_{\text{out}}}+5\eta^4$	(引理 C.7)
(14)、(12)、(23)、(34)、(1324)、(1423), (1243), (1342)	$\frac{d_{\text{in}}^2}{d_{\text{out}}^2}+\frac{d_{\text{in}}}{d_{\text{out}}}\eta^2+\frac{m^2}{d_{\text{out}}}+5m\eta^3$	（引理 C.11）
(12)(34), (14)(23), (234), (124)	$\frac{d_{\text{in}}^3}{d_{\text{out}}^2}+2\frac{d_{\text{in}}}{d_{\text{out}}}m^2+m^2\eta^2$	（引理 C.10）

表 2：不同输入排列下函数 F 的上界。

对前述近似应用数据处理不等式，得到：$\left\|\text{Tr}_2(M^\dagger M)-\frac{1}{d_{\text{out}}}\mathbb{I}\right\|_1 \le 5\eta^2$，该结果用于排列 $\alpha=$ id 和 (14)。事实证明，应用这种近似无法为 F((12)(34)) 给出足够好的上界，因为它可以写成 F((12)(34)) $=\text{Tr}\left(\left(MM^\dagger\right)^{T_2}\cdot\mathcal{M}(\mathbb{I})^{\otimes 2}\text{F}\right)+\frac{d_{\text{in}}^3}{d_{\text{out}}^2}+2\frac{d_{\text{in}}}{d_{\text{out}}}\text{Tr}(\mathcal{M}(\mathbb{I})^2)$，其依赖的反而是矩阵 $MM^\dagger$。在这种情况下，我们将 $MM^\dagger$投影到与 $|\Psi\rangle$正交的超平面上。对此可以用表示论来解释。事实上，由 $|\Psi\rangle$ 及其补空间张成的空间，是在 U 为酉矩阵时，群 $U\otimes\bar{U}$ 作用下空间 $\left(\mathbb{C}^d\right)^{\otimes 2}$ 的两个不可约表示。另一方面，在量子信道 $\mathcal{N}$ 的表达式中更换 Kraus 算子 $A_k\leftrightarrow UA_k$ 或 $A_k\leftrightarrow A_kU$，不会影响 X 的方差，因为 Haar测度在酉矩阵的左乘和右乘下保持不变。这些上界的详细证明见附录C.3。

现在我们已经具备了所需的工具，可以设计一个用于检验量子信道是否为去极化信道的算法，并证明该算法的正确性。

定理 **4 4** $N=$。存在一种非相干无辅助系统算法，所需的测量次数为 $\mathcal{O}\left(\frac{d_{\text{in}}^2 d_{\text{out}}^{1.5}}{\varepsilon^2}\right)$，能够以成功概率 $\mathcal{N}=\mathcal{D}$ $d_\diamond\,\mathcal{N}\;\mathcal{D}\;\ge\varepsilon$ $2/3$ 区分 和 (,)。

如前文所述，我们的算法可归约为量子态恒等性检验。为方便读者，我们在附录 E 中给出了该检验及其正确性的证明。请注意，我们需要在 2-范数下对量子态进行检验，这不同于通常的量子态认证 [Bubeck 等人，2020]。恒等信道到去极化信道测试的算法见算法 2。

我们指出，算法 2 仅在数量为常数的随机输入态 $\{|\phi_k\rangle\langle\phi_k|\}_k$ 上使用该量子信道。人们可能会认为，在更多样化的输入 $\mathcal{N}$ 上查询该量子信道，能够得到更高效的算法。然而，事实证明，算法 2 基本上是最优的，正如我们通过证明一个匹配的下界（仅相差一个多对数因子）所示。

定理4.5. 设 $\varepsilon\le 1/32$, $d_{\text{in}}\ge 80$ 和 $d_{\text{out}}\ge 10$。任何用于恒等信道到去极化信道测试（针对迹距离和菱形距离）的辅助系统辅助的非自适应算法，在最坏情况下所需的测量次数满足：

$$N=\Omega\left(\frac{d_{\text{in}}^2 d_{\text{out}}^{1.5}}{\log(d_{\text{in}}d_{\text{out}}/\varepsilon)^2\varepsilon^2}\right).$$

算法 2：恒等信道到去极化信道的菱形范数测试

$M = 2200$。对于 $k = 1:\ M$，执行以下操作：采样 ϕ_k 一个来自 $\mathsf{S}^{d_{\text{in}}}$ 的 Haar 随机向量。使用量子态恒等性检验算法 3 测试 $h_0:\ \mathcal{N}(|\phi_k\rangle\langle\phi_k|) = \frac{\mathbb{I}}{d_{\text{out}}}$还是 $h_1:\ \left\|\mathcal{N}(|\phi_k\rangle\langle\phi_k|) - \frac{\mathbb{I}}{d_{\text{out}}}\right\|_2 \geq \frac{\varepsilon}{2\sqrt{d_{\text{out}}d_{\text{in}}}}$，错误概率为 $\delta = 1/(3M)$，并回答假设h_{i_k}, $i_k \in \{0, 1\}$。结束循环。如果 $\exists k:\ i_k = 1$，则返回 $\mathcal{N}$与 $\mathcal{D}$ 相距至少 ε；否则返回 $\mathcal{N} = \mathcal{D}$。

该定理表明，我们提出的算法 2 在维数 $(d_{\text{in}}, d_{\text{out}})$ 和精度参数 ε 下几乎是最优的，因此恒等信道到去极化信道测试的复杂度为 $\tilde{\Theta}(d_{\text{in}}^2 d_{\text{out}}^{1.5}/\varepsilon^2)$，这略微令人意外。事实上，我们可以指出，在相同设置下，离散分布和量子态的恒等性检验复杂度是相应学习问题复杂度的平方根（当 ε 为常数时）。这条规律不适用于量子信道，因为我们从[Surawy-Stepney 等，2022，Oufkir， 2023] 得知，采用非自适应非相干策略，以菱形距离学习量子信道的复杂度为 $\tilde{\Theta}(d_{\text{in}}^3 d_{\text{out}}^3/\varepsilon^2)$。

证明概要。在零假设下 $\mathcal{N} = \mathcal{D}$。在备择假设下，我们随机构造如下形式的量子信道 $\mathcal{N} \sim \mathcal{P}$：$\mathcal{N}(\rho) = \mathcal{D}(\rho) + \frac{\varepsilon}{d_{\text{out}}\|u\|_2^2} \langle u|\rho|u\rangle U$，其中 $|u\rangle$ 是一个标准高斯向量，而 U 具有高斯元素：对于所有 $i \leq j \in [d_{\text{out}}]$, $U_{j,\ i} = U_{i,\ j} \sim \mathbf{1}\{i \neq j\}\mathcal{N}_c(0, 16/d_{\text{out}})$，并以事件 $\mathcal{G} = \{\|U\|_1 \geq d_{\text{out}}, \|U\|_\infty \leq 32\}$ 为条件。请注意，对 Choi 态应用通常的构造，在迹距离或菱形距离下会得到次优下界。利用高斯随机变量的 Lipschitz 函数集中不等式 [Wainwright, 2019], ，我们证明以高概率 $\mathcal{N}$ 在迹距离和菱形距离下与 $\mathcal{D}$ 相距至少 ε。随后，我们使用 Le Cam 方法，对两个假设下观测值分布之间的全变差距离给出下界：$\text{TV}\left(\mathrm{P}_{\mathcal{D}}^{I_1 \cdots I_N}\right\|, \ , \ \mathrm{E}_{\mathcal{N}\sim\mathcal{P}}\mathrm{P}_{\mathcal{N}}^{I_1 \cdots I_N}\Big) \geq \frac{1}{3}, \ , \ ,$ 其中 $I_1, \ldots, I_N$ 是算法在完成测量后获得的观测值，而 N 是保证算法正确性所需的测量次数。我们不失一般性地假设输入态是纯态 $\rho_t = |\psi_t\rangle\langle\psi_t|$ ，且测量装置由如下形式的正算子值测度给出 $\mathcal{M}_t = \{\lambda_{i_t}^t \left|\phi_{i_t}^t\right\rangle\!\left\langle\phi_{i_t}^t\right|\}$。此外，我们可以写出

$$|\psi_t\rangle = A_t \otimes \mathbb{I}\,|\Psi_{d_{\text{in}}}\rangle\,, \left|\phi_{i_t}^t\right\rangle = B_{i_t}^t \otimes \mathbb{I}\,|\Psi_{d_{\text{out}}}\rangle \quad \text{where} \quad |\Psi_d\rangle = \frac{1}{\sqrt{d}}\sum_{i=1}^{d}|ii\rangle\,.$$

然后我们以事件 $\mathcal{E}$ 为条件，即 u 满足 $\|u\|_2 \geq \sqrt{\frac{d_{\text{in}}}{6}}$且

$$\forall t \in [N] : P_u^t = \sum_{i_t, j_t} \frac{\lambda_{i_t}^t \lambda_{j_t}^t \langle u|\, A_t^\dagger B_{i_t}^t B_{j_t}^{t,\dagger} A_t\, |u\rangle^4}{\mathrm{Tr}(B_{i_t}^{t,\dagger} A_t A_t^\dagger B_{i_t}^t)\mathrm{Tr}(B_{j_t}^{t,\dagger} A_t A_t^\dagger B_{j_t}^t)} \leq (7\log(N))^4 d_{\text{in}}^2 d_{\text{out}}^3. \tag{2}$$

注意到， P_u^t 是关于 u各元素的 8 次多项式。我们可以利用由高斯多项式超收缩性 [推导出的集中不等式（Aubrun 和 Szarek，2017，推论 5）以及并合界，证明事件 $\mathcal{E}$ 以至少 $9/10$ 的概率发生。注意，这里的并合界只会增加一个 $\log(N)^4$ 因子，因为对于非自适应策略，输入/测量对最多有 N 个。为了进行分析，我们需要给随机变量的矩一个上界：

$$Z_t(U, V) = \varepsilon^2 \mathbb{E}_{i_t}\left[\Phi_{u,U}^{t,i_t}\Phi_{v,V}^{t,i_t}\right] \quad \text{where} \quad \Phi_{u,U}^{t,i_t} = \frac{\mathrm{Tr}(B_{i_t}^{t,\dagger} A_t\, |u\rangle\langle u|\, A_t^\dagger B_{i_t}^t U)}{\|u\|_2^2 \mathrm{Tr}(B_{i_t}^{t,\dagger} A_t A_t^\dagger B_{i_t}^t)}.$$

由于 Z_t 是关于 U 和 V 各元素的 2 次多项式，且期望为 0，因此超收缩性[（Aubrun 和 Szarek, 2017，命题 5.48]）对所有 $k \in \{1, \ldots, N\}$ 均有：$\mathrm{E}\left(|Z_t|^k\right) \leq k^k \mathrm{E}\left(Z_t^2\right)^{k/2}$。因此，只需对二阶矩求上界，这可以利用不等式（2）得到：$\mathrm{E}\left(Z_t^2\right) \leq \mathcal{O}\left(\frac{\varepsilon^4 \log(N^4)}{d_{\mathrm{in}}^4 d_{\mathrm{out}}^3}\right)$。通过反证法并将所有这些元素分组，我们可以证明 $N\log(N)^2 \geq \Omega\left(\frac{d_{\mathrm{in}}^2 d_{\mathrm{out}}^{1.5}}{\varepsilon^2}\right)$，最终得到 $N \geq \Omega\left(\frac{d_{\mathrm{in}}^2 d_{\mathrm{out}}^{1.5}}{d_{\mathrm{in}} d_{\mathrm{out}}/\varepsilon \log()^2 \varepsilon^2}\right)$.。详细证明见附录 D.1。

该证明关键依赖于策略的非自适应性。因此，一个自然的问题是：自适应策略能否胜过其非自适应对应策略？本文并未完全解决这一问题。不过，我们为自适应策略提出了一个下界，表明如果两者之间存在差距，其优势至多为 $\mathcal{O}(\sqrt{d_{\mathrm{out}}})$。

定理 4.6. 设 $\varepsilon \leq 1/32$ 和 $d_{\mathrm{out}} \geq 10$。对于恒等信道到去极化信道测试，任何非相干辅助系统辅助的自适应算法在最坏情况下都需要 $N = \Omega\left(\frac{d_{\mathrm{in}}^2 d_{\mathrm{out}} + d_{\mathrm{out}}^{1.5}}{\varepsilon^2}\right)$ 次测量。

该定理的证明采用了与非自适应下界证明相同的构造。主要区别在于，使用 KL 散度而非全变差距离来比较两个假设下的观测值 $(I_1, \ldots, I_N)$。一方面，数据处理意味着 $\mathrm{KL}\left(\mathrm{P}_{\mathcal{D}}^{I_1 \cdots I_N} \middle\| \mathrm{E}_{\mathcal{N}\sim\mathcal{P}} \mathrm{P}_{\mathcal{N}}^{I_1 \cdots I_N}\right) \geq \frac{1}{3}\log(2)$。另一方面，利用詹森不等式和对数函数的不等式，我们给出 KL 散度的上界：$\mathrm{KL}\left(\mathrm{P}_{\mathcal{D}}^{I_1 \cdots I_N} \middle\| \mathrm{E}_{\mathcal{N}\sim\mathcal{P}} \mathrm{P}_{\mathcal{N}}^{I_1 \cdots I_N}\right) \leq \frac{256 N \varepsilon^2}{d_{\mathrm{in}}^2 d_{\mathrm{out}}}$.这两个不等式推出下界的 $d_{\mathrm{in}}^2 d_{\mathrm{out}}$ 部分。下界的 $d_{\mathrm{out}}^{1.5}$ 部分则可直接由量子态认证的困难性得出 [Chen 等，2022b]。详细证明见附录 D.2。

5 结论与开放问题

我们将恒等性检验问题推广到了量子通道。特别是，我们确定了在自适应设置下对酉信道进行恒等性检验的最优复杂度 $\Theta(d/\varepsilon^2)$。此外，我们证明了在非自适应设置下对去极化信道进行恒等性检验的复杂度为 $\tilde{\Theta}(d_{\mathrm{in}}^2 d_{\mathrm{out}}^{1.5}/\varepsilon^2)$。这些结果引出了若干有趣的问题：能否弥合去极化信道认证中非自适应策略与自适应策略之间的差距？如何实现实例最优性（如 [Valiant 和 Valiant，2016年，Chen 等人，2022a] 所示）？这将使复杂度能够根据待检验过程 $\mathcal{N}_0$ 进行调整。另一个有趣的问题是，4-设计可以在算法 2 中替代 Haar 分布酉矩阵。但对于 3-设计（及更低阶设计），能否达到相同的复杂度？最后，考虑允许在多次使用量子信道之间存在纠缠的一般策略也很有意思，这与 [O'Donnell 和 Wright, 2015] 对量子态所做的工作类似。

致谢

我们感谢欧洲研究委员会（欧洲研究委员会 AlgoQIP 资助项目，协议编号：851716）以及欧盟地平线 2020 研究与创新计划在 QuantERAII 计划框架下通过资助协议编号 101017733 提供的支持。

Aurélien Garivier 感谢 SeqALO 教席（ANR-20-CHIA-0020-01）提供的支持。
Aadil Oufkir 谨向 Guillaume Aubrun 致谢，感谢他进行的有益讨论；并感谢 Moritz Weber 的热情款待，以及他在萨尔兰大学组织量子信息专题学期。

参考文献

Trystan Surawy-Stepney、Jonas Kahn、Richard Kueng 和 Madalin Guta。投影最小二乘量子过程层析。Quantum，6:844，2022年。Aadil Oufkir。采用非自适应非相干测量的样本最优量子过程层析。arXiv 预印本 arXiv:2301.12925，2023年。Lucien LeCam。维数限制下的估计收敛。The Annals of Statistics，第 38–53 页，1973 年。Sebastien Bubeck、Sitan Chen 和 Jerry Li。最优量子性质测试离不开纠缠。载于 2020 年 IEEE 第 61 届计算机科学基础年度研讨会（FOCS），第 692–703 页。IEEE，2020 年。Guillaume Aubrun 和 Stanisław J Szarek。Alice 与 Bob 遇见 Banach，第 223 卷。美国数学会，2017。Gregory Valiant 和 Paul Valiant。离散分布的实例最优学习。载于第四十八届 ACM 理论计算年度研讨会论文集，第 142–155 页，2016。Sitan Chen、Jerry Li 和 Ryan O’Donnell。迈向采用非相干测量的实例最优状态认证。载于学习理论会议，第 2541–2596 页。PMLR，2022a。Guoming Wang。酉算子的性质测试。Physical Review A，84(5):052328，2011 年。Ashley Montanaro 和 Ronald de Wolf。量子性质测试综述。arXiv 预印本 arXiv:1310.2035，2013年。Ilias Diakonikolas、Themis Gouleakis、John Peebles 和 Eric Price。高概率下的最优恒等性检验。arXiv 预印本 arXiv:1708.02728，2017。Sitan Chen、Brice Huang、Jerry Li 和 Allen Liu。采用非相干测量进行量子态认证的紧界。arXiv 预印本 arXiv:2204.07155，2022b。Kean Chen、Qisheng Wang、Peixun Long 和 Mingsheng Ying。量子通道的幺正性估计。arXiv 预印本 arXiv:2212.09319，2022c。Sitan Chen、Jordan Cotler、Hsin-Yuan Huang 和 Jerry Li。使用量子存储器与不使用量子存储器进行学习之间的指数级分离。载于 2021 年 IEEE 第 62 届计算机科学基础年度研讨会（FOCS），第 574–585 页。IEEE，2022d。Costin B˘adescu、Ryan O’Donnell 和 John Wright。量子态认证。载于第 51 届 ACM SIGACT 理论计算年度研讨会论文集，第 503–514 页，2019 年。Man-Duen Choi。复矩阵上的完全正线性映射。《线性代数及其应用》，10(3):285–290，1975 年。Andrzej Jamiołkowski。保持算子迹和半正定性的线性变换。《数学物理报告》，3(4):275–278，1972 年。John Watrous。《量子信息理论》。剑桥大学出版社，2018 年。Max Born。《关于碰撞过程的量子力学》。《物理学杂志》，37(12):863–867，1926年12月。doi: 10.1007/BF01397477。

Senrui Chen、Sisi Zhou、Alireza Seif 和 Liang Jiang。泡利信道估计的量子优势。Physical Review A，105(3):032435，2022e。Christopher A Fuchs 和 Jeroen Van De Graaf。量子态的密码学可区分性度量。《IEEE信息论汇刊》，45(4):1216–1227，1999年。Anna Jenˇcová 和 Martin Plávala。量子通道判别中最优输入态的条件。《数学物理学杂志》，57(12):122203，2016年。Koenraad MR Audenaert。量子偏斜散度。《数学物理学杂志》，55(11):112202，2014年。Jonathan Kunjummen、Minh C Tran、Daniel Carney 和 Jacob M Taylor。量子信道的影子过程层析。arXiv 预印本 arXiv:2110.03629，2021年。Martin J Wainwright。《高维统计学：非渐近视角》，第48卷。剑桥大学出版社，2019年。

Ryan O'Donnell 和 John Wright。《量子谱检验》。载于第四十七届 ACM 计算理论年度研讨会论文集，第 529–538 页，2015年。

´Benoît Collins 和 Piotr Sniady。关于酉群、正交群和辛群上的 Haar 测度积分。《数学物理通讯》，264(3)：773–795，2006。

Sitan Chen、Brice Huang、Jerry Li、Allen Liu 和 Mark Sellke。利用非相干测量进行态层析的紧界。arXiv 预印本 arXiv:2206.05265，2022f。

William Matthews、Stephanie Wehner 和 Andreas Winter。受限测量族下量子态的可区分性及其在量子数据隐藏中的应用。《数学物理通讯》，291(3)：813–843，2009年。

Yinzheng Gu。随机矩阵的矩与魏因加滕函数。博士论文，2013年。

Benoit Collins、Sho Matsumoto 和 Nadia Saad。 不变矩阵的积分及其在统计学中的应用。arXiv 预印本 arXiv:1205.0956，2012年。

Elizabeth Meckes、Mark Meckes 等。随机矩阵的幂的谱测度。《电子概率通讯》，18，2013年。

Tim Van Erven 和 Peter Harremos。Rényi散度与 Kullback–Leibler散度。《IEEE信息论汇刊》，60(7):3797–3820，2014年。

恒等性检验算法 1 分析的延后证明

引理A.1. 设 $|\phi\rangle$ 为一个维度为 d的随机哈尔向量。我们有

$$\mathbb{E}_{\phi}\left[\mathrm{F}(\mathcal{N}(|\phi\rangle\langle\phi|),|\phi\rangle\langle\phi|))\right]=\frac{1+d\,\mathrm{F}(\mathcal{J}_{\mathcal{N}},|\Psi\rangle\langle\Psi|)}{1+d}.$$

证明. 利用引理 F.1和引理 F.3，我们有

$$\begin{aligned}\mathbb{E}_\phi\left[\mathrm{F}(\mathcal{N}(|\phi\rangle\langle\phi|),|\phi\rangle\langle\phi|)\right] &= \sum_k \mathbb{E}_U\left[\langle 0|\, U^\dagger A_k U\,|0\rangle\langle 0|\, U^\dagger A_k^\dagger U\,|0\rangle\right] \\ &= \sum_k \frac{(\mathrm{Tr}(A_k A_k^\dagger)+\mathrm{Tr}(A_k)\mathrm{Tr}(A_k^\dagger))}{d(d+1)} \\ &= \frac{d+\sum_k|\mathrm{Tr}(A_k)|^2}{d(d+1)} = \frac{1+d\,\mathrm{F}(\mathcal{J}_\mathcal{N},|\Psi\rangle\langle\Psi|)}{1+d}\end{aligned}$$

其中我们使用引理 A.2。

引理 A.2. 设 $\mathcal{N}$ 是由 Kraus 算子 $\{A_k\}_k$ 表示的量子信道。设 $S=\sum_k|\mathrm{Tr}(A_k)|^2$。平均保真度与 S 的关系如下：

$$\mathrm{F}(\mathcal{J}_\mathcal{N},|\Psi\rangle\langle\Psi|)=\frac{S}{d^2}.$$

证明. 我们有：

$$\begin{aligned}\mathrm{F}(\mathcal{J}_\mathcal{N},|\Psi\rangle\langle\Psi|) &= \frac{1}{d^2}\sum_{i,j,k,l}\langle ii|\,\mathrm{id}\otimes\mathcal{N}(|kk\rangle\langle ll|)\,|jj\rangle = \frac{1}{d^2}\sum_{i,j,k,l}\langle i|\,I\,|k\rangle\langle l|\,|j\rangle\langle i|\,\mathcal{N}(|k\rangle\langle l|)\,|j\rangle \\ &= \frac{1}{d^2}\sum_{i,j}\langle i|\,\mathcal{N}(|i\rangle\langle j|)\,|j\rangle = \frac{1}{d^2}\sum_{i,j,k}\langle i|\,A_k\,|i\rangle\langle j|\,A_k^\dagger\,|j\rangle = \frac{1}{d^2}\sum_k|\mathrm{Tr}(A_k)|^2=\frac{S}{d^2}.\end{aligned}$$

□

□

引理 A.3. 对所有量子通道 $\mathcal{N}$，我们有：

$$\mathrm{F}(\mathcal{J}_\mathcal{N},|\Psi\rangle\langle\Psi|)\le 1-\frac{d_{\mathrm{Tr}}(\mathcal{N},\mathrm{id})^2}{4d}\le 1-\frac{d_\diamond(\mathcal{N},\mathrm{id})^4}{16d}.$$

证明. 以下不等式可用于证明第二个不等式 [Watrous, 2018, 定理 3.56，改述如下]

$$d_{\mathrm{Tr}}(\mathcal{N},\mathrm{id})\ge\frac{d_\diamond(\mathcal{N},\mathrm{id})^2}{2}.$$

还需证明第一个不等式。为此，令 $\varepsilon=d_{\mathrm{Tr}}(\mathcal{N},\mathrm{id})=\max_{|\phi\rangle\in\mathbf{S}^d}\|\mathcal{N}(|\phi\rangle\langle\phi|)-|\phi\rangle\langle\phi|\,\|_1$。设 $|\phi\rangle$ 是满足前述最大化条件的单位向量，我们利用 Fuchs–van de Graaf 不等式[Fuchs 和 Van De Graaf, 1999] 来证明：

$$\langle\phi|\,\mathcal{N}(|\phi\rangle\langle\phi|)\,|\phi\rangle=\mathrm{F}(\mathcal{N}(|\phi\rangle\langle\phi|),|\phi\rangle\langle\phi|)\le 1-\frac{1}{4}\|\mathcal{N}(|\phi\rangle\langle\phi|)-|\phi\rangle\langle\phi|\,\|_1^2\le 1-\frac{\varepsilon^2}{4}.$$

另一方面，我们使用 Kraus 分解来描述量子信道 $\mathcal{N}(\rho)=\sum_k A_k\rho A_k^\dagger$.我们可以用 Kraus 算子表示前述保真度：

$$\langle\phi|\,\mathcal{N}(|\phi\rangle\langle\phi|)\,|\phi\rangle=\sum_k\langle\phi|\,A_k\,|\phi\rangle\langle\phi|\,A_k^\dagger\,|\phi\rangle=\sum_k|\langle\phi|\,A_k\,|\phi\rangle\,|^2.$$

因此：

$$\sum_k |\langle\phi| A_k |\phi\rangle|^2 \leq 1 - \frac{\varepsilon^2}{4}. \tag{3}$$

设 $|\phi_1\rangle = |\phi\rangle$，我们可以将其补全为一组正交归一基 $\{|\phi_i\rangle\}_{i=1}^d$。此外，我们有 $F(\mathcal{J}_\mathcal{N}, |\Psi\rangle\langle\Psi|) = \frac{1}{d^2}\sum_k |迹(A_k)|^2$（引理 A.2）。应用柯西-施瓦茨不等式并利用不等式 (3)：

$$\begin{aligned}
\sum_k |\mathrm{Tr}(A_k)|^2 = \sum_k \left|\sum_{i=1}^d \langle\phi_i| A_k |\phi_i\rangle\right|^2 &\leq \sum_{k,i} d|\langle\phi_i| A_k |\phi_i\rangle|^2 \\
&= d\sum_k |\langle\phi_1| A_k |\phi_1\rangle|^2 + d\sum_{i=2}^d \sum_k |\langle\phi_i| A_k |\phi_i\rangle|^2 \\
&\leq d(1-\varepsilon^2/4) + d(d-1) = d(d-\varepsilon^2/4)
\end{aligned}$$

因为对于所有 $i \geq 2$：

$$\sum_k |\langle\phi_i| A_k |\phi_i\rangle|^2 \leq \sum_k \langle\phi_i| A_k^\dagger A_k |\phi_i\rangle = \langle\phi_i| \sum_k A_k^\dagger A_k |\phi_i\rangle = 1.$$

最后，$F(\mathcal{J}_\mathcal{N}, |\Psi\rangle\langle\Psi|) = \frac{1}{d^2}\sum_k |迹(A_k)|^2 \leq 1 - \frac{\varepsilon^2}{4d}$. □

B 恒等性检验的下界

本节将为使用辅助系统策略进行恒等性检验的任意算法（可能是自适应的）建立一个一般下界。

定理 B.1. 任何非相干自适应辅助系统策略所需的步骤数满足：

$$N = \Omega\left(\frac{d}{\varepsilon^2}\right)$$

区分 b etween $\mathcal{N} = \mathrm{id}$ 和 $d_\diamond(\mathcal{N}, \mathrm{id}) \geq \varepsilon$（或 $d_{\mathrm{Tr}}(\mathcal{N}, \mathrm{id}) \geq \varepsilon$），且概率至少为 $2/3$.

该定理表明，算法 1 具有最优复杂度。

证明。在零假设 H_0 下，量子信道为 $\mathcal{N} = \mathrm{id}$。在备择假设 H_1 下，我们可以选择 $\mathcal{N}$，使得 $d_\diamond(\mathcal{N}, \mathrm{id}) \geq d_{\mathrm{Tr}}(\mathcal{N}, \mathrm{id}) \geq \varepsilon$。难以检验的量子信道是将基中的几乎每个向量映射到其自身的量子信道。基于这一思路，我们选择 $V \in \mathrm{Haar}(d)$，并构造量子信道$\mathcal{N}_V(\rho) = \frac{1}{2}\rho + \frac{1}{2}U_V\rho U_V^\dagger$，其中 U_V满足：

$$U_V V |l\rangle = \begin{cases} \sqrt{1-\varepsilon^2} V |0\rangle + \varepsilon V |1\rangle & \text{if } l = 0 \\ \sqrt{1-\varepsilon^2} V |1\rangle - \varepsilon V |0\rangle & \text{if } l = 1 \\ V |l\rangle & \text{otherwise.} \end{cases}$$

在 $\mathcal{N}_V$ 的定义中，取恒等信道与酉信道 $U_V \cdot U_V^\dagger$ 的混合，这一点对本证明至关重要，其灵感源自 Audenaert 的量子偏斜散度 [2014]。我们首先需要证明

这样的量子信道与恒等信道相距 ε。事实上，令 $|\phi\rangle = V|0\rangle$，我们有：

$$\begin{aligned} d_\diamond(\mathcal{N}_V, \mathrm{id}) &\geq d_{\mathrm{Tr}}(\mathcal{N}_V, \mathrm{id}) \geq \| \mathcal{N}_V(|\phi\rangle\langle\phi|) - \mathrm{id}(|\phi\rangle\langle\phi|)\|_1 \\ &= \left\| \frac{1}{2}|\phi\rangle\langle\phi| + \frac{1}{2} U_V |\phi\rangle\langle\phi| U_V^\dagger - |\phi\rangle\langle\phi| \right\|_1 \\ &= \frac{1}{2}\left\| V|0\rangle\langle 0| V^\dagger - U_V V|0\rangle\langle 0| V^\dagger U_V^\dagger \right\|_1 \\ &= \frac{1}{2}\left\| |0\rangle\langle 0| - \left(\sqrt{1-\varepsilon^2}|0\rangle + \varepsilon|1\rangle\right)\left(\sqrt{1-\varepsilon^2}\langle 0| + \varepsilon\langle 1|\right) \right\|_1 \\ &= \frac{1}{2}\left\| \varepsilon^2 |0\rangle\langle 0| - \varepsilon\sqrt{1-\varepsilon^2}(|0\rangle\langle 1| + |1\rangle\langle 0|) - \varepsilon^2 |1\rangle\langle 1| \right\|_1 = \varepsilon. \end{aligned}$$

因此，一个 $1/3$-正确算法应当以至少 $2/3$ 的成功概率区分恒等信道与 $\mathcal{N}_V$。该算法每一步只能选择一个输入 ρ_t，我们可以假设（根据 KL 散度的凸性）该输入为秩一，即 $\rho_t = |\psi_t\rangle\langle\psi_t|$，并使用正算子值测度 $\mathcal{M}_t = \{\lambda_i^t |\phi_i^t\rangle\langle\phi_i^t|\}_{i\in\mathcal{I}_t}$ 对输出量子态 $\mathrm{id} \otimes \mathcal{N}(\rho_t)$ 进行测量。请注意，恒等信道 id 作用于辅助空间。这些选择可以取决于之前的观测值，也就是说，该算法可以是自适应的。令 $I_{\leq N} = (I_1, \ldots, I_N)$ 表示该算法的观测值，其中 N是以至少 $2/3$的概率作出正确判断所需的步骤数。我们可以使用 Kullback–Leibler散度比较两种假设下观测值的概率分布。令 P（分别为 Q）表示在 H_0（分别为 H_1）下 $(I_1, \ldots, I_N)$ 的分布。在 H_0 下，$(I_1, \ldots, I_N)$ 的分布为：

$$P := \left\{ \prod_{t=1}^N \lambda_{i_t}^t \langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle \right\}_{i_1,\ldots,i_N} = \left\{ \prod_{t=1}^N \lambda_{i_t}^t |\langle \phi_{i_t}^t | \psi_t \rangle|^2 \right\}_{i_1,\ldots,i_N}.$$

另一方面，在给定 V的条件下，$(I_1, \ldots, I_N)$在 H_1下的分布为：

$$Q_V := \left\{ \prod_{t=1}^N \lambda_{i_t}^t \langle \phi_{i_t}^t | \mathrm{id} \otimes \mathcal{N}_V(\rho_t) | \phi_{i_t}^t \rangle \right\}_{i_1,\ldots,i_N}.$$

此外，我们可以将每个秩一输入态和测量向量写成如下形式：

$$|\psi_t\rangle = A_t \otimes \mathbb{I}|w\rangle \quad \text{and} \quad |\phi_{i_t}^t\rangle = B_{i_t}^t \otimes \mathbb{I}|w\rangle$$

其中 $|w\rangle = \sum_{i=1}^d |ii\rangle$，且矩阵 $A_t \in \mathbb{C}^{d_{\mathrm{anc}}\times d}$ 和 $B_{i_t}^t \in \mathbb{C}^{d_{\mathrm{anc}}\times d}$ 满足：

$$\mathrm{Tr}(A_t A_t^\dagger) = 1 \quad \text{and} \quad \mathrm{Tr}(B_{i_t}^t B_{i_t}^{t,\dagger}) = 1.$$

注意，对于所有 t，对于所有 $X \in \mathbb{C}^{d_{\mathrm{anc}}\times d_{\mathrm{anc}}}$，我们都有 $\sum_{i_t} \lambda_{i_t}^t {B^t}_{,i_t}{}^\dagger X B_{i_t}^t = \mathrm{Tr}(X)\mathbb{I}$。事实上，正算子值测度 $\mathcal{M}_t$ 的条件意味着：

$$X \otimes \mathbb{I} = X \otimes \mathbb{I} \sum_{i_t} \lambda_{i_t}^t |\phi_{i_t}^t\rangle\langle\phi_{i_t}^t| = \sum_{i_t} \lambda_{i_t}^t X B_{i_t}^t \otimes \mathbb{I}|w\rangle\langle w| B_{i_t}^{t,\dagger} \otimes \mathbb{I}$$

因此，对第一系统取偏迹可得

$$\mathrm{Tr}(X)\mathbb{I} = \sum_{i_t,i,j} \lambda_{i_t}^t \langle j| B_{i_t}^{t,\dagger} X B_{i_t}^t |i\rangle |i\rangle\langle j|.$$

最后

$$\sum_{i_t} \lambda_{i_t}^t B_{i_t}^{t,\dagger} X B_{i_t}^t = \mathrm{Tr}(X)\mathbb{I}.$$

取 $X = \mathbb{I}$ 并对第二个系统求偏迹，我们得到

$$\sum_{i_t} \lambda_{i_t}^t B_{i_t}^t B_{i_t}^{t,\dagger} = d\, \mathbb{I}_{d_{\mathrm{anc}}}.$$

回顾一下，对于自适应策略，对于所有 $t \in [N]$、ρ_t 和 $\mathcal{M}_t = \{\lambda_{i_t}^t \left|\phi_{i_t}^t\right\rangle\!\left\langle\phi_{i_t}^t\right|\}_{i_t}$，它们都依赖于 $(i_1, \ldots, i_{t-1})$。因此，P 和 Q_V 之间的 KL 散度可以表示如下：

$$\begin{aligned}
\mathrm{KL}(P\|Q_V) &= \mathbb{E}_{i\sim P}(-\log)\left(\frac{Q_{V,i}}{P_i}\right) \\
&= \sum_{t=1}^N \mathbb{E}_{i\le N}(-\log)\left(\frac{\left\langle\phi_{i_t}^t\right| \mathrm{id}\otimes\mathcal{N}_V(\rho_t)\left|\phi_{i_t}^t\right\rangle}{\left\langle\phi_{i_t}^t\right|\rho_t\left|\phi_{i_t}^t\right\rangle}\right) \\
&= \sum_{t=1}^N \mathbb{E}_{i\le t}(-\log)\left(\frac{\left\langle\phi_{i_t}^t\right| \mathrm{id}\otimes\mathcal{N}_V(\rho_t)\left|\phi_{i_t}^t\right\rangle}{\left\langle\phi_{i_t}^t\right|\rho_t\left|\phi_{i_t}^t\right\rangle}\right)
\end{aligned}$$

其中，我们使用了 $t \in [N]$、$\mathbb{E}_{i\le t}(X(i_1,\ldots,i_t)) = \sum_{i_1,\ldots,i_t}\prod_{k=1}^t \lambda_{i_k}^k \left\langle\phi_{i_k}^k\right|\rho_k\left|\phi_{i_k}^k\right\rangle X(i_1,\ldots,i_t)$ 的记号，以及项 $\frac{\left\langle\phi_{i_t}^t\right|\mathrm{id}\otimes\mathcal{N}_V\ \rho_t\ \left|\phi_{i_t}^t\right\rangle}{\left\langle\phi_{i_t}^t\right|\rho_t\left|\phi_{i_t}^t\right\rangle}()$ 仅依赖于 $(i_1,\ldots,i_t)$ 这一事实。

令 $\mathcal{E}$ 表示算法接受 H_0 的事件，我们对 KL 散度应用数据处理不等式（见命题 F.3）：

$$\begin{aligned}
\mathrm{KL}(P\|Q_V) &\ge \mathrm{KL}(P(\mathcal{E})\|Q_V(\mathcal{E})) \\
&\ge \mathrm{KL}\left(\frac{2}{3}\middle\|\frac{1}{3}\right) = \frac{2}{3}\log(2) - \frac{1}{3}\log(2) = \frac{1}{3}\log(2)
\end{aligned}$$

其中 $\mathrm{KL}(p\|q)$ = KL(伯努利分布(p)‖伯努利分布(q))。因此

$$\mathbb{E}_{V\sim\mathrm{Haar}(d)}\,\mathrm{KL}(P\|Q_V) \ge \frac{1}{3}\log(2).$$

令 $M_V = \mathbb{I} - U_V$ 和 $S_V = \mathbb{I} - \frac{1}{2}M_V$。我们可以将 $\mathrm{KL}(P\|Q_V)$ 表达式中的对数项写为：

$$\begin{aligned}
&(-\log)\left(\frac{\left\langle\phi_{i_t}^t\right| \mathrm{id}\otimes\mathcal{N}_V(\rho_t)\left|\phi_{i_t}^t\right\rangle}{\left\langle\phi_{i_t}^t\right|\rho_t\left|\phi_{i_t}^t\right\rangle}\right) \\
&= (-\log)\left(\frac{\left\langle\phi_{i_t}^t\right| (\frac{1}{2}\rho_t + \frac{1}{2}(\mathbb{I}\otimes U_V)\rho_t(\mathbb{I}\otimes U_V^\dagger))\left|\phi_{i_t}^t\right\rangle}{\left\langle\phi_{i_t}^t\right|\rho_t\left|\phi_{i_t}^t\right\rangle}\right) \\
&= (-\log)\left(1 - \frac{\Re(\left\langle\phi_{i_t}^t\right|(\mathbb{I}\otimes M_V)\rho_t\left|\phi_{i_t}^t\right\rangle)}{\left\langle\phi_{i_t}^t\right|\rho_t\left|\phi_{i_t}^t\right\rangle} + \frac{1}{2}\frac{\left\langle\phi_{i_t}^t\right|(\mathbb{I}\otimes M_V)\rho_t(\mathbb{I}\otimes M_V^\dagger)\left|\phi_{i_t}^t\right\rangle}{\left\langle\phi_{i_t}^t\right|\rho_t\left|\phi_{i_t}^t\right\rangle}\right) \\
&= (-\log)\left(1 - \frac{1}{2}\frac{\left\langle\phi_{i_t}^t\right|(\mathbb{I}\otimes M_V)\rho_t(\mathbb{I}\otimes S_V^\dagger)\left|\phi_{i_t}^t\right\rangle}{\left\langle\phi_{i_t}^t\right|\rho_t\left|\phi_{i_t}^t\right\rangle} - \frac{1}{2}\frac{\left\langle\phi_{i_t}^t\right|(\mathbb{I}\otimes S_V)\rho_t(\mathbb{I}\otimes M_V^\dagger)\left|\phi_{i_t}^t\right\rangle}{\left\langle\phi_{i_t}^t\right|\rho_t\left|\phi_{i_t}^t\right\rangle}\right).
\end{aligned}$$

对于 $t \in [N]$ 和 $i_{\le t} = (i_1, \dots, i_t)$，定义事件 $\mathcal{G}(t, i_{\le t}) = \left\{ \langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle \le \frac{\varepsilon^2}{d^2} \text{迹}(A_t^\dagger B_{i_t}^t B^{t,\ _{i_t}\dagger} A_t) \right\}$。我们可以区分事件 $\mathcal{G}$ 是否成立：

$$\mathbb{E}_{V\sim \mathrm{Haar}(d)} \mathrm{KL}(P\|Q_V) = \sum_{t=1}^{N} \mathbb{E}_{V\sim \mathrm{Haar}(d)} \mathbb{E}_{i\le t} (\mathbf{1}\{\mathcal{G}(t, i_{\le t})\} + \mathbf{1}\{\mathcal{G}^c(t, i_{\le t})\}) (-\log) \left(\frac{\langle \phi_{i_t}^t | \operatorname{id} \otimes \mathcal{N}_V(\rho_t) | \phi_{i_t}^t \rangle}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} \right).$$

我们先分析事件 $\mathcal{G}$ 成立时的情形。固定 $t \in [N]$，注意到有如下不等式：

$$\begin{aligned}
(-\log) \left(\frac{\langle \phi_{i_t}^t | \operatorname{id} \otimes \mathcal{N}_V(\rho_t) | \phi_{i_t}^t \rangle}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} \right) &= (-\log) \left(\frac{\langle \phi_{i_t}^t | (\frac{1}{2}\rho_t + \frac{1}{2}(\mathbb{I}\otimes U_V)\rho_t(\mathbb{I}\otimes U_V^\dagger)) | \phi_{i_t}^t \rangle}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} \right) \\
&= (-\log) \left(\frac{1}{2} + \frac{\langle \phi_{i_t}^t | (\frac{1}{2}(\mathbb{I}\otimes U_V)\rho_t(\mathbb{I}\otimes U_V^\dagger)) | \phi_{i_t}^t \rangle}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} \right) \le \log(2) \le 1.
\end{aligned}$$

那么，我们可以如下控制事件 $\mathcal{G}$ 下的期望：

$$\begin{aligned}
&\mathbb{E}_{V\sim \mathrm{Haar}(d)} \mathbb{E}_{i\le t} \mathbf{1}\{\mathcal{G}(t, i_{\le t})\} (-\log) \left(\frac{\langle \phi_{i_t}^t | \operatorname{id} \otimes \mathcal{N}_V(\rho_t) | \phi_{i_t}^t \rangle}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} \right) \\
&\le \mathbb{E}_{V\sim \mathrm{Haar}(d)} \mathbb{E}_{i\le t-1} \sum_{i_t} \lambda_{i_t}^t \langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle \mathbf{1}\{\mathcal{G}(t, i_{\le t})\} \\
&\le \mathbb{E}_{V\sim \mathrm{Haar}(d)} \mathbb{E}_{i\le t-1} \sum_{i_t} \lambda_{i_t}^t \left(\frac{\varepsilon^2}{d^2} \mathrm{Tr}(A_t^\dagger B_{i_t}^t B_{i_t}^{t,\dagger} A_t) \right) \mathbf{1}\{\mathcal{G}(t, i_{\le t})\} \\
&\le \mathbb{E}_{V\sim \mathrm{Haar}(d)} \mathbb{E}_{i\le t-1} \sum_{i_t} \lambda_{i_t}^t \left(\frac{\varepsilon^2}{d^2} \mathrm{Tr}(A_t^\dagger B_{i_t}^t B_{i_t}^{t,\dagger} A_t) \right) \\
&= \mathbb{E}_{V\sim \mathrm{Haar}(d)} \mathbb{E}_{i\le t-1} \left(\frac{\varepsilon^2}{d^2} \mathrm{Tr}(A_t^\dagger dA_t) \right) = \mathbb{E}_{V\sim \mathrm{Haar}(d)} \mathbb{E}_{i\le t-1} \left(\frac{\varepsilon^2}{d} \right) = \frac{\varepsilon^2}{d}
\end{aligned} \tag{4}$$

这里我们利用了以下事实：在事件 $\mathcal{G}$ 下，有 $\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle \le \frac{\varepsilon^2}{d^2} \text{迹}(A_t^\dagger B_{i_t}^t B^{t,\ _{i_t}\dagger} A_t)$，迹$(A_t^\dagger A_t) = 1$ 以及 $\sum_{i_t} \lambda_{i_t}^t B_{i_t}^t B^{t,\ _{i_t}\dagger} = d\mathbb{I}$，这是 $\mathcal{M}_t = \{\lambda_i^t |\phi_i^t\rangle\langle\phi_i^t|\}_{i\in\mathcal{I}_t}$ 是正算子值测度这一事实的推论。另一方面，在 $\mathcal{G}^c(t, i_{\le t})$ 下，我们将改用不等式

$$(-\log)(x) \le (1-x) + (x-1)^2 \quad \text{valid for all} \quad x \in \left[\frac{1}{2}, +\infty\right).$$

我们将此不等式应用于 $x = \frac{\langle \phi_{i_t}^t | \operatorname{id} \otimes \mathcal{N}_V \ \rho_t \ | \phi_{i_t}^t \rangle}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} = \frac{1}{2} + \frac{\langle \phi_{i_t}^t | ()(\frac{1}{2}(\mathbb{I}\otimes U_V \ \rho_t \ \mathbb{I}\otimes U_V^\dagger \ | \phi_{i_t}^t \rangle}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} \ge \frac{1}{2}^{)())}$，第一项

上界为:

$$
\begin{aligned}
(1-x) &= 1-\frac{\left\langle\phi_{i_t}^t\right|\mathrm{id}\otimes\mathcal{N}_V(\rho_t)\left|\phi_{i_t}^t\right\rangle}{\left\langle\phi_{i_t}^t\right|\rho_t\left|\phi_{i_t}^t\right\rangle} \\
&= \frac{1}{2}\frac{\left\langle\phi_{i_t}^t\right|(\mathbb{I}\otimes M_V)\rho_t(\mathbb{I}\otimes S_V^\dagger)\left|\phi_{i_t}^t\right\rangle}{\left\langle\phi_{i_t}^t\right|\rho_t\left|\phi_{i_t}^t\right\rangle}+\frac{1}{2}\frac{\left\langle\phi_{i_t}^t\right|(\mathbb{I}\otimes S_V)\rho_t(\mathbb{I}\otimes M_V^\dagger)\left|\phi_{i_t}^t\right\rangle}{\left\langle\phi_{i_t}^t\right|\rho_t\left|\phi_{i_t}^t\right\rangle} \\
&= \frac{\Re\left\langle\phi_{i_t}^t\right|(\mathbb{I}\otimes M_V)\left|\psi_t\right\rangle\left\langle\psi_t\right|(\mathbb{I}\otimes S_V^\dagger)\left|\phi_{i_t}^t\right\rangle}{\left\langle\phi_{i_t}^t\right|\rho_t\left|\phi_{i_t}^t\right\rangle} \\
&= \frac{\Re\left\langle w\right|(B_{i_t}^{t,\dagger}A_t\otimes M_V)\left|w\right\rangle\left\langle w\right|(A_t^\dagger B_{i_t}^t\otimes S_V^\dagger)\left|w\right\rangle}{\left\langle w\right|(B_{i_t}^{t,\dagger}A_t\otimes\mathbb{I})\left|w\right\rangle\left\langle w\right|(A_t^\dagger B_{i_t}^t\otimes\mathbb{I})\left|w\right\rangle} \\
&= \frac{\Re\,\mathrm{Tr}(B_{i_t}^{t,\dagger}A_tM_V^\top)\mathrm{Tr}(A_t^\dagger B_{i_t}^t\bar{S}_V)}{\mathrm{Tr}(B_{i_t}^{t,\dagger}A_t)\mathrm{Tr}(A_t^\dagger B_{i_t}^t)}
\end{aligned}
\tag{5}
$$

首先利用不等式（$(x+y)^2\le 2(x^2+y^2)$），然后对向量 $\sqrt{\rho_t}\left|\phi_{i_t}^t\right\rangle$ 和 $\sqrt{\rho_t}M_V^\dagger\left|\phi_{i_t}^t\right\rangle$ 应用柯西-施瓦茨不等式，可得第二项的上界如下:

$$
\begin{aligned}
(x-1)^2 &= \left(\frac{\left\langle\phi_{i_t}^t\right|\mathrm{id}\otimes\mathcal{N}_V(\rho_t)\left|\phi_{i_t}^t\right\rangle}{\left\langle\phi_{i_t}^t\right|\rho_t\left|\phi_{i_t}^t\right\rangle}-1\right)^2 \\
&= \left(\frac{\Re(\left\langle\phi_{i_t}^t\right|(\mathbb{I}\otimes M_V)\rho_t\left|\phi_{i_t}^t\right\rangle)}{\left\langle\phi_{i_t}^t\right|\rho_t\left|\phi_{i_t}^t\right\rangle}-\frac{1}{2}\frac{\left\langle\phi_{i_t}^t\right|(\mathbb{I}\otimes M_V)\rho_t(\mathbb{I}\otimes M_V^\dagger)\left|\phi_{i_t}^t\right\rangle}{\left\langle\phi_{i_t}^t\right|\rho_t\left|\phi_{i_t}^t\right\rangle}\right)^2 \\
&\le 2\left(\frac{|\left\langle\phi_{i_t}^t\right|(\mathbb{I}\otimes M_V)\rho_t\left|\phi_{i_t}^t\right\rangle|}{\left\langle\phi_{i_t}^t\right|\rho_t\left|\phi_{i_t}^t\right\rangle}\right)^2+2\left(\frac{1}{2}\frac{\left\langle\phi_{i_t}^t\right|(\mathbb{I}\otimes M_V)\rho_t(\mathbb{I}\otimes M_V^\dagger)\left|\phi_{i_t}^t\right\rangle}{\left\langle\phi_{i_t}^t\right|\rho_t\left|\phi_{i_t}^t\right\rangle}\right)^2 \\
&\le 2\left(\frac{\left\langle\phi_{i_t}^t\right|(\mathbb{I}\otimes M_V)\rho_t(\mathbb{I}\otimes M_V^\dagger)\left|\phi_{i_t}^t\right\rangle}{\left\langle\phi_{i_t}^t\right|\rho_t\left|\phi_{i_t}^t\right\rangle}\right)+2\left(\frac{1}{2}\frac{\left\langle\phi_{i_t}^t\right|(\mathbb{I}\otimes M_V)\rho_t(\mathbb{I}\otimes M_V^\dagger)\left|\phi_{i_t}^t\right\rangle}{\left\langle\phi_{i_t}^t\right|\rho_t\left|\phi_{i_t}^t\right\rangle}\right)^2 \\
&= 2\frac{\mathrm{Tr}(B_{i_t}^{t,\dagger}A_tM_V^\top)\mathrm{Tr}(A_t^\dagger B_{i_t}^t\bar{M}_V)}{\mathrm{Tr}(B_{i_t}^{t,\dagger}A_t)\mathrm{Tr}(A_t^\dagger B_{i_t}^t)}+\frac{1}{2}\left(\frac{\mathrm{Tr}(B_{i_t}^{t,\dagger}A_tM_V^\top)\mathrm{Tr}(A_t^\dagger B_{i_t}^t\bar{M}_V)}{\mathrm{Tr}(B_{i_t}^{t,\dagger}A_t)\mathrm{Tr}(A_t^\dagger B_{i_t}^t)}\right)^2
\end{aligned}
\tag{6}
$$

我们来计算（5）的期望。设 M,S 使得 $M_V=VMV^\dagger$ 和 $S_V=VSV^\dagger$。具体而言

$$
M=\left(\begin{array}{cc|c}1-\sqrt{1-\varepsilon^2} & -\varepsilon & 0\\ \varepsilon & 1-\sqrt{1-\varepsilon^2} & \\ \hline 0 & & 0_{d-2}\end{array}\right)\quad\text{and}\quad S=\left(\begin{array}{cc|c}\frac{1}{2}+\frac{\sqrt{1-\varepsilon^2}}{2} & \frac{\varepsilon}{2} & 0\\ \frac{-\varepsilon}{2} & \frac{1}{2}+\frac{\sqrt{1-\varepsilon^2}}{2} & \\ \hline 0 & & \mathbb{I}_{d-2}\end{array}\right).
$$

注意，迹$(M)=2(1-\sqrt{1-\varepsilon^2})$, 迹$(S)=d-1+\sqrt{1-\varepsilon^2}$, 迹$(MS^\dagger)$ =迹$(M^\dagger S)=0$和 $MM^\dagger=$

$M + M^\dagger = M^\dagger M$. 令 $\varepsilon' = (1 - \sqrt{1-\varepsilon^2}) = \Theta(\varepsilon^2)$，由 Weingarten演算（引理 F.1）可得:

$$
\begin{aligned}
&\left|\mathbb{E}_{V\sim\mathrm{Haar}(d)}\left(\frac{\Re\,\mathrm{Tr}(B_{i_t}^{t,\dagger}A_t M_V^\top)\mathrm{Tr}(A_t^\dagger B_{i_t}^t \bar{S}_V)}{\mathrm{Tr}(B_{i_t}^{t,\dagger}A_t)\mathrm{Tr}(A_t^\dagger B_{i_t}^t)}\right)\right| \\
&= \left|\frac{1}{\mathrm{Tr}(B_{i_t}^{t,\dagger}A_t)\mathrm{Tr}(A_t^\dagger B_{i_t}^t)}\Re\mathbb{E}_{V\sim\mathrm{Haar}(d)}\left(\sum_{x,y}\langle x|\, B_{i_t}^{t,\dagger}A_t V M^\top V^\dagger\,|x\rangle\,\langle y|\, A_t^\dagger B_{i_t}^t V S V^\dagger\,|y\rangle\right)\right| \\
&= \left|\frac{1}{\mathrm{Tr}(B_{i_t}^{t,\dagger}A_t)\mathrm{Tr}(A_t^\dagger B_{i_t}^t)}\Re\sum_{\alpha,\beta\in\mathfrak{S}_2}\sum_{x,y}\mathrm{Wg}(\alpha\beta)\mathrm{Tr}_\alpha(M^\top,S)\mathrm{Tr}_{\beta(12)}(|x\rangle\langle y|\, A_t^\dagger B_{i_t}^t, |y\rangle\langle x|\, B_{i_t}^{t,\dagger}A_t)\right| \\
&= \left|\Re\left(\frac{\mathrm{Tr}(MS^\dagger)(d\mathrm{Tr}(A_t^\dagger B_{i_t}^t B_{i_t}^{t,\dagger}A_t) - |\mathrm{Tr}(A_t^\dagger B_{i_t}^t)|^2) + \mathrm{Tr}(M)\mathrm{Tr}(S)(d|\mathrm{Tr}(A_t^\dagger B_{i_t}^t)|^2 - \mathrm{Tr}(A_t^\dagger B_{i_t}^t B_{i_t}^{t,\dagger}A_t))}{d(d^2-1)\mathrm{Tr}(B_{i_t}^{t,\dagger}A_t)\mathrm{Tr}(A_t^\dagger B_{i_t}^t)}\right)\right| \\
&= \left|\Re\left(\frac{2\varepsilon'(d-\varepsilon')(d|\mathrm{Tr}(A_t^\dagger B_{i_t}^t)|^2 - \mathrm{Tr}(A_t^\dagger B_{i_t}^t B_{i_t}^{t,\dagger}A_t))}{d(d^2-1)\mathrm{Tr}(B_{i_t}^{t,\dagger}A_t)\mathrm{Tr}(A_t^\dagger B_{i_t}^t)}\right)\right| \\
&\le \frac{2\varepsilon^2}{d} + \frac{2\varepsilon^2\mathrm{Tr}(A_t^\dagger B_{i_t}^t B_{i_t}^{t,\dagger}A_t)}{(d^2-1)\mathrm{Tr}(B_{i_t}^{t,\dagger}A_t)\mathrm{Tr}(A_t^\dagger B_{i_t}^t)}
\end{aligned}
$$

回顾记号 $\mathrm{E}_{i\le t}(X(i_1,\ldots,i_t)) = \sum_{i_1,\ \ldots,\ i_t}\prod_{k=1}^t \lambda_{i_k}^k \left\langle \phi_{i_k}^k\right| \rho_k \left|\phi_{i_k}^k\right\rangle X(i_1,\ldots,i_t)$。若我们在事件 $\mathcal{G}^c(t, i_{\le t})$ 条件下取期望 $\mathrm{E}_{i\le t}$，则得到

$$
\begin{aligned}
&\mathbb{E}_{V\sim\mathrm{Haar}(d)}\mathbb{E}_{i\le t}\mathbf{1}\{\mathcal{G}^c(t,i_t)\}\left(\frac{\Re\left\langle\phi_{i_t}^t\right|(\mathbb{I}\otimes M_V)\rho_t(\mathbb{I}\otimes S_V^\dagger)\left|\phi_{i_t}^t\right\rangle}{\left\langle\phi_{i_t}^t\right|\rho_t\left|\phi_{i_t}^t\right\rangle}\right) \\
&\le \mathbb{E}_{i\le t}\mathbf{1}\{\mathcal{G}^c(t,i_t)\}\left|\mathbb{E}_{V\sim\mathrm{Haar}(d)}\left(\frac{\Re\left\langle\phi_{i_t}^t\right|(\mathbb{I}\otimes M_V)\rho_t(\mathbb{I}\otimes S_V^\dagger)\left|\phi_{i_t}^t\right\rangle}{\left\langle\phi_{i_t}^t\right|\rho_t\left|\phi_{i_t}^t\right\rangle}\right)\right| \\
&\le \mathbb{E}_{i\le t}\mathbf{1}\{\mathcal{G}^c(t,i_t)\}\left(\frac{2\varepsilon^2}{d} + \frac{2\varepsilon^2\mathrm{Tr}(A_t^\dagger B_{i_t}^t B_{i_t}^{t,\dagger}A_t)}{(d^2-1)\mathrm{Tr}(B_{i_t}^{t,\dagger}A_t)\mathrm{Tr}(A_t^\dagger B_{i_t}^t)}\right) \\
&\le \mathbb{E}_{i\le t}\left(\frac{2\varepsilon^2}{d} + \frac{2\varepsilon^2\mathrm{Tr}(A_t^\dagger B_{i_t}^t B_{i_t}^{t,\dagger}A_t)}{(d^2-1)\mathrm{Tr}(B_{i_t}^{t,\dagger}A_t)\mathrm{Tr}(A_t^\dagger B_{i_t}^t)}\right) \\
&= \frac{2\varepsilon^2}{d} + \mathbb{E}_{i_{\le t-1}}\sum_{i_t}\lambda_{i_t}^t\left\langle\phi_{i_t}^t\right|\rho_t\left|\phi_{i_t}^t\right\rangle \times \frac{2\varepsilon^2\mathrm{Tr}(A_t^\dagger B_{i_t}^t B_{i_t}^{t,\dagger}A_t)}{(d^2-1)\left\langle\phi_{i_t}^t\right|\rho_t\left|\phi_{i_t}^t\right\rangle} \\
&= \frac{2\varepsilon^2}{d} + \mathbb{E}_{i_{\le t-1}}\frac{2\varepsilon^2}{d^2-1}\sum_{i_t}\lambda_{i_t}^t\mathrm{Tr}(A_t^\dagger B_{i_t}^t B_{i_t}^{t,\dagger}A_t) \\
&= \frac{2\varepsilon^2}{d} + \mathbb{E}_{i_{\le t-1}}\frac{2\varepsilon^2}{d^2-1}\mathrm{Tr}(A_t^\dagger d A_t) \le \frac{5\varepsilon^2}{d}
\end{aligned}
\tag{7}
$$

其中我们使用 $\sum_{i_t}\lambda_{i_t}^t B_{i_t}^t B^{t,}{}_{i_t}{}^\dagger = d\,\mathbb{I}$，且 $\mathrm{Tr}(A_t A_t^\dagger) = 1$。现在考虑第一项的期望 $\mathrm{E}_{i\le t}$

对于式 (6)，它是非负的，因此我们可以放心地去掉条件 $\mathbf{1}\{\mathcal{G}^c(t,i_t)\}$:

$$\begin{aligned}
&\mathbb{E}_V\mathbb{E}_{i\le t}\mathbf{1}\{\mathcal{G}^c(t,i_t)\}\frac{2\left\langle\phi_{i_t}^t\right|(\mathbb{I}\otimes M_V)\rho_t(\mathbb{I}\otimes M_V^\dagger)\left|\phi_{i_t}^t\right\rangle}{\left\langle\phi_{i_t}^t\right|\rho_t\left|\phi_{i_t}^t\right\rangle}\\
&\le \mathbb{E}_V\mathbb{E}_{i\le t}\frac{2\left\langle\phi_{i_t}^t\right|(\mathbb{I}\otimes M_V)\rho_t(\mathbb{I}\otimes M_V^\dagger)\left|\phi_{i_t}^t\right\rangle}{\left\langle\phi_{i_t}^t\right|\rho_t\left|\phi_{i_t}^t\right\rangle}\\
&= \mathbb{E}_V\mathbb{E}_{i\le t-1}\sum_{i_t}2\lambda_{i_t}^t\left\langle\phi_{i_t}^t\right|(\mathbb{I}\otimes M_V)\rho_t(\mathbb{I}\otimes M_V^\dagger)\left|\phi_{i_t}^t\right\rangle\\
&= \mathbb{E}_{i\le t-1}\mathbb{E}_V 2\mathrm{Tr}((\mathbb{I}\otimes M_V)\rho_t(\mathbb{I}\otimes M_V^\dagger))\\
&= \mathbb{E}_{i\le t-1}\mathbb{E}_V 2\mathrm{Tr}[\left(\mathbb{I}\otimes(M_V+M_V^\dagger)\right)\rho_t]\\
&= \mathbb{E}_{i\le t-1}\frac{8\varepsilon'}{d}\le\frac{8\varepsilon^2}{d}
\end{aligned}\tag{8}$$

因为 $\mathrm{E}_V M_V = {}^{2\ (1-\sqrt{1-\varepsilon^2})}_{\quad d}\ \mathbb{I}\preccurlyeq\frac{2\varepsilon^2}{d}\mathbb{I}$。

关于式（6）中第二项的期望，我们在记 $C=A_l^\dagger B_{i_t}^t$后再次应用 Weingarten演算（引理 F.1）：

$$\begin{aligned}
&\mathbb{E}_{V\sim\mathrm{Haar}(d)}\frac{1}{2}\left(\frac{\mathrm{Tr}(B_{i_t}^{t,\dagger}A_tM_V^\top)\mathrm{Tr}(A_l^\dagger B_{i_t}^t\bar{M}_V)}{\left\langle\phi_{i_t}^t\right|\rho_t\left|\phi_{i_t}^t\right\rangle}\right)^2=\frac{1}{2}\frac{\mathbb{E}_{V\sim\mathrm{Haar}(d)}\mathrm{Tr}(B_{i_t}^{t,\dagger}A_tM_V^\top)^2\mathrm{Tr}(A_t^\dagger B_{i_t}^t\bar{M}_V)^2}{\left\langle\phi_{i_t}^t\right|\rho_t\left|\phi_{i_t}^t\right\rangle^2}\\
&=\frac{1}{2}\sum_{x,y,z,t}\frac{\mathbb{E}_{V\sim\mathrm{Haar}(d)}\mathrm{Tr}(|t\rangle\langle x|C^\dagger VM^\top V^\dagger|x\rangle\langle z|CVMV^\dagger|z\rangle\langle y|C^\dagger VM^\top V^\dagger|y\rangle\langle t|CVMV^\dagger)}{\left\langle\phi_{i_t}^t\right|\rho_t\left|\phi_{i_t}^t\right\rangle^2}\\
&=\frac{1}{2\left\langle\phi_{i_t}^t\right|\rho_t\left|\phi_{i_t}^t\right\rangle^2}\sum_{x,y,z,t}\sum_{\alpha,\beta\in\mathfrak{S}_4}\mathrm{Wg}(\alpha\beta)\mathrm{Tr}_\beta(M^\top,M,M^\top,M)\mathrm{Tr}_{\alpha\gamma}(|t\rangle\langle x|C^\dagger,|x\rangle\langle z|C,|z\rangle\langle y|C^\dagger,|y\rangle\langle t|C)
\end{aligned}$$

我们可以指出，对于所有 $\alpha\in\mathfrak{S}_4$，存在 $\beta\in\mathfrak{S}_4$ 使得:

$$\begin{aligned}
\left|\sum_{x,y,z,t}\mathrm{Tr}_\alpha(|t\rangle\langle x|C^\dagger,|x\rangle\langle z|C,|z\rangle\langle y|C^\dagger,|y\rangle\langle t|C)\right|&=\left|\mathrm{Tr}_\beta(C^\dagger,C,C^\dagger,C)\right|\\
&\le\max\{\mathrm{Tr}(CC^\dagger),|\mathrm{Tr}(C)|^2\}^2
\end{aligned}$$

其中，最后一个不等式仅在 $\beta=(ijk)$时是非平凡的。例如，若 $\beta=(123)$，根据柯西-施瓦茨不等式，我们有:

$$\begin{aligned}
\mathrm{Tr}_\beta(C^\dagger,C,C^\dagger,C)&=\mathrm{Tr}(C^\dagger CC^\dagger)\mathrm{Tr}(C)\le\sqrt{\mathrm{Tr}(CC^\dagger CC^\dagger)\mathrm{Tr}(CC^\dagger)}|\mathrm{Tr}(C)|\\
&\le\mathrm{Tr}(CC^\dagger)^{3/2}|\mathrm{Tr}(C)|\\
&\le\max\{\mathrm{Tr}(CC^\dagger),|\mathrm{Tr}(C)|^2\}^{3/2}\max\{\mathrm{Tr}(CC^\dagger),|\mathrm{Tr}(C)|^2\}^{1/2}\\
&=\max\{\mathrm{Tr}(CC^\dagger),|\mathrm{Tr}(C)|^2\}^2.
\end{aligned}$$

此外，显然，当 β不是 4-循环时，我们有 $|\mathrm{Tr}_\beta(M,M^\top,M,M^\top)|\le\mathcal{O}(\varepsilon^4)$，因为它可以写成至少两个元素的乘积，且每个元素都是 $\mathcal{O}(\varepsilon^2)$。当 β 是一个 4-循环时，我们有 $\mathrm{Tr}(MM^\top MM^\top)=\mathrm{Tr}(MMM^\top M^\dagger)=\mathrm{Tr}((M+M^\top)^2)=2(2-2\sqrt{1-\varepsilon^2})^2\le 8\varepsilon^4$。另一方面

，我们知道，对于所有的 $(\alpha,\beta)\in\mathfrak{S}_4^2$, $|\mathrm{Wg}(\alpha\beta)|\leq\frac{2}{d^4}$ [Collins 和 ´Sniady, 2006] 所以

$$\sum_{x,y,z,t}\sum_{\alpha,\beta\in\mathfrak{S}_4}\mathrm{Wg}(\alpha\beta)\mathrm{Tr}_\beta(M^\top,M,M^\top,M)\mathrm{Tr}_{\alpha\gamma}(|t\rangle\langle x|C^\dagger,|x\rangle\langle z|C,|z\rangle\langle y|C^\dagger,|y\rangle\langle t|C)$$
$$\leq\mathcal{O}\left(\frac{\varepsilon^4}{d^4}\max\{\mathrm{Tr}(CC^\dagger),|\mathrm{Tr}(C)|^2\}^2\right).$$

因此我们有:

$$\mathbb{E}_{V\sim\mathrm{Haar}(d)}\frac{1}{2}\left(\frac{\mathrm{Tr}(B_{i_t}^{t,\dagger}A_tM_V^\top)\mathrm{Tr}(A_t^\dagger B_{i_t}^t\bar{M}_V)}{\langle\phi_{i_t}^t|\rho_t|\phi_{i_t}^t\rangle}\right)^2\leq\mathcal{O}\left(\frac{\varepsilon^4\max\{\mathrm{Tr}(CC^\dagger),|\mathrm{Tr}(C)|^2\}^2}{d^4\langle\phi_{i_t}^t|\rho_t|\phi_{i_t}^t\rangle^2}\right).$$

回想一下 $C=A_t^\dagger B_{i_t}^t$，现在，如果我们在事件下取期望 $\mathrm{E}_{i\leq t}$

$$\mathcal{G}^c(t,i_{\leq t})=\left\{\langle\phi_{i_t}^t|\rho_t|\phi_{i_t}^t\rangle>\frac{\varepsilon^2}{d^2}\mathrm{Tr}(A_t^\dagger B_{i_t}^tB_{i_t}^{t,\dagger}A_t)\right\}=\left\{|\mathrm{Tr}(C)|^2>\frac{\varepsilon^2}{d^2}\mathrm{Tr}(CC^\dagger)\right\},$$

我们得到:

$$\mathbb{E}_{i_{\leq t}}\mathbb{E}_{V\sim\mathrm{Haar}(d)}\mathbf{1}\{\mathcal{G}^c(t,i_{\leq t})\}\frac{1}{2}\left(\frac{\mathrm{Tr}(B_{i_t}^{t,\dagger}A_tM_V^\top)\mathrm{Tr}(A_t^\dagger B_{i_t}^t\bar{M}_V)}{\langle\phi_{i_t}^t|\rho_t|\phi_{i_t}^t\rangle}\right)^2$$
$$\leq\mathbb{E}_{i_{\leq t}}\mathbf{1}\{\mathcal{G}^c(t,i_{\leq t})\}\mathcal{O}\left(\frac{\varepsilon^4\max\{\mathrm{Tr}(CC^\dagger),|\mathrm{Tr}(C)|^2\}^2}{d^4\langle\phi_{i_t}^t|\rho_t|\phi_{i_t}^t\rangle^2}\right)$$
$$\leq\mathbb{E}_{i_{\leq t}}\mathbf{1}\{\mathcal{G}^c(t,i_{\leq t})\}\mathcal{O}\left(\frac{\varepsilon^4|\mathrm{Tr}(C)|^4}{d^4\langle\phi_{i_t}^t|\rho_t|\phi_{i_t}^t\rangle^2}+\frac{\varepsilon^4}{d^4\langle\phi_{i_t}^t|\rho_t|\phi_{i_t}^t\rangle}\times\frac{\mathrm{Tr}(CC^\dagger)^2}{\langle\phi_{i_t}^t|\rho_t|\phi_{i_t}^t\rangle}\right)$$
$$=\mathbb{E}_{i_{\leq t}}\mathbf{1}\{\mathcal{G}^c(t,i_{\leq t})\}\mathcal{O}\left(\frac{\varepsilon^4}{d^4}+\frac{\varepsilon^4}{d^4\langle\phi_{i_t}^t|\rho_t|\phi_{i_t}^t\rangle}\times\frac{\mathrm{Tr}(CC^\dagger)^2}{|\mathrm{Tr}(C)|^2}\right)$$
$$\leq\mathbb{E}_{i_{\leq t}}\mathbf{1}\{\mathcal{G}^c(t,i_{\leq t})\}\mathcal{O}\left(\frac{\varepsilon^4}{d^4}+\frac{\varepsilon^4}{d^4\langle\phi_{i_t}^t|\rho_t|\phi_{i_t}^t\rangle}\times\frac{d^2\mathrm{Tr}(CC^\dagger)}{\varepsilon^2}\right)\quad\left(\text{under }\mathcal{G}^c:|\mathrm{Tr}(C)|^2>\frac{\varepsilon^2}{d^2}\mathrm{Tr}(CC^\dagger)\right)$$
$$\leq\mathbb{E}_{i_{\leq t-1}}\sum_{i_t}\lambda_{i_t}^t\langle\phi_{i_t}^t|\rho_t|\phi_{i_t}^t\rangle\mathcal{O}\left(\frac{\varepsilon^4}{d^4}+\frac{\varepsilon^2\mathrm{Tr}(A_t^\dagger B_{i_t}^tB_{i_t}^{t,\dagger}A_t)}{d^2\langle\phi_{i_t}^t|\rho_t|\phi_{i_t}^t\rangle}\right)$$
$$\leq\mathbb{E}_{i_{\leq t-1}}\mathcal{O}\left(\frac{\varepsilon^4}{d^4}\right)+\mathcal{O}\left(\frac{\varepsilon^2\sum_{i_t}\lambda_{i_t}^t\mathrm{Tr}(A_t^\dagger B_{i_t}^tB_{i_t}^{t,\dagger}A_t)}{d^2}\right)$$
$$\leq\mathbb{E}_{i_{\leq t-1}}\mathcal{O}\left(\frac{\varepsilon^4}{d^4}\right)+\mathcal{O}\left(\frac{\varepsilon^2\mathrm{Tr}(A_t^\dagger dA_t)}{d^2}\right)=\mathbb{E}_{i_{\leq t-1}}\mathcal{O}\left(\frac{d\varepsilon^2}{d^2}\right)=\mathcal{O}\left(\frac{\varepsilon^2}{d}\right)\tag{9}$$

其中我们使用 $\sum_{i_t}\lambda_{i_t}^tB_{i_t}^tB^{t,}{}_{i_t}{}^\dagger=d\mathbb{I}$ 且 $\mathrm{Tr}(A_tA_t^\dagger)=1$。将 (7)、(8) 和 (9) 相加，得到:

$$\mathbb{E}_{i_{\leq t}}\mathbb{E}_{V\sim\mathrm{Haar}(d)}\mathbf{1}\{\mathcal{G}^c(t,i_{\leq t})\}(-\log)\left(\frac{\langle\phi_{i_t}^t|\,\mathrm{id}\otimes\mathcal{N}_V(\rho_t)\,|\phi_{i_t}^t\rangle}{\langle\phi_{i_t}^t|\rho_t|\phi_{i_t}^t\rangle}\right)$$
$$\leq\mathbb{E}_{i_{\leq t}}\mathbb{E}_{V\sim\mathrm{Haar}(d)}\mathbf{1}\{\mathcal{G}^c(t,i_{\leq t})\}\left(\frac{\Re(\langle\phi_{i_t}^t|(\mathbb{I}\otimes M_V)\rho_t(\mathbb{I}\otimes S_V^\dagger)|\phi_{i_t}^t\rangle)}{\langle\phi_{i_t}^t|\rho_t|\phi_{i_t}^t\rangle}+\frac{1}{2}\frac{\langle\phi_{i_t}^t|(\mathbb{I}\otimes M_V)\rho_t(\mathbb{I}\otimes M_V^\dagger)|\phi_{i_t}^t\rangle^2}{\langle\phi_{i_t}^t|\rho_t|\phi_{i_t}^t\rangle^2}\right)$$
$$+\mathbb{E}_{i_{\leq t}}\mathbb{E}_{V\sim\mathrm{Haar}(d)}\mathbf{1}\{\mathcal{G}^c(t,i_{\leq t})\}\left(2\frac{\langle\phi_{i_t}^t|(\mathbb{I}\otimes M_V)\rho_t(\mathbb{I}\otimes M_V^\dagger)|\phi_{i_t}^t\rangle}{\langle\phi_{i_t}^t|\rho_t|\phi_{i_t}^t\rangle}\right)=\mathcal{O}\left(\frac{\varepsilon^2}{d}\right).$$

因此，利用这个上界和上界 (4)，我们可以得到期望 KL 散度的一个上界：

$$\begin{aligned}\mathbb{E}_{V\sim\mathrm{Haar}(d)}\,\mathrm{KL}(P\|Q_V) &= \sum_{t=1}^{N}\mathbb{E}_{i\le t}\mathbb{E}_{V\sim\mathrm{Haar}(d)}(\mathbf{1}\{\mathcal{G}(t,i_{\le t})\}+\mathbf{1}\{\mathcal{G}^c(t,i_{\le t})\})(-\log)\left(\frac{\left\langle\phi_{i_t}^t\right|\mathrm{id}\otimes\mathcal{N}_V(\rho_t)\left|\phi_{i_t}^t\right\rangle}{\left\langle\phi_{i_t}^t\right|\rho_t\left|\phi_{i_t}^t\right\rangle}\right)\\ &\le \sum_{t=1}^{N}\mathcal{O}\left(\frac{\varepsilon^2}{d}\right)+\mathcal{O}\left(\frac{\varepsilon^2}{d}\right)=\mathcal{O}\left(\frac{N\varepsilon^2}{d}\right).\end{aligned}$$

最后，由于 $\mathrm{E}_{V\sim\mathrm{Haar}(d)}\,\mathrm{KL}(P\|Q_V)\ge\log(2)/3$，我们得出：

$$N=\Omega\left(\frac{d}{\varepsilon^2}\right).$$

□

C 延后证明：算法 2 中恒等性检验对去极化量子信道的分析

C.1 引理 4.2 的证明

引理 C.1. 设 $\mathcal{N}_1$ 和 $\mathcal{N}_2$ 是两个量子信道，d_{in}（分别为 d_{out}）是其输入（分别为输出）量子态的维数。我们有：

$$d_\diamond(\mathcal{N}_1,\mathcal{N}_2)\le d_{\mathrm{in}}\sqrt{d_{\mathrm{out}}}\|\mathcal{J}_{\mathcal{N}_1}-\mathcal{J}_{\mathcal{N}_2}\|_2.$$

证明. 记为 $\mathcal{M}=\mathcal{N}_1-\mathcal{N}_2$ 和 $\mathcal{J}=\mathcal{J}_{\mathcal{M}}=\mathcal{J}_{\mathcal{N}_1}-\mathcal{J}_{\mathcal{N}_2}$。设 $|\phi\rangle$ 是使菱形范数达到最大值的单位向量，即 $\|\mathrm{id}\otimes\mathcal{M}(|\phi\rangle\langle\phi|)\|_1=d_\diamond(\mathcal{N}_1,\mathcal{N}_2)$。我们可以写成 $|\phi\rangle=A\otimes\mathbb{I}\,|\Psi\rangle$，其中 $|\Psi\rangle=\frac{1}{\sqrt{d_{\mathrm{in}}}}\sum_{i=1}^{d_{\mathrm{in}}}|i\rangle\otimes|i\rangle$ 是最大纠缠态。$|\phi\rangle$ 的范数为 1，因此 $\mathrm{Tr}(A^\dagger A)=d_{\mathrm{in}}\langle\Psi|A^\dagger A\otimes\mathbb{I}\,|\Psi\rangle=d_{\mathrm{in}}\langle\phi|\phi\rangle=d_{\mathrm{in}}$.。我们可以将菱形距离写为：

$$\begin{aligned}d_\diamond(\mathcal{N}_1,\mathcal{N}_2)&=\|\mathrm{id}\otimes\mathcal{M}(|\phi\rangle\langle\phi|)\|_1=\|\mathrm{id}\otimes\mathcal{M}(A\otimes\mathbb{I}\,|\Psi\rangle\langle\Psi|\,A^\dagger\otimes\mathbb{I})\|_1\\ &=\|(A\otimes\mathbb{I})\mathrm{id}\otimes\mathcal{M}(|\Psi\rangle\langle\Psi|)(A^\dagger\otimes\mathbb{I})\|_1=\|(A\otimes\mathbb{I})\mathcal{J}_{\mathcal{M}}(A^\dagger\otimes\mathbb{I})\|_1.\end{aligned}$$

$\mathcal{J}_{\mathcal{M}}$ 是厄米的，因此可以写成：$\mathcal{J}_{\mathcal{M}}=\sum_i\lambda_i|\psi_i\rangle\langle\psi_i|$。利用三角不等式和柯西-施瓦茨不等式，我们得到：

$$\begin{aligned}\|(A\otimes\mathbb{I})\mathcal{J}_{\mathcal{M}}(A^\dagger\otimes\mathbb{I})\|_1&=\left\|(A\otimes\mathbb{I})\sum_i\lambda_i|\psi_i\rangle\langle\psi_i|\,(A^\dagger\otimes\mathbb{I})\right\|_1\\ &\le\sum_i|\lambda_i|\|(A\otimes\mathbb{I})\,|\psi_i\rangle\langle\psi_i|\,(A^\dagger\otimes\mathbb{I})\|_1\le\sqrt{\sum_i\lambda_i^2}\sqrt{\sum_i\langle\psi_i|\,(A^\dagger A\otimes\mathbb{I})\,|\psi_i\rangle^2}\\ &\le\|\mathcal{J}\|_2\sqrt{\sum_i\langle\psi_i|\,(A^\dagger AA^\dagger A\otimes\mathbb{I})\,|\psi_i\rangle}=\|\mathcal{J}_{\mathcal{M}}\|_2\sqrt{\mathrm{Tr}(A^\dagger AA^\dagger A\otimes\mathbb{I})}\\ &=\|\mathcal{J}_{\mathcal{M}}\|_2\sqrt{d_{\mathrm{out}}\mathrm{Tr}(A^\dagger AA^\dagger A)}\le\|\mathcal{J}_{\mathcal{M}}\|_2\sqrt{d_{\mathrm{out}}(\mathrm{Tr}(A^\dagger A))^2}=d_{\mathrm{in}}\sqrt{d_{\mathrm{out}}}\|\mathcal{J}_{\mathcal{M}}\|_2.\end{aligned}$$

□

C.2 引理 4.1 的证明

Le引理 C.2. 设 $\mathcal{J} = \mathrm{id} \otimes \mathcal{N}(|\Psi\rangle\langle\Psi|)$ 为量子信道 $\mathcal{N}$ 对应的 Choi 态 .

$$\mathbb{E}\left(\left\|\mathcal{N}(|\phi\rangle\langle\phi|) - \frac{\mathbb{I}}{d_{\mathrm{out}}}\right\|_2^2\right) = \frac{\left(\mathrm{Tr}\left(\mathcal{N}(\mathbb{I}) - \frac{d_{\mathrm{in}}}{d_{\mathrm{out}}}\mathbb{I}\right)^2 + d_{\mathrm{in}}^2\left\|\mathcal{J} - \frac{\mathbb{I}}{d_{\mathrm{in}}d_{\mathrm{out}}}\right\|_2^2\right)}{d_{\mathrm{in}}(d_{\mathrm{in}}+1)} \geq \frac{d_{\mathrm{in}}}{d_{\mathrm{in}}+1}\left\|\mathcal{J} - \frac{\mathbb{I}}{d_{\mathrm{in}}d_{\mathrm{out}}}\right\|_2^2.$$

证明。我们写作

$$\mathbb{E}\left(\left\|\mathcal{N}(|\phi\rangle\langle\phi|) - \frac{\mathbb{I}}{d_{\mathrm{out}}}\right\|_2^2\right) = \mathbb{E}\left(\mathrm{Tr}(\mathcal{N}(|\phi\rangle\langle\phi|)^2)\right) - \frac{1}{d_{\mathrm{out}}}.$$

那么，如果我们使用量子信道 $\mathcal{N}(\rho) = \sum_k A_k\rho A_k^\dagger$ 的 Kraus 分解，就可以利用 Weingarten演算计算以下期望（引理 F.1 和引理 F.3）：

$$\begin{aligned}
\mathbb{E}\left(\mathrm{Tr}(\mathcal{N}(|\phi\rangle\langle\phi|)^2)\right) &= \mathbb{E}\left(\mathrm{Tr}\left(\sum_k A_k|\phi\rangle\langle\phi|A_k^\dagger\right)^2\right) = \sum_{k,l}\mathbb{E}\left(\mathrm{Tr}(A_k|\phi\rangle\langle\phi|A_k^\dagger A_l|\phi\rangle\langle\phi|A_l^\dagger)\right) \\
&= \frac{1}{d_{\mathrm{in}}(d_{\mathrm{in}}+1)}\left(\sum_{k,l}\mathrm{Tr}(A_k^\dagger A_l A_l^\dagger A_k) + \sum_{k,l}|\mathrm{Tr}(A_k A_l^\dagger)|^2\right) \\
&= \frac{1}{d_{\mathrm{in}}(d_{\mathrm{in}}+1)}\left(\mathrm{Tr}\left(\sum_k A_k A_k^\dagger\right)^2 + \sum_{k,l}|\mathrm{Tr}(A_k A_l^\dagger)|^2\right) \\
&= \frac{1}{d_{\mathrm{in}}(d_{\mathrm{in}}+1)}\left(\mathrm{Tr}(\mathcal{N}(\mathbb{I})^2) + \sum_{k,l}|\mathrm{Tr}(A_k A_l^\dagger)|^2\right)
\end{aligned}$$

注意，$\mathrm{Tr}(\mathcal{N}(\mathbb{I})^2) = \mathrm{Tr}\left(\mathcal{N}(\mathbb{I}) - \frac{d_{\mathrm{in}}}{d_{\mathrm{out}}}\mathbb{I}\right)^2 + \frac{d_{\mathrm{in}}^2}{d_{\mathrm{out}}}$。此外，

$$\begin{aligned}
\mathrm{Tr}(\mathcal{J}^2) &= \mathrm{Tr}\left(\frac{1}{d_{\mathrm{in}}}\sum_{i,j}|i\rangle\langle j| \otimes \mathcal{N}(|i\rangle\langle j|)\right)^2 = \frac{1}{d_{\mathrm{in}}^2}\sum_{i,j}\mathrm{Tr}(\mathcal{N}(|i\rangle\langle j|)\mathcal{N}(|j\rangle\langle i|)) \\
&= \frac{1}{d_{\mathrm{in}}^2}\sum_{i,j,k,l}\mathrm{Tr}(A_k|i\rangle\langle j|A_k^\dagger A_l|j\rangle\langle i|A_l^\dagger) = \frac{1}{d_{\mathrm{in}}^2}\sum_{k,l}|\mathrm{Tr}(A_k^\dagger A_l)|^2
\end{aligned}$$

因此:

$$\begin{aligned}
\mathbb{E}\left(\mathrm{Tr}(\mathcal{N}(|\phi\rangle\langle\phi|)^2)\right) &= \mathbb{E}\left(\mathrm{Tr}\left(\sum_k A_k|\phi\rangle\langle\phi|A_k^\dagger\right)^2\right) \\
&= \frac{1}{d_{\mathrm{in}}(d_{\mathrm{in}}+1)}\left(\mathrm{Tr}\left(\mathcal{N}(\mathbb{I}) - \frac{d_{\mathrm{in}}}{d_{\mathrm{out}}}\mathbb{I}\right)^2 + \frac{d_{\mathrm{in}}^2}{d_{\mathrm{out}}} + d_{\mathrm{in}}^2\mathrm{Tr}(\mathcal{J}^2)\right)
\end{aligned}$$

最后，

$$\begin{aligned}
\mathbb{E}\left(\left\|\mathcal{N}(|\phi\rangle\langle\phi|)-\frac{\mathbb{I}}{d_{\text{out}}}\right\|_2^2\right) &= \mathbb{E}\left(\text{Tr}(\mathcal{N}(|\phi\rangle\langle\phi|)^2)\right)-\frac{1}{d_{\text{out}}} \\
&= \frac{1}{d_{\text{in}}(d_{\text{in}}+1)}\left(\text{Tr}\left(\mathcal{N}(\mathbb{I})-\frac{d_{\text{in}}}{d_{\text{out}}}\mathbb{I}\right)^2+\frac{d_{\text{in}}^2}{d_{\text{out}}}+d_{\text{in}}^2\text{Tr}(\mathcal{J}^2)\right)-\frac{1}{d_{\text{out}}} \\
&= \frac{1}{d_{\text{in}}(d_{\text{in}}+1)}\left(\text{Tr}\left(\mathcal{N}(\mathbb{I})-\frac{d_{\text{in}}}{d_{\text{out}}}\mathbb{I}\right)^2+d_{\text{in}}^2\text{Tr}(\mathcal{J}^2)-\frac{d_{\text{in}}}{d_{\text{out}}}\right) \\
&= \frac{1}{d_{\text{in}}(d_{\text{in}}+1)}\left(\text{Tr}\left(\mathcal{N}(\mathbb{I})-\frac{d_{\text{in}}}{d_{\text{out}}}\mathbb{I}\right)^2+d_{\text{in}}^2\left\|\mathcal{J}-\frac{\mathbb{I}}{d_{\text{in}}d_{\text{out}}}\right\|_2^2\right).
\end{aligned}$$

□

C.3 定理 4.3 的证明

定理 C.3. 设 $|\phi\rangle$ 是 S^d 中的 Haar 分布向量。设 $X=\left\|\mathcal{N}(|\phi\rangle\langle\phi|)-\frac{\mathbb{I}}{d_{\text{out}}}\right\|_2^2$。我们有：

$$\text{Var}(X)=\mathcal{O}\left(\mathbb{E}\,(X)^2\right).$$

证明. 回忆一下，$X=\left\|\mathcal{N}(|\phi\rangle\langle\phi|)-\frac{\mathbb{I}}{d_{\text{out}}}\right\|_2^2$。我们可以观察到：

$$\text{Var}(X)=\text{Var}\left(\text{Tr}\left(\mathcal{N}(|\phi\rangle\langle\phi|)\right)^2-\frac{1}{d_{\text{out}}}\right)=\text{Var}\left(\text{Tr}\left(\mathcal{N}(|\phi\rangle\langle\phi|)\right)^2\right).$$

我们使用 Kraus记号 $\mathcal{N}(\rho)=\sum_k A_k\rho A_k^\dagger$ 和 $d=d_{\text{in}}$。通过 Weingarten演算（引理 F.1 和引理 F.3），我们可以计算期望：

$$\begin{aligned}
&\mathbb{E}\left(\left(\text{Tr}\left(\mathcal{N}(|\phi\rangle\langle\phi|)\right)^2\right)^2\right)=\mathbb{E}\left(\left(\text{Tr}\sum_{k,l}A_k|\phi\rangle\langle\phi|A_k^\dagger A_l|\phi\rangle\langle\phi|A_l^\dagger\right)^2\right) \\
&=\sum_{i,j}\sum_{k,l,k',l'}\mathbb{E}\left(\text{Tr}A_{l'}^\dagger|j\rangle\langle i|A_k|\phi\rangle\langle\phi|A_k^\dagger A_l|\phi\rangle\langle\phi|A_l^\dagger|i\rangle\langle j|A_{k'}|\phi\rangle\langle\phi|A_{k'}^\dagger A_{l'}|\phi\rangle\langle\phi|\right) \\
&=\sum_{i,j}\sum_{k,l,k',l'}\frac{1}{d(d+1)(d+2)(d+3)}\sum_{\alpha\in\mathfrak{S}_4}\text{Tr}_\alpha(A_{l'}^\dagger|j\rangle\langle i|A_k,A_k^\dagger A_l,A_l^\dagger|i\rangle\langle j|A_{k'},A_{k'}^\dagger A_{l'}) \\
&=\frac{1}{d(d+1)(d+2)(d+3)}\sum_{\alpha\in\mathfrak{S}_4}\sum_{i,j,k,l,k',l'}\text{Tr}_\alpha(A_{l'}^\dagger|j\rangle\langle i|A_k,A_k^\dagger A_l,A_l^\dagger|i\rangle\langle j|A_{k'},A_{k'}^\dagger A_{l'}) \\
&=\frac{1}{d(d+1)(d+2)(d+3)}\sum_{\alpha\in\mathfrak{S}_4}F(\alpha)
\end{aligned}$$

其中，对于 $\alpha\in\mathfrak{S}_4$，我们采用记号 $F(\alpha)=\sum_{i,\ j,\ k,\ l,\ k',\ l'}$迹$_\alpha(A_{l'}^\dagger|j\rangle\langle i|A_k,A_k^\dagger A_l,A_l^\dagger|i\rangle\langle j|A_{k'},A_{k'}^\dagger A_{l'})$，其中 $\text{Tr}_\alpha(M_1,\ldots,M_n)=\Pi_j\text{Tr}(\Pi_{i\in C_j}M_i)$，对于 $\alpha=\Pi_jC_j$和 C_j，它们是循环。因此，为了得到方差的上界，必须控制这 24 项中的每一项。此外，我们还需要谨慎处理，以便

使我们对 $\{F(\alpha)\}_{\alpha\in\mathfrak{S}_4}$ 的上界取决于检验问题的实际参数。回想一下， X 的期望值可表示如下：

$$\mathbb{E}(X)=\frac{1}{d_{\text{in}}(d_{\text{in}}+1)}\left(\operatorname{Tr}\left(\mathcal{N}(\mathbb{I})-\frac{d_{\text{in}}}{d_{\text{out}}}\mathbb{I}\right)^2+d_{\text{in}}^2\left\|\mathcal{J}-\frac{\mathbb{I}}{d_{\text{in}}d_{\text{out}}}\right\|_2^2\right).$$

我们定义 $\mathcal{M}=\mathcal{N}-\mathcal{D}$、 $m=\|\mathcal{M}(\mathbb{I}_{d_{\text{in}}})\|_2=\left\|\mathcal{N}(\mathbb{I})-\frac{d_{\text{in}}}{d_{\text{out}}}\mathbb{I}\right\|_2$ 以及 $\eta=d_{\text{in}}\left\|\mathcal{J}-\frac{\mathbb{I}}{d_{\text{in}}d_{\text{out}}}\right\|_2$。我们陈述一个联系 η、 $\mathcal{M}$ 和 Kraus 算子 $\{A_k\}_k$的有用引理：

引理 C.4. 设 $\eta=d_{\text{in}}\|\mathcal{J}-\mathbb{I}/(d_{\text{in}}d_{\text{out}})\|_2$ 和 $\mathcal{M}=\mathcal{N}-\mathcal{D}$，则有：

- $\eta^2=\sum_{k,l}|\operatorname{Tr}(A_k^\dagger A_l)|^2-\frac{d_{\text{in}}}{d_{\text{out}}}$,
- $\eta^2=\sum_{x,y=1}^{d_{\text{in}}}\|\mathcal{M}(|x\rangle\langle y|)\|_2^2$.

证明。回顾 w e 使用量子信道 $\mathcal{N}(\rho)=\sum_k A_k\rho A_k^\dagger$ 的 Kraus 表示。我们可以表示 η^2 ：

$$\begin{aligned}\eta^2&=\left\|d_{\text{in}}\mathcal{J}-\frac{\mathbb{I}}{d_{\text{out}}}\right\|_2^2=d_{\text{in}}^2\operatorname{Tr}(\mathcal{J}^2)-\frac{d_{\text{in}}}{d_{\text{out}}}=\operatorname{Tr}\left(\sum_{i,j,k}|i\rangle\langle j|\otimes A_k|i\rangle\langle j|A_k^\dagger\right)^2-\frac{d_{\text{in}}}{d_{\text{out}}}\\&=\sum_{i,j,k,l}\operatorname{Tr}(A_k|i\rangle\langle j|A_k^\dagger A_l|j\rangle\langle i|A_l^\dagger)-\frac{d_{\text{in}}}{d_{\text{out}}}=\sum_{k,l}|\operatorname{Tr}(A_k^\dagger A_l)|^2-\frac{d_{\text{in}}}{d_{\text{out}}}.\end{aligned}$$

转到第二点，我们有 $\mathcal{J}-\mathbb{I}/(d_{\text{in}}d_{\text{out}})=\mathcal{J}_{\mathcal{N}}-\mathcal{J}_{\mathcal{D}}=\mathcal{J}_{\mathcal{M}}=\text{id}\otimes\mathcal{M}(|\Psi\rangle\langle\Psi|)$，因此

$$\begin{aligned}\eta^2&=d_{\text{in}}^2\operatorname{Tr}(\text{id}\otimes\mathcal{M}(|\Psi\rangle\langle\Psi|))^2=\operatorname{Tr}(\text{id}\otimes\mathcal{M}(d_{\text{in}}|\Psi\rangle\langle\Psi|))^2=\operatorname{Tr}\left(\sum_{x,y}|x\rangle\langle y|\otimes\mathcal{M}(|x\rangle\langle y|)\right)^2\\&=\sum_{x,y}\operatorname{Tr}(\mathcal{M}(|x\rangle\langle y|)\mathcal{M}(|y\rangle\langle x|))=\sum_{x,y}\|\mathcal{M}(|x\rangle\langle y|)\|_2^2.\end{aligned}$$

□

另一方面，在处理某些 $F(\alpha)$'s 时，我们需要矩阵$\sum_k A_k\otimes A_k$的一些性质。

引理 C.5. 设 $M=\sum_k A_k\otimes\bar{A}_k$。设 $\{\lambda_i\}_i$ 为与本征态 $\{|\phi_i\rangle\}_i$相对应的 $M^\dagger M$ 的特征值集合（按降序排列）。我们有：

- $\sum_i\lambda_i=\frac{d_{\text{in}}}{d_{\text{out}}}+\eta^2$,
- $\lambda_1\geq\frac{d_{\text{in}}}{d_{\text{out}}},\sum_{i>1}\lambda_i\leq\eta^2$,
- $\frac{d_{\text{in}}^2}{d_{\text{out}}^2}(1-|\langle\phi_1|\Psi\rangle|^2)\leq\frac{2m^2\eta^2}{d_{\text{in}}}+2\eta^4$,
- $\langle\Psi|MM^\dagger|\Psi\rangle=\frac{d_{\text{in}}}{d_{\text{out}}}$.

证明。由引理 C.4 可得 $\sum_i \lambda_i = \mathrm{Tr}(M^\dagger M) = \sum_{k,l} \mathrm{Tr}(A_k^\dagger A_l)\mathrm{Tr}(A_k^\top \bar{A}_l) = \sum_{k,l} |\mathrm{Tr}(A_k^\dagger A_l)|^2 = \frac{d_{\mathrm{in}}}{d_{\mathrm{out}}} + \eta^2$。回顾未归一化最大纠缠态 $\sqrt{d_{\mathrm{in}}}\,|\Psi\rangle = \sum_i |i\rangle \otimes |i\rangle$ 的定义，我们可以计算它在矩阵 $M^\dagger M$ 下的像：

$$\begin{aligned} M^\dagger M(\sqrt{d_{\mathrm{in}}}\,|\Psi\rangle) &= \sum_{i,k,l} A_k^\dagger A_l\,|i\rangle \otimes A_k^\top \bar{A}_l\,|i\rangle = \sum_{x,y,i,k,l} \langle x|\, A_k^\dagger A_l\,|i\rangle\, \langle y|\, A_k^\top \bar{A}_l\,|i\rangle\, |xy\rangle \\ &= \sum_{x,y,i,k,l} \langle x|\, A_k^\dagger A_l\,|i\rangle\, \langle i|\, A_l^\dagger A_k\,|y\rangle\, |xy\rangle = \sum_{x,y,k} \langle x|\, A_k^\dagger \mathcal{N}(\mathbb{I}) A_k\,|y\rangle\, |xy\rangle \end{aligned}$$

因此

$$\langle\Psi|\, M^\dagger M\,|\Psi\rangle = \frac{1}{d_{\mathrm{in}}} \sum_{i,k} \langle i|\, A_k^\dagger \mathcal{N}(\mathbb{I}) A_k\,|i\rangle = \frac{\mathrm{Tr}(\mathcal{N}(\mathbb{I})^2)}{d_{\mathrm{in}}} \geq \frac{d_{\mathrm{in}}^2}{d_{\mathrm{in}} d_{\mathrm{out}}} = \frac{d_{\mathrm{in}}}{d_{\mathrm{out}}}$$

其中我们使用了柯西-施瓦茨不等式。这意味着最大特征值满足 $\lambda_1 \geq \frac{d_{\mathrm{in}}}{d_{\mathrm{out}}}$因此 $\sum_{i>1} \lambda_i = \frac{d_{\mathrm{in}}}{d_{\mathrm{out}}} + \eta^2 - \lambda_1 \leq \eta^2$。

下面证明第三点。回顾记号 $\mathcal{M}(\rho) = (\mathcal{N} - \mathcal{D})(\rho) = \sum_k A_k \rho A_k^\dagger - \text{迹}(\rho)\,\frac{\mathbb{I}}{d_{\mathrm{out}}}$。一方面，我们有：

$$\begin{aligned} M^\dagger M(\sqrt{d_{\mathrm{in}}}\,|\Psi\rangle) &= \sum_{x,y,k} \langle x|\, A_k^\dagger \mathcal{N}(\mathbb{I}) A_k\,|y\rangle\, |xy\rangle = \sum_{x,y} \mathrm{Tr}(\mathcal{N}(\mathbb{I})\mathcal{N}(|y\rangle\langle x|))\,|xy\rangle \\ &= \sum_{x,y} \mathrm{Tr}(\mathcal{N}(\mathbb{I})\mathcal{M}(|y\rangle\langle x|))\,|xy\rangle + \sum_{x,y} \mathrm{Tr}(\mathcal{N}(\mathbb{I})\mathcal{D}(|y\rangle\langle x|))\,|xy\rangle \\ &= \sum_{x,y} \mathrm{Tr}(\mathcal{M}(\mathbb{I})\mathcal{M}(|y\rangle\langle x|))\,|xy\rangle + \sum_x \frac{1}{d_{\mathrm{out}}} \mathrm{Tr}(\mathcal{N}(\mathbb{I})\mathbb{I})\,|xx\rangle \\ &= \sum_{x,y} \mathrm{Tr}(\mathcal{M}(\mathbb{I})\mathcal{M}(|y\rangle\langle x|))\,|xy\rangle + \frac{d_{\mathrm{in}}}{d_{\mathrm{out}}} \sqrt{d_{\mathrm{in}}}\,|\Psi\rangle\,. \end{aligned}$$

另一方面，利用 $M^\dagger M$ 的谱分解，我们可以写出：

$$\sum_{x,y} \mathrm{Tr}(\mathcal{M}(\mathbb{I})\mathcal{M}(|y\rangle\langle x|))\,|xy\rangle + \frac{d_{\mathrm{in}}}{d_{\mathrm{out}}} \sqrt{d_{\mathrm{in}}}\,|\Psi\rangle = M^\dagger M(\sqrt{d_{\mathrm{in}}}\,|\Psi\rangle) = \sum_i \lambda_i \sqrt{d_{\mathrm{in}}} \langle\phi_i|\Psi\rangle\,|\phi_i\rangle\,.$$

因此

$$\lambda_1 \langle\phi_1|\Psi\rangle\,|\phi_1\rangle - \frac{d_{\mathrm{in}}}{d_{\mathrm{out}}}\,|\Psi\rangle = \frac{1}{\sqrt{d_{\mathrm{in}}}} \sum_{x,y} \mathrm{Tr}(\mathcal{M}(\mathbb{I})\mathcal{M}(|y\rangle\langle x|))\,|xy\rangle - \sum_{i>1} \lambda_i \langle\phi_i|\Psi\rangle\,|\phi_i\rangle\,.$$

对两边取 2-范数的平方，然后应用三角不等式、事实 $(x+y)^2 \leq 2(x^2+y^2)$

以及柯西-施瓦茨不等式，可得：

$$\begin{aligned}
&\lambda_1^2|\langle\phi_1|\Psi\rangle|^2+\frac{d_{\text{in}}^2}{d_{\text{out}}^2}-2\frac{d_{\text{in}}}{d_{\text{out}}}\lambda_1|\langle\phi_1|\Psi\rangle|^2\\
&=\left\|\frac{1}{\sqrt{d_{\text{in}}}}\sum_{x,y}\text{Tr}(\mathcal{M}(\mathbb{I})\mathcal{M}(|y\rangle\langle x|))|xy\rangle-\sum_{i>1}\lambda_i\langle\phi_i|\Psi\rangle|\phi_i\rangle\right\|_2^2\\
&\leq\left(\left\|\frac{1}{\sqrt{d_{\text{in}}}}\sum_{x,y}\text{Tr}(\mathcal{M}(\mathbb{I})\mathcal{M}(|y\rangle\langle x|))|xy\rangle\right\|_2+\left\|\sum_{i>1}\lambda_i\langle\phi_i|\Psi\rangle|\phi_i\rangle\right\|_2\right)^2\\
&\leq 2\left\|\frac{1}{\sqrt{d_{\text{in}}}}\sum_{x,y}\text{Tr}(\mathcal{M}(\mathbb{I})\mathcal{M}(|y\rangle\langle x|))|xy\rangle\right\|_2^2+2\left\|\sum_{i>1}\lambda_i\langle\phi_i|\Psi\rangle|\phi_i\rangle\right\|_2^2\\
&\leq\frac{2}{d_{\text{in}}}\sum_{x,y}|\text{Tr}(\mathcal{M}(\mathbb{I})\mathcal{M}(|y\rangle\langle x|))|^2+2\sum_{i>1}\lambda_i^2\\
&\leq\frac{2}{d_{\text{in}}}\sum_{x,y}\|\mathcal{M}(\mathbb{I})\|_2^2\|\mathcal{M}(|y\rangle\langle x|)\|_2^2+2\left(\sum_{i>1}\lambda_i\right)^2\leq\frac{2m^2\eta^2}{d_{\text{in}}}+2\eta^4.
\end{aligned}$$

注意到，左端可以按如下方式给出下界：

$$\begin{aligned}
\lambda_1^2|\langle\phi_1|\Psi\rangle|^2+\frac{d_{\text{in}}^2}{d_{\text{out}}^2}-2\frac{d_{\text{in}}}{d_{\text{out}}}\lambda_1|\langle\phi_1|\Psi\rangle|^2&=\left(\lambda_1-\frac{d_{\text{in}}}{d_{\text{out}}}\right)^2|\langle\phi_1|\Psi\rangle|^2+\frac{d_{\text{in}}^2}{d_{\text{out}}^2}-\frac{d_{\text{in}}^2}{d_{\text{out}}^2}|\langle\phi_1|\Psi\rangle|^2\\
&\geq\frac{d_{\text{in}}^2}{d_{\text{out}}^2}(1-|\langle\phi_1|\Psi\rangle|^2).
\end{aligned}$$

最后，我们由前两个不等式推得：

$$\frac{d_{\text{in}}^2}{d_{\text{out}}^2}(1-|\langle\phi_1|\Psi\rangle|^2)\leq\frac{2m^2\eta^2}{d_{\text{in}}}+2\eta^4.$$

接下来讨论第四点。我们有：

$$\begin{aligned}
MM^\dagger(\sqrt{d_{\text{in}}}|\Psi\rangle)&=\sum_{i,k,l}A_kA_l^\dagger|i\rangle\otimes\bar{A}_kA_l^\top|i\rangle=\sum_{x,y,i,k,l}\langle x|A_kA_l^\dagger|i\rangle\langle y|\bar{A}_kA_l^\top|i\rangle|xy\rangle\\
&=\sum_{x,y,i,k,l}\langle x|A_kA_l^\dagger|i\rangle\langle i|A_lA_k^\dagger|y\rangle|xy\rangle=\sum_{x,y}\langle x|\mathcal{N}(\mathbb{I})|y\rangle|xy\rangle\\
&=\sum_{x,y}\langle x|\mathcal{M}(\mathbb{I})|y\rangle|xy\rangle+\frac{d_{\text{in}}}{d_{\text{out}}}\sqrt{d_{\text{in}}}|\Psi\rangle.
\end{aligned}$$

因此：

$$\langle\Psi|MM^\dagger|\Psi\rangle=\frac{1}{d_{\text{in}}}\sum_x\langle x|\mathcal{M}(\mathbb{I})|x\rangle+\frac{d_{\text{in}}}{d_{\text{out}}}\langle\Psi|\Psi\rangle=\frac{1}{d_{\text{in}}}\text{Tr}(\mathcal{M}(\mathbb{I}))+\frac{d_{\text{in}}}{d_{\text{out}}}=\frac{d_{\text{in}}}{d_{\text{out}}}.$$

□

第一点和第四点将用于引理 C.10 的证明。前三点表明，矩阵 $M^\dagger M$（归一化后）在 1-范数意义下接近最大纠缠态。

引理 C.6。设 $M = \sum_k A_k \otimes \bar{A}_k$ 和 $|\Psi\rangle = \frac{1}{\sqrt{d_{\text{in}}}} \sum_{i=1}^{d_{\text{in}}} |i\rangle \otimes |i\rangle$。我们有：

$$\left\| M^\dagger M - \frac{d_{\text{in}}}{d_{\text{out}}} |\Psi\rangle\langle\Psi| \right\|_1 \leq 5\eta^2.$$

证明。令 $|\phi_1\rangle$ 为对应于 $M^\dagger M$ 最大特征值的特征向量。利用 Fuchs–van de Graaf 不等式 [Fuchs 和 Van De Graaf, 1999] 以及引理 C.5：

$$\| |\phi_1\rangle\langle\phi_1| - |\Psi\rangle\langle\Psi| \|_1 \leq 2\sqrt{1 - |\langle\phi_1|\Psi\rangle|^2} \leq 2\frac{d_{\text{out}}}{d_{\text{in}}}\sqrt{\frac{2m^2\eta^2}{d_{\text{in}}} + 2\eta^4} \leq 4\frac{d_{\text{out}}}{d_{\text{in}}}\eta^2$$

这里我们使用柯西-施瓦茨不等式和引理 C.4：

$$\begin{aligned} m^2 = \text{Tr}(\mathcal{M}(\mathbb{I})^2) &= \sum_{i,j} \text{Tr}(\mathcal{M}(|i\rangle\langle i|)\mathcal{M}(|j\rangle\langle j|)) \\ &\leq \sum_{i,j} \text{Tr}(\mathcal{M}(|i\rangle\langle i|)^2) = d_{\text{in}} \sum_i \text{Tr}(\mathcal{M}(|i\rangle\langle i|)^2) \leq d_{\text{in}}\eta^2. \end{aligned}$$

由三角不等式和引理 C.5，我们可得：

$$\begin{aligned} \left\| M^\dagger M - \frac{d_{\text{in}}}{d_{\text{out}}} |\Psi\rangle\langle\Psi| \right\|_1 &\leq \left\| M^\dagger M - \frac{d_{\text{in}}}{d_{\text{out}}} |\phi_1\rangle\langle\phi_1| \right\|_1 + \frac{d_{\text{in}}}{d_{\text{out}}} \| |\phi_1\rangle\langle\phi_1| - |\Psi\rangle\langle\Psi| \|_1 \\ &\leq \lambda_1 - \frac{d_{\text{in}}}{d_{\text{out}}} + \sum_{i>1} \lambda_i + 4\eta^2 = 5\eta^2. \end{aligned}$$

□

该引理将在引理 C.7、C.9、C.8 和 C.11 的证明中使用。现在我们来求函数 F不同取值的上界。

引理 C.7。我们可以如下给出 F((142)) 和 F((243)) 的上界：

$$F((142)) = F((243)) \leq \frac{d_{\text{in}}/d_{\text{out}} + \eta^2}{d_{\text{out}}} + \frac{\eta^2}{d_{\text{out}}} + 5\eta^4.$$

证明。回顾记号 $\mathcal{M}(\rho) = (\mathcal{N} - \mathcal{D})(\rho) = \sum_k A_k \rho A_k^\dagger - \text{迹}(\rho)\frac{\mathbb{I}}{d_{\text{out}}}$。我们首先将 F((142)) 写成两项之和：一项是反映零假设的理想项（$\mathcal{N} = \mathcal{D}$），另一项是反映 $\mathcal{N}$ 与 $\mathcal{D}$ 之间差异的误差项。理想项可以精确计算，且取决于维数 d_{in} 和 d_{out}。误差项还可以拆分为一项仅取决于 η 和 d_{out} 的简单误差，以及一项更复杂的误差，该项取决于 Kraus 算子 $\{A_k\}_k$ 和量子信道 $\mathcal{M}$ 之间的差异。为了控制后一项误差，我们首先用 $\mathcal{M}$、$M = \sum_k A_k \otimes A_k^\dagger$ 和翻转算子 F 将其写成闭式。接着，我们可以利用矩阵 $M^\dagger M - \frac{d_{\text{in}}}{d_{\text{out}}} |\Psi\rangle\langle\Psi|$ 的谱分解，将此误差项分解为若干可忽略项的组合。最后一步需要控制该组合系数的 ℓ_1 范数，这可通过引理 C.6 完成。

我们有：

$$
\begin{aligned}
F((142)) &= \sum_{k,l,k',l'} \mathrm{Tr}(A_k A_{k'}^\dagger A_{l'} A_k^\dagger A_l A_{l'}^\dagger A_{k'} A_l^\dagger) = \sum_{k,l} \mathrm{Tr}(\mathcal{N}(A_l^\dagger A_k)\mathcal{N}(A_k^\dagger A_l)) \\
&= \sum_{k,l} \mathrm{Tr}(\mathcal{M}(A_l^\dagger A_k)\mathcal{N}(A_k^\dagger A_l)) + \mathrm{Tr}(\mathcal{D}(A_l^\dagger A_k)\mathcal{N}(A_k^\dagger A_l)) \\
&= \sum_{k,l} \mathrm{Tr}(\mathcal{M}(A_l^\dagger A_k)\mathcal{M}(A_k^\dagger A_l)) + \mathrm{Tr}(\mathcal{D}(A_l^\dagger A_k)\mathcal{N}(A_k^\dagger A_l)) + \mathrm{Tr}(\mathcal{M}(A_l^\dagger A_k)\mathcal{D}(A_k^\dagger A_l)) \\
&= \sum_{k,l} \mathrm{Tr}(\mathcal{M}(A_l^\dagger A_k)\mathcal{M}(A_k^\dagger A_l)) + \frac{\mathrm{Tr}(A_l^\dagger A_k)}{d_{\mathrm{out}}}\mathrm{Tr}(\mathcal{N}(A_k^\dagger A_l)) + \frac{\mathrm{Tr}(A_k^\dagger A_l)}{d_{\mathrm{out}}}\mathrm{Tr}(\mathcal{M}(A_l^\dagger A_k)) \\
&= \sum_{k,l} \mathrm{Tr}(\mathcal{M}(A_l^\dagger A_k)\mathcal{M}(A_k^\dagger A_l)) + \frac{\mathrm{Tr}(A_l^\dagger A_k)}{d_{\mathrm{out}}}\mathrm{Tr}(A_k^\dagger A_l) \\
&= \sum_{k,l} \mathrm{Tr}(\mathcal{M}(A_l^\dagger A_k)\mathcal{M}(A_k^\dagger A_l)) + \frac{\eta^2 + d_{\mathrm{in}}/d_{\mathrm{out}}}{d_{\mathrm{out}}}.
\end{aligned}
$$

接下来需要控制求和 $\sum_{k,l} \mathrm{Tr}(\mathcal{M}(A_l^\dagger A_k)\mathcal{M}(A_k^\dagger A_l))$。令 $\mathrm{T}_2 : \ X \otimes Y \mapsto X \otimes Y^\top$ 为部分转置算子，并令 $M = \sum_l A_l \otimes \bar{A}_l$。令 $\mathrm{F} = \sum_{i,j=1}^d |i\rangle \otimes |j\rangle)(\langle j| \otimes \langle i|)$ 为翻转算子，则有 $\mathrm{Tr}(A \otimes B\mathrm{F}) = \sum_{i,j,k,l} A_{i,j} B_{k,l} \mathrm{Tr}(|i\rangle \langle j| \otimes |k\rangle \langle l| \mathrm{F}) = \sum_{i,j,k,l} A_{i,j} B_{k,l} \mathrm{Tr}(|i\rangle \langle l| \otimes |k\rangle \langle j|) = \sum_{i,j} A_{i,j} B_{j,i} = \mathrm{Tr}(AB)$，这被称为复制技巧。利用复制技巧，我们有：

$$
\begin{aligned}
\sum_{k,l} \mathrm{Tr}(\mathcal{M}(A_l^\dagger A_k)\mathcal{M}(A_k^\dagger A_l)) &= \sum_{k,l} \mathrm{Tr}(\mathcal{M}(A_l^\dagger A_k) \otimes \mathcal{M}(A_k^\dagger A_l)\mathbb{F}) \\
&= \mathrm{Tr}\left(\mathcal{M} \otimes \mathcal{M}\left(\sum_{k,l} A_l^\dagger A_k \otimes A_k^\dagger A_l\right)\mathbb{F}\right) \\
&= \mathrm{Tr}\left(\mathcal{M} \otimes \mathcal{M} \circ \mathrm{T}_2\left(\sum_{k,l} A_l^\dagger A_k \otimes A_l^\top \bar{A}_k\right)\mathbb{F}\right) \\
&= \mathrm{Tr}\left(\mathcal{M} \otimes \mathcal{M} \circ \mathrm{T}_2(M^\dagger M)\mathbb{F}\right)
\end{aligned}
$$

令 $|\phi\rangle$ 为一个单位向量，我们可以写成 $|\phi\rangle = \sum_{x,y} \phi_{x,y} |x\rangle \otimes |y\rangle$ 于是可以表示为:

$$\begin{aligned}
|\mathrm{Tr}\left(\mathcal{M}\otimes\mathcal{M}\circ \mathrm{T}_2(|\phi\rangle\langle\phi|)\mathbb{F}\right)| &= \left|\sum_{x,y,z,t} \phi_{x,y}\bar{\phi}_{z,t}\mathrm{Tr}\left(\mathcal{M}\otimes\mathcal{M}\circ \mathrm{T}_2(|x\rangle\langle z|\otimes|y\rangle\langle t|)\mathbb{F}\right)\right| \\
&= \left|\sum_{x,y,z,t} \phi_{x,y}\bar{\phi}_{z,t}\mathrm{Tr}\left(\mathcal{M}\otimes\mathcal{M}(|x\rangle\langle z|\otimes|t\rangle\langle y|)\mathbb{F}\right)\right| \\
&= \left|\sum_{x,y,z,t} \phi_{x,y}\bar{\phi}_{z,t}\mathrm{Tr}\left(\mathcal{M}(|x\rangle\langle z|)\otimes\mathcal{M}(|t\rangle\langle y|)\mathbb{F}\right)\right| \\
&= \left|\sum_{x,y,z,t} \phi_{x,y}\bar{\phi}_{z,t}\mathrm{Tr}\left(\mathcal{M}(|x\rangle\langle z|)\mathcal{M}(|t\rangle\langle y|)\right)\right| \\
&\le \sqrt{\sum_{x,y,z,t} |\phi_{x,y}\bar{\phi}_{z,t}|^2 \sum_{x,y,z,t} |\mathrm{Tr}\left(\mathcal{M}(|x\rangle\langle z|)\mathcal{M}(|t\rangle\langle y|)\right)|^2} \\
&= \sqrt{\sum_{x,y,z,t} \|\mathcal{M}(|x\rangle\langle z|)\|_2^2 \|\mathcal{M}(|t\rangle\langle y|)\|_2^2} = \eta^2
\end{aligned}$$

其中我们使用了柯西-施瓦茨不等式和引理 C.4。另一方面，我们可以计算:

$$\begin{aligned}
\mathrm{Tr}(\mathcal{M}\otimes\mathcal{M}\circ \mathrm{T}_2(|\Psi\rangle\langle\Psi|)\mathbb{F}) &= \frac{1}{d_{\mathrm{in}}}\sum_{i,j}\mathrm{Tr}(\mathcal{M}\otimes\mathcal{M}\circ \mathrm{T}_2(|ii\rangle\langle jj|)\mathbb{F}) \\
&= \frac{1}{d_{\mathrm{in}}}\sum_{i,j}\mathrm{Tr}(\mathcal{M}(|i\rangle\langle j|)\mathcal{M}(|j\rangle\langle i|)) = \frac{\eta^2}{d_{\mathrm{in}}}.
\end{aligned}$$

接着，我们可以对厄米矩阵 $M^\dagger M - \frac{d_{\mathrm{in}}}{d_{\mathrm{out}}}|\Psi\rangle\langle\Psi| = \sum_i \mu_i |\psi_i\rangle\langle\psi_i|$ 进行分解。因此，由引理 C.6 可得:

$$\begin{aligned}
&\sum_{k,l}\mathrm{Tr}(\mathcal{M}(A_l^\dagger A_k)\mathcal{M}(A_k^\dagger A_l)) = \mathrm{Tr}\left(\mathcal{M}\otimes\mathcal{M}\circ \mathrm{T}_2(M^\dagger M)\mathbb{F}\right) \\
&= \frac{d_{\mathrm{in}}}{d_{\mathrm{out}}}\mathrm{Tr}\left(\mathcal{M}\otimes\mathcal{M}\circ \mathrm{T}_2(|\Psi\rangle\langle\Psi|)\mathbb{F}\right) + \sum_i \mu_i \mathrm{Tr}\left(\mathcal{M}\otimes\mathcal{M}\circ \mathrm{T}_2(|\psi_i\rangle\langle\psi_i|)\mathbb{F}\right) \\
&\le \frac{\eta^2}{d_{\mathrm{out}}} + \sum_i |\mu_i|\eta^2 = \frac{\eta^2}{d_{\mathrm{out}}} + \mathrm{Tr}\left|M^\dagger M - \frac{d_{\mathrm{in}}}{d_{\mathrm{out}}}|\Psi\rangle\langle\Psi|\right|\eta^2 \le \frac{\eta^2}{d_{\mathrm{out}}} + 5\eta^4.
\end{aligned}$$

最后,

$$F((142)) = \sum_{k,l}\mathrm{Tr}(\mathcal{M}(A_l^\dagger A_k)\mathcal{M}(A_k^\dagger A_l)) + \frac{\frac{d_{\mathrm{in}}}{d_{\mathrm{out}}}+\eta^2}{d_{\mathrm{out}}} \le \frac{\frac{d_{\mathrm{in}}}{d_{\mathrm{out}}}+\eta^2}{d_{\mathrm{out}}} + \frac{\eta^2}{d_{\mathrm{out}}} + 5\eta^4.$$

□

引理 C.8. 我们可以将 $F(\mathrm{id})$ $F((132))$ $F((314))$ 和 $F((24)(13))$ 的上界估计如下:

$$F(\mathrm{id}) = F((132)) = F((314)) = F((24)(13)) \le \frac{d_{\mathrm{in}}/d_{\mathrm{out}}+\eta^2}{d_{\mathrm{out}}} + \frac{\eta^2}{d_{\mathrm{out}}} + 5\eta^4.$$

证明. 对于恒等置换，函数 F 可表示如下：

$$
\begin{aligned}
F(\mathrm{id}) &= \sum_{k,l,k',l'} \mathrm{Tr}(A_k A_{l'}^\dagger A_{k'} A_l^\dagger)\mathrm{Tr}(A_{k'}^\dagger A_{l'})\mathrm{Tr}(A_k^\dagger A_l) \\
&= \sum_{k,l,k',l'} \sum_{i,j} \mathrm{Tr}(|j\rangle\langle i| A_{l'}^\dagger A_{k'} A_l^\dagger A_k |i\rangle\langle j| A_k^\dagger A_l)\mathrm{Tr}(A_{k'}^\dagger A_{l'}) \\
&= \sum_{k',l'}\sum_{i,j} \mathrm{Tr}(\mathcal{N}(|j\rangle\langle i| A_{l'}^\dagger A_{k'})\mathcal{N}(|i\rangle\langle j|))\mathrm{Tr}(A_{k'}^\dagger A_{l'}) \\
&= \sum_{k',l'}\sum_{i,j} \mathrm{Tr}(\mathcal{N}(|j\rangle\langle i| A_{l'}^\dagger A_{k'})\mathcal{M}(|i\rangle\langle j|))\mathrm{Tr}(A_{k'}^\dagger A_{l'}) + \sum_{k',l'}\sum_{i,j} \mathrm{Tr}(\mathcal{N}(|j\rangle\langle i| A_{l'}^\dagger A_{k'})\mathcal{D}(|i\rangle\langle j|))\mathrm{Tr}(A_{k'}^\dagger A_{l'}) \\
&= \sum_{k',l'}\sum_{i,j} \mathrm{Tr}(\mathcal{N}(|j\rangle\langle i| A_{l'}^\dagger A_{k'})\mathcal{M}(|i\rangle\langle j|))\mathrm{Tr}(A_{k'}^\dagger A_{l'}) + \sum_{k',l'}\sum_{i} \frac{1}{d_{\mathrm{out}}}\mathrm{Tr}(\mathcal{N}(|i\rangle\langle i| A_{l'}^\dagger A_{k'}))\mathrm{Tr}(A_{k'}^\dagger A_{l'}) \\
&= \sum_{k',l'}\sum_{i,j} \mathrm{Tr}(\mathcal{N}(|j\rangle\langle i| A_{l'}^\dagger A_{k'})\mathcal{M}(|i\rangle\langle j|))\mathrm{Tr}(A_{k'}^\dagger A_{l'}) + \sum_{k',l'} \frac{1}{d_{\mathrm{out}}}\mathrm{Tr}(A_{l'}^\dagger A_{k'})\mathrm{Tr}(A_{k'}^\dagger A_{l'}) \\
&= \sum_{k',l'}\sum_{i,j} \mathrm{Tr}(\mathcal{M}(|j\rangle\langle i| A_{l'}^\dagger A_{k'})\mathcal{M}(|i\rangle\langle j|))\mathrm{Tr}(A_{k'}^\dagger A_{l'}) + \frac{d_{\mathrm{in}}/d_{\mathrm{out}}+\eta^2}{d_{\mathrm{out}}} \text{ (because } \mathcal{M} \text{ is a trace less channel)} \\
&= \sum_{i,j} \mathrm{Tr}(\mathcal{M}(|j\rangle\langle i| N)\mathcal{M}(|i\rangle\langle j|)) + \frac{d_{\mathrm{in}}/d_{\mathrm{out}}+\eta^2}{d_{\mathrm{out}}}
\end{aligned}
$$

其中 $N = \sum_{k,\ l}$迹$(A_k^\dagger A_l)A_l^\dagger A_k$。引入 $\tilde{N} = N - \frac{\mathbb{I}}{d_{\mathrm{out}}} = \sum_i \mu_x |\psi_x\rangle\langle\psi_x|$（这是可行的，因为 N 是厄米的），于是我们可以利用引理 C.4 写成：

$$
\begin{aligned}
\sum_{i,j} \mathrm{Tr}(\mathcal{M}(|j\rangle\langle i| N)\mathcal{M}(|i\rangle\langle j|)) &= \sum_{i,j} \mathrm{Tr}(\mathcal{M}(|j\rangle\langle i| \tilde{N})\mathcal{M}(|i\rangle\langle j|)) + \frac{1}{d_{\mathrm{out}}}\sum_{i,j} \mathrm{Tr}(\mathcal{M}(|j\rangle\langle i|)\mathcal{M}(|i\rangle\langle j|)) \\
&= \sum_{i,j,x} \mu_x \mathrm{Tr}(\mathcal{M}(|j\rangle\langle i| |\psi_x\rangle\langle\psi_x|)\mathcal{M}(|i\rangle\langle j|)) + \frac{\eta^2}{d_{\mathrm{out}}} \\
&= \sum_{i,j,x} \mu_x \langle i|\psi_x\rangle \mathrm{Tr}(\mathcal{M}(|j\rangle\langle\psi_x|)\mathcal{M}(|i\rangle\langle j|)) + \frac{\eta^2}{d_{\mathrm{out}}} \\
&= \sum_{i,j,x,k} \mu_x \mathrm{Tr}(\langle i|\psi_x\rangle \mathcal{M}(|j\rangle\langle k|)\langle\psi_x|k\rangle \mathcal{M}(|i\rangle\langle j|)) + \frac{\eta^2}{d_{\mathrm{out}}} \\
&\le \frac{1}{2}\sum_{i,j,x,k} |\mu_x|(\|\langle i|\psi_x\rangle \mathcal{M}(|j\rangle\langle k|)\|_2^2 + \|\langle\psi_x|k\rangle \mathcal{M}(|i\rangle\langle j|)\|_2^2) + \frac{\eta^2}{d_{\mathrm{out}}} \\
&= \mathrm{Tr}|\tilde{N}|\eta^2 + \frac{\eta^2}{d_{\mathrm{out}}}.
\end{aligned}
$$

我们可以将矩阵 $N = \sum_{k,\ l}$Tr$(A_k^\dagger A_l)A_l^\dagger A_k$看作 $M^\dagger M$ 的偏迹：

$$
\begin{aligned}
\mathrm{Tr}_2(M^\dagger M) &= \mathrm{Tr}_2\left(\sum_{k,l} A_l^\dagger A_k \otimes A_l^\top \bar{A}_k\right) = \sum_{k,l} \mathrm{Tr}(A_l^\top \bar{A}_k) A_l^\dagger A_k \\
&= \sum_{k,l} \mathrm{Tr}(A_l A_k^*) A_l^\dagger A_k = N.
\end{aligned}
$$

此外，$\frac{\mathbb{I}}{d_{\text{in}}} = \text{Tr}_2(|\Psi\rangle\langle\Psi|)$，因此根据数据处理不等式（偏迹是有效量子信道）和引理 C.6，我们推得：

$$\text{Tr}|\tilde{N}| = \left\|\text{Tr}_2(M^\dagger M) - \frac{d_{\text{in}}}{d_{\text{out}}}\text{Tr}_2(|\Psi\rangle\langle\Psi|)\right\|_1 \leq \left\|M^\dagger M - \frac{d_{\text{in}}}{d_{\text{out}}}|\Psi\rangle\langle\Psi|\right\|_1 \leq 5\eta^2.$$

最后，

$$F(\text{id}) = \sum_{i,j}\text{Tr}(\mathcal{M}(|j\rangle\langle i|N)\mathcal{M}(|i\rangle\langle j|)) + \frac{d_{\text{in}}/d_{\text{out}} + \eta^2}{d_{\text{out}}} \leq \frac{d_{\text{in}}/d_{\text{out}} + \eta^2}{d_{\text{out}}} + \frac{\eta^2}{d_{\text{out}}} + 5\eta^4.$$

□

引理 C.9. 我们可以对 $F((24))$ 和 $F((1432))$ 给出如下上界：

$$F((24)) = F((1432)) \leq \frac{d_{\text{in}}^2}{d_{\text{out}}^2} + \frac{2m^2}{d_{\text{out}}} + 25\eta^4.$$

证明. 回忆一下，$\langle\Psi|M^\dagger M|\Psi\rangle = \text{Tr}(\mathcal{N}(\frac{\mathbb{I}}{d_{\text{in}}}) = \frac{d_{\text{in}}}{d_{\text{out}}} + \frac{m^2}{d_{\text{in}}})^2)$。我们利用如下事实：$\text{Tr}(X)\text{Tr}(Y) = \text{Tr}(X\otimes Y)$：

$$\begin{aligned}
F((24)) &= \sum_{k,l,k',l'}\text{Tr}(A_k^\dagger A_l A_{k'}^\dagger A_{l'})\text{Tr}(A_k A_{l'}^\dagger A_{k'} A_l^\dagger) \\
&= \sum_{k,l,k',l'}\text{Tr}(A_k^\dagger A_l A_{k'}^\dagger A_{l'} \otimes A_l^\dagger A_k A_{l'}^\dagger A_{k'}) \\
&= \text{Tr}\left(\sum_{k,l}A_k^\dagger A_l \otimes A_l^\dagger A_k\right)\left(\sum_{k,l}A_k^\dagger A_l \otimes A_l^\dagger A_k\right) \\
&= \text{Tr}\left(\sum_{k,l}A_k^\dagger A_l \otimes A_k^\top \bar{A}_l\right)^{\text{T}_2}\left(\sum_{k,l}A_k^\dagger A_l \otimes A_k^\top \bar{A}_l\right)^{\text{T}_2} \\
&= \text{Tr}(M^\dagger M)^{\text{T}_2}(M^\dagger M)^{\text{T}_2} = \text{Tr}(M^\dagger M)(M^\dagger M) \\
&= \text{Tr}\left(M^\dagger M - \frac{d_{\text{in}}}{d_{\text{out}}}|\Psi\rangle\langle\Psi|\right)M^\dagger M + \frac{d_{\text{in}}}{d_{\text{out}}}\text{Tr}(|\Psi\rangle\langle\Psi|M^\dagger M) \\
&= \text{Tr}\left(M^\dagger M - \frac{d_{\text{in}}}{d_{\text{out}}}|\Psi\rangle\langle\Psi|\right)\left(M^\dagger M - \frac{d_{\text{in}}}{d_{\text{out}}}|\Psi\rangle\langle\Psi|\right) \\
&+ \frac{d_{\text{in}}}{d_{\text{out}}}\langle\Psi|\left(M^\dagger M - \frac{d_{\text{in}}}{d_{\text{out}}}|\Psi\rangle\langle\Psi|\right)|\Psi\rangle + \frac{d_{\text{in}}^2}{d_{\text{out}}^2} + \frac{m^2}{d_{\text{out}}} \\
&\leq \left(\text{Tr}\left|M^\dagger M - \frac{d_{\text{in}}}{d_{\text{out}}}|\Psi\rangle\langle\Psi|\right|\right)^2 + \frac{d_{\text{in}}^2}{d_{\text{out}}^2} + \frac{2m^2}{d_{\text{out}}} \\
&\leq \frac{d_{\text{in}}^2}{d_{\text{out}}^2} + \frac{2m^2}{d_{\text{out}}} + 25\eta^4
\end{aligned}$$

其中我们用到了 $\text{Tr}\left(A^{\text{T}_2}B^{\text{T}_2}\right) = \text{Tr}(AB)$ 这一事实以及引理 C.6。

□

引理 C.10. 我们可以如下给出 $F((12)(34))$ $F((14)(23))$ $F((234))$ 和 $F((124))$ 的上界：

$$F((12)(34)) = F((14)(23)) = F((234)) = F((124)) \leq \frac{d_{\text{in}}^3}{d_{\text{out}}^2} + 2\frac{d_{\text{in}}}{d_{\text{out}}}m^2 + \eta^2 m^2.$$

证明。利用排列 $\alpha = (12)(34)$ 对应的 $F(\alpha)$ 表达式以及事实 $\sum_k A_k^\dagger A_k = \mathbb{I}$，我们有：

$$
\begin{aligned}
F((12)(34)) &= \sum_{k,l,k',l'} \mathrm{Tr}(A_k A_k^\dagger A_l A_{l'}^\dagger A_{k'} A_{k'}^\dagger A_{l'} A_l^\dagger) = \sum_{k,l} \mathrm{Tr}(A_l^\dagger \mathcal{N}(\mathbb{I}) A_l A_k^\dagger \mathcal{N}(\mathbb{I}) A_k) \\
&= \sum_{k,l} \mathrm{Tr}(A_l^\dagger \mathcal{M}(\mathbb{I}) A_l A_k^\dagger \mathcal{N}(\mathbb{I}) A_k) + \frac{d_{\mathrm{in}}}{d_{\mathrm{out}}} \sum_{k,l} \mathrm{Tr}(A_l^\dagger A_l A_k^\dagger \mathcal{N}(\mathbb{I}) A_k) \\
&= \sum_{k,l} \mathrm{Tr}(A_l^\dagger \mathcal{M}(\mathbb{I}) A_l A_k^\dagger \mathcal{M}(\mathbb{I}) A_k) + \frac{d_{\mathrm{in}}}{d_{\mathrm{out}}} \sum_{k,l} \mathrm{Tr}(A_l^\dagger \mathcal{M}(\mathbb{I}) A_l A_k^\dagger A_k) + \frac{d_{\mathrm{in}}}{d_{\mathrm{out}}} \sum_{k} \mathrm{Tr}(A_k^\dagger \mathcal{N}(\mathbb{I}) A_k) \\
&= \sum_{k,l} \mathrm{Tr}(A_l^\dagger \mathcal{M}(\mathbb{I}) A_l A_k^\dagger \mathcal{M}(\mathbb{I}) A_k) + \frac{d_{\mathrm{in}}}{d_{\mathrm{out}}} \mathrm{Tr}(\mathcal{M}(\mathbb{I}) \mathcal{N}(\mathbb{I})) + \frac{d_{\mathrm{in}}}{d_{\mathrm{out}}} \mathrm{Tr}(\mathcal{N}(\mathbb{I})^2) \\
&= \sum_{k,l} \mathrm{Tr}(A_l^\dagger \mathcal{M}(\mathbb{I}) A_l A_k^\dagger \mathcal{M}(\mathbb{I}) A_k) + \frac{d_{\mathrm{in}}^3}{d_{\mathrm{out}}^2} + 2\frac{d_{\mathrm{in}}}{d_{\mathrm{out}}} \mathrm{Tr}(\mathcal{M}(\mathbb{I})^2)
\end{aligned}
$$

接下来，若我们关注第一项，

我们可以再次使用复制技巧，得到：

$$
\begin{aligned}
&\sum_{k,l} \mathrm{Tr}(A_l^\dagger \mathcal{M}(\mathbb{I}) A_l A_k^\dagger \mathcal{M}(\mathbb{I}) A_k) = \sum_{k,l} \mathrm{Tr}(A_k A_l^\dagger \mathcal{M}(\mathbb{I}) \otimes A_l A_k^\dagger \mathcal{M}(\mathbb{I}) \mathbb{F}) \\
&= \mathrm{Tr}\left(\sum_{k,l} A_k A_l^\dagger \otimes A_l A_k^\dagger \cdot \mathcal{M}(\mathbb{I})^{\otimes 2} \mathbb{F} \right) = \mathrm{Tr}\left(\mathrm{T}_2 \left(\sum_{k,l} A_k A_l^\dagger \otimes \bar{A}_k A_l^\top \right) \cdot \mathcal{M}(\mathbb{I})^{\otimes 2} \mathbb{F} \right) \\
&= \mathrm{Tr}\left(\left(M M^\dagger \right)^{T_2} \cdot \mathcal{M}(\mathbb{I})^{\otimes 2} \mathbb{F} \right) \\
&= \mathrm{Tr}\left(\left((\mathbb{I} - |\Psi\rangle\langle\Psi|) M M^\dagger (\mathbb{I} - |\Psi\rangle\langle\Psi|) \right)^{T_2} \cdot \mathcal{M}(\mathbb{I})^{\otimes 2} \mathbb{F} \right) + \mathrm{Tr}\left(\left(M M^\dagger |\Psi\rangle\langle\Psi| \right)^{T_2} \cdot \mathcal{M}(\mathbb{I})^{\otimes 2} \mathbb{F} \right) \\
&+ \mathrm{Tr}\left(\left(|\Psi\rangle\langle\Psi| M M^\dagger \right)^{T_2} \cdot \mathcal{M}(\mathbb{I})^{\otimes 2} \mathbb{F} \right) - \mathrm{Tr}\left(\left(|\Psi\rangle\langle\Psi| M M^\dagger |\Psi\rangle\langle\Psi| \right)^{T_2} \cdot \mathcal{M}(\mathbb{I})^{\otimes 2} \mathbb{F} \right).
\end{aligned}
$$

我们可以简化后面的各项。首先有 $|\Psi\rangle\langle\Psi|^{T_2} = \mathrm{F}$ 和 $\mathrm{F}^2 = \mathbb{I}$，因此

$$
\begin{aligned}
&\mathrm{Tr}\left(\left(|\Psi\rangle\langle\Psi| M M^\dagger |\Psi\rangle\langle\Psi| \right)^{T_2} \cdot \mathcal{M}(\mathbb{I})^{\otimes 2} \mathbb{F} \right) = \langle\Psi| M M^\dagger |\Psi\rangle \, \mathrm{Tr}\left((|\Psi\rangle\langle\Psi|)^{T_2} \cdot \mathcal{M}(\mathbb{I})^{\otimes 2} \mathbb{F} \right) \\
&= \langle\Psi| M M^\dagger |\Psi\rangle \, \mathrm{Tr}\left(\mathbb{F} \mathcal{M}(\mathbb{I})^{\otimes 2} \mathbb{F} \right) = \langle\Psi| M M^\dagger |\Psi\rangle \, \mathrm{Tr}\left(\mathcal{M}(\mathbb{I})^{\otimes 2} \right) = \langle\Psi| M M^\dagger |\Psi\rangle \, \mathrm{Tr}\left(\mathcal{M}(\mathbb{I}) \right)^2 = 0.
\end{aligned}
$$

接下来，根据引理 C.5，我们有 $M M^\dagger |\Psi\rangle = \frac{1}{\sqrt{d_{\mathrm{in}}}} \sum_{x,y} \langle x| \mathcal{N}(\mathbb{I}) \, |y\rangle \, |xy\rangle$ 因此

$$
\begin{aligned}
\mathrm{Tr}\left(\left(M M^\dagger |\Psi\rangle\langle\Psi| \right)^{T_2} \cdot \mathcal{M}(\mathbb{I})^{\otimes 2} \mathbb{F} \right) &= \frac{1}{d_{\mathrm{in}}} \sum_{x,y,z} \langle x| \mathcal{N}(\mathbb{I}) |y\rangle \, \mathrm{Tr}\left((|xy\rangle \langle zz|)^{T_2} \cdot \mathcal{M}(\mathbb{I})^{\otimes 2} \mathbb{F} \right) \\
&= \frac{1}{d_{\mathrm{in}}} \sum_{x,y,z} \langle x| \mathcal{N}(\mathbb{I}) |y\rangle \, \mathrm{Tr}\left(|x\rangle \langle z| \otimes |z\rangle \langle y| \cdot \mathcal{M}(\mathbb{I})^{\otimes 2} \mathbb{F} \right) \\
&= \frac{1}{d_{\mathrm{in}}} \sum_{x,y,z} \langle x| \mathcal{N}(\mathbb{I}) |y\rangle \, \mathrm{Tr}\left(|x\rangle \langle z| \, \mathcal{M}(\mathbb{I}) \, |z\rangle \langle y| \, \mathcal{M}(\mathbb{I}) \right) \\
&= \frac{1}{d_{\mathrm{in}}} \sum_{x,y} \langle x| \mathcal{N}(\mathbb{I}) |y\rangle \, \mathrm{Tr}\left(|x\rangle \, \mathrm{Tr}(\mathcal{M}(\mathbb{I})) \langle y| \, \mathcal{M}(\mathbb{I}) \right) = 0.
\end{aligned}
$$

类似地，我们可以证明：

$$\begin{aligned}
\mathrm{Tr}\left(\left(|\Psi\rangle\langle\Psi| MM^\dagger\right)^{T_2}\cdot\mathcal{M}(\mathbb{I})^{\otimes 2}\mathbb{F}\right) &= \frac{1}{d_{\text{in}}}\sum_{x,y,z}\langle x|\mathcal{N}(\mathbb{I})|y\rangle\,\mathrm{Tr}\left(\left(|zz\rangle\langle xy|\right)^{T_2}\cdot\mathcal{M}(\mathbb{I})^{\otimes 2}\mathbb{F}\right)\\
&= \frac{1}{d_{\text{in}}}\sum_{x,y,z}\langle x|\mathcal{N}(\mathbb{I})|y\rangle\,\mathrm{Tr}\left(|z\rangle\langle x|\otimes|y\rangle\langle z|\cdot\mathcal{M}(\mathbb{I})^{\otimes 2}\mathbb{F}\right)\\
&= \frac{1}{d_{\text{in}}}\sum_{x,y,z}\langle x|\mathcal{N}(\mathbb{I})|y\rangle\,\mathrm{Tr}\left(|z\rangle\langle x|\mathcal{M}(\mathbb{I})|y\rangle\langle z|\mathcal{M}(\mathbb{I})\right)\\
&= \frac{1}{d_{\text{in}}}\sum_{x,y}\langle x|\mathcal{N}(\mathbb{I})|y\rangle\langle y|\mathcal{M}(\mathbb{I})|x\rangle\,\mathrm{Tr}(\mathcal{M}(\mathbb{I}))=0.
\end{aligned}$$

现在，矩阵 $(\mathbb{I}-|\Psi\rangle\langle\Psi|)MM^\dagger(\mathbb{I}-|\Psi\rangle\langle\Psi|)$ 是厄米且半正定的，因此可写为 $(\mathbb{I}-|\Psi\rangle\langle\Psi|)MM^\dagger(\mathbb{I}-|\Psi\rangle\langle\Psi|)$ $=\sum_i\lambda_i|\phi_i\rangle\langle\phi_i|$。对于每个 i，我们可以写出 $|\phi\rangle=\sum_{x,\ y}\phi_{x,\ y}|xy\rangle$ 的施密特分解。因此

$$\begin{aligned}
&\sum_{k,l}\mathrm{Tr}(A_l^\dagger\mathcal{M}(\mathbb{I})A_lA_k^\dagger\mathcal{M}(\mathbb{I})A_k)=\mathrm{Tr}\left(\left((\mathbb{I}-|\Psi\rangle\langle\Psi|)MM^\dagger(\mathbb{I}-|\Psi\rangle\langle\Psi|)\right)^{T_2}\cdot\mathcal{M}(\mathbb{I})^{\otimes 2}\mathbb{F}\right)\\
&=\sum_i\lambda_i\mathrm{Tr}\left(\mathrm{T}_2\left(|\phi_i\rangle\langle\phi_i|\right)\cdot\mathcal{M}(\mathbb{I})^{\otimes 2}\mathbb{F}\right)=\sum_i\sum_{x,y,z,t}\lambda_i\phi_{x,y}\bar{\phi}_{z,t}\mathrm{Tr}\left(\mathrm{T}_2\left(|xy\rangle\langle zt|\right)\cdot\mathcal{M}(\mathbb{I})^{\otimes 2}\mathbb{F}\right)\\
&=\sum_i\sum_{x,y,z,t}\lambda_i\phi_{x,y}\bar{\phi}_{z,t}\mathrm{Tr}\left(|x\rangle\langle z|\otimes|t\rangle\langle y|\cdot\mathcal{M}(\mathbb{I})^{\otimes 2}\mathbb{F}\right)\\
&=\sum_i\sum_{x,y,z,t}\lambda_i\phi_{x,y}\bar{\phi}_{z,t}\mathrm{Tr}\left(|x\rangle\langle z|\mathcal{M}(\mathbb{I})\otimes|t\rangle\langle y|\mathcal{M}(\mathbb{I})\mathbb{F}\right)\\
&=\sum_i\sum_{x,y,z,t}\lambda_i\phi_{x,y}\bar{\phi}_{z,t}\mathrm{Tr}\left(|x\rangle\langle z|\mathcal{M}(\mathbb{I})|t\rangle\langle y|\mathcal{M}(\mathbb{I})\right)\\
&=\sum_i\sum_{x,y,z,t}\lambda_i\phi_{x,y}\bar{\phi}_{z,t}\langle z|\mathcal{M}(\mathbb{I})|t\rangle\langle y|\mathcal{M}(\mathbb{I})|x\rangle\\
&\le\sum_i\sum_{x,y,z,t}\lambda_i|\phi_{x,y}|^2|\langle z|\mathcal{M}(\mathbb{I})|t\rangle|^2+\sum_i\sum_{x,y,z,t}\lambda_i|\phi_{z,t}|^2|\langle y|\mathcal{M}(\mathbb{I})|x\rangle|^2\\
&\le\sum_i\sum_{x,y,z,t}\lambda_i|\phi_{x,y}|^2|\langle z|\mathcal{M}(\mathbb{I})|t\rangle|^2+\sum_i\sum_{x,y,z,t}\lambda_i|\phi_{z,t}|^2|\langle y|\mathcal{M}(\mathbb{I})|x\rangle|^2\\
&=\mathrm{Tr}\left|(\mathbb{I}-|\Psi\rangle\langle\Psi|)MM^\dagger(\mathbb{I}-|\Psi\rangle\langle\Psi|)\right|\mathrm{Tr}(\mathcal{M}(\mathbb{I})^2)
\end{aligned}$$

由引理 C.5 可得 $\langle\Psi|MM^\dagger|\Psi\rangle=\frac{d_{\text{in}}}{d_{\text{out}}}$ 且 $\mathrm{Tr}(MM^\dagger)=\frac{d_{\text{in}}}{d_{\text{out}}}+\eta^2$，因此我们有：

$$\mathrm{Tr}\left|(\mathbb{I}-|\Psi\rangle\langle\Psi|)MM^\dagger(\mathbb{I}-|\Psi\rangle\langle\Psi|)\right|=\mathrm{Tr}(\mathbb{I}-|\Psi\rangle\langle\Psi|)MM^\dagger(\mathbb{I}-|\Psi\rangle\langle\Psi|)=\eta^2.$$

最后

$$F((12)(34))\le\frac{d_{\text{in}}^3}{d_{\text{out}}^2}+2\frac{d_{\text{in}}}{d_{\text{out}}}m^2+\eta^2m^2.$$

至此，$F((12)(34))$ 的证明完成。 □

引理 C.11。我们可以如下给出 $F((14))$ $F((12))$ $F((23))$ 和 $F((34))$ 的上界：

$$F((14)) = F((12)) = F((23)) = F((34)) \leq \frac{d_{\text{in}}^2}{d_{\text{out}}^2} + \frac{d_{\text{in}}}{d_{\text{out}}}\eta^2 + \frac{m^2}{d_{\text{out}}} + 5m\eta^3.$$

证明。回顾记号 $N = \sum_{k,\ l} \mathrm{Tr}(A_k A_l^\dagger) A_k^\dagger A_l$。我们可以写出厄米矩阵的谱分解：

$$N - \frac{\mathbb{I}}{d_{\text{out}}} = \mathrm{Tr}_2\left(\sum_{k,l} A_l^\dagger A_k \otimes A_l^\top \bar{A}_k - \frac{d_{\text{in}}}{d_{\text{out}}} |\Psi\rangle\langle\Psi|\right) = \sum_i \lambda_i |\phi_i\rangle\langle\phi_i| .$$

然后利用三角不等式以及以下事实： $\sum_k A_k^\dagger A_k = \mathbb{I}$

$$\begin{aligned}
F(14) &= \sum_{k,l,k',l'} \mathrm{Tr}(A_k^\dagger A_l)\mathrm{Tr}(A_l^\dagger A_k A_{k'}^\dagger A_{l'} A_{l'}^\dagger A_{k'}) = \sum_{k'} \mathrm{Tr}(N A_{k'}^\dagger \mathcal{N}(\mathbb{I}) A_{k'}) \\
&= \sum_{k'} \mathrm{Tr}(N A_{k'}^\dagger \mathcal{M}(\mathbb{I}) A_{k'}) + \frac{d_{\text{in}}}{d_{\text{out}}}\mathrm{Tr}(N) = \mathrm{Tr}(\mathcal{N}(N)\mathcal{M}(\mathbb{I})) + \frac{d_{\text{in}}}{d_{\text{out}}}\mathrm{Tr}(N) \\
&= \mathrm{Tr}(\mathcal{M}(N)\mathcal{M}(\mathbb{I})) + \frac{d_{\text{in}}}{d_{\text{out}}}\mathrm{Tr}(N) = \mathrm{Tr}\left(\mathcal{M}\left(N - \frac{\mathbb{I}}{d_{\text{out}}}\right)\mathcal{M}(\mathbb{I})\right) + \frac{\mathrm{Tr}(\mathcal{M}(\mathbb{I})^2)}{d_{\text{out}}} + \frac{d_{\text{in}}}{d_{\text{out}}}\mathrm{Tr}(N) \\
&= \frac{d_{\text{in}}}{d_{\text{out}}}\left(\frac{d_{\text{in}}}{d_{\text{out}}} + \eta^2\right) + \frac{\mathrm{Tr}(\mathcal{M}(\mathbb{I})^2)}{d_{\text{out}}} + \sum_i \lambda_i \mathrm{Tr}(\mathcal{M}(|\phi_i\rangle\langle\phi_i|)\mathcal{M}(\mathbb{I})) \\
&\leq \frac{d_{\text{in}}}{d_{\text{out}}}\left(\frac{d_{\text{in}}}{d_{\text{out}}} + \eta^2\right) + \frac{\mathrm{Tr}(\mathcal{M}(\mathbb{I})^2)}{d_{\text{out}}} + \sum_i |\lambda_i| \|\mathcal{M}(|\phi_i\rangle\langle\phi_i|)\|_2 \|\mathcal{M}(\mathbb{I})\|_2 \\
&\leq \frac{d_{\text{in}}}{d_{\text{out}}}\left(\frac{d_{\text{in}}}{d_{\text{out}}} + \eta^2\right) + \frac{m^2}{d_{\text{out}}} + m\eta \sum_i |\lambda_i| = \frac{d_{\text{in}}}{d_{\text{out}}}\left(\frac{d_{\text{in}}}{d_{\text{out}}} + \eta^2\right) + \frac{m^2}{d_{\text{out}}} + m\eta \cdot \mathrm{Tr}\left|N - \frac{\mathbb{I}}{d_{\text{out}}}\right|
\end{aligned}$$

因为对于所有单位向量 $|\phi\rangle = \sum_i \phi_i |i\rangle$，利用柯西-施瓦茨不等式、算术-几何平均不等式和引理 C.4，我们有：

$$\begin{aligned}
\|\mathcal{M}(|\phi\rangle\langle\phi|)\|_2^2 &= \sum_{i,j,k,l} \phi_i \bar{\phi}_j \phi_k \bar{\phi}_l \mathrm{Tr}\left(\mathcal{M}(|i\rangle\langle j|)\mathcal{M}(|k\rangle\langle l|)\right) \leq \sum_{i,j,k,l} |\phi_i \bar{\phi}_j \phi_k \bar{\phi}_l| \|\mathcal{M}(|i\rangle\langle j|)\|_2 \|\mathcal{M}(|k\rangle\langle l|)\|_2 \\
&\leq \frac{1}{2}\sum_{i,j,k,l} |\phi_i|^2 |\phi_j|^2 \|\mathcal{M}(|k\rangle\langle l|)\|_2^2 + \frac{1}{2}\sum_{i,j,k,l} |\phi_k|^2 |\phi_l|^2 \|\mathcal{M}(|i\rangle\langle j|)\|_2^2 = \eta^2.
\end{aligned}$$

此外，利用数据处理不等式和引理 C.6：

$$\begin{aligned}
\mathrm{Tr}\left|N - \frac{\mathbb{I}}{d_{\text{out}}}\right| &= \mathrm{Tr}\left|\mathrm{Tr}_2\left(\sum_{k,l} A_l^\dagger A_k \otimes A_l^\top \bar{A}_k - \frac{d_{\text{in}}}{d_{\text{out}}} |\Psi\rangle\langle\Psi|\right)\right| \\
&\leq \mathrm{Tr}\left|\sum_{k,l} A_l^\dagger A_k \otimes A_l^\top \bar{A}_k - \frac{d_{\text{in}}}{d_{\text{out}}} |\Psi\rangle\langle\Psi|\right| = \mathrm{Tr}\left|M^\dagger M - \frac{d_{\text{in}}}{d_{\text{out}}} |\Psi\rangle\langle\Psi|\right| \leq 5\eta^2.
\end{aligned}$$

证明至此结束。 □

对于其余排列，我们可以得到函数 F 的闭式。对于换位 (13)，函数 F 的像可表示如下：

$$\begin{aligned}F((13)) &= \sum_{i,j,k,l,k',l'} \mathrm{Tr}(A_{l'}^\dagger |j\rangle\langle i| A_k A_l^\dagger |i\rangle\langle j| A_{k'}) \mathrm{Tr}(A_k^\dagger A_l)\mathrm{Tr}(A_{k'}^\dagger A_{l'}) \\ &= \sum_{k,l,k',l'} \mathrm{Tr}(A_{k'}A_{l'}^\dagger)\mathrm{Tr}(A_k A_l^\dagger)\mathrm{Tr}(A_k^\dagger A_l)\mathrm{Tr}(A_{k'}^\dagger A_{l'}) \\ &= \left(\sum_{k,l} |\mathrm{Tr}(A_k A_l^\dagger)|^2\right)^2 = \left(\frac{d_{\mathrm{in}}}{d_{\mathrm{out}}} + \eta^2\right)^2.\end{aligned}$$

接下来，我们指出，排列 (312) 和 (134) 具有相同的像：

$$\begin{aligned}F((312)) = F((134)) &= \sum_{i,j,k,l,k',l'} \mathrm{Tr}(A_l^\dagger |i\rangle\langle j| A_{k'} A_{l'}^\dagger |j\rangle\langle i| A_k A_k^\dagger A_l)\mathrm{Tr}(A_{k'}^\dagger A_{l'}) \\ &= \sum_{k,l,k',l'} \mathrm{Tr}(A_{k'}A_{l'}^\dagger)\mathrm{Tr}(A_k A_k^\dagger A_l A_l^\dagger)\mathrm{Tr}(A_{k'}^\dagger A_{l'}) \\ &= \sum_{k,l} \mathrm{Tr}(A_k A_k^\dagger A_l A_l^\dagger) \sum_{k,l} |\mathrm{Tr}(A_k A_l^\dagger)|^2 \\ &= \mathrm{Tr}(\mathcal{N}(\mathbb{I})^2)\left(\frac{d_{\mathrm{in}}}{d_{\mathrm{out}}} + \eta^2\right) = \left(\frac{d_{\mathrm{in}}^2}{d_{\mathrm{out}}} + m^2\right)\left(\frac{d_{\mathrm{in}}}{d_{\mathrm{out}}} + \eta^2\right).\end{aligned}$$

接下来，循环 (1234) 的像也有一个闭式表达式：

$$\begin{aligned}F((1234)) &= \sum_{i,j,k,l,k',l'} \mathrm{Tr}(A_{l'}^\dagger |j\rangle\langle i| A_k A_k^\dagger A_l A_l^\dagger |i\rangle\langle j| A_{k'} A_{k'}^\dagger A_{l'}) \\ &= \sum_{k,l,k',l'} \mathrm{Tr}(A_k A_k^\dagger A_l A_l^\dagger)\mathrm{Tr}(A_{k'} A_{k'}^\dagger A_{l'} A_{l'}^\dagger) \\ &= (\mathrm{Tr}(\mathcal{N}(\mathbb{I})^2))^2 = \left(\frac{d_{\mathrm{in}}^2}{d_{\mathrm{out}}} + m^2\right)^2.\end{aligned}$$

总而言之，到目前为止我们已经证明：

引理 C.12. 设 $m = \|\mathcal{M}(\mathbb{I})\|_2 = \|\mathcal{N}(\mathbb{I}) - \mathcal{D}(\mathbb{I})\|_2$ 和 $\eta = d_{\mathrm{in}} \left\|\mathcal{J} - \frac{\mathbb{I}}{d_{\mathrm{in}} d_{\mathrm{out}}}\right\|_2$。我们有：

因此，利用不等式 $m^2 \le d\eta^2$，我们得到二阶矩的以下上界：

$$\begin{aligned}&\mathbb{E}\left(\left(\mathrm{Tr}(\mathcal{N}(|\phi\rangle\langle\phi|)^2)\right)^2\right) = \frac{1}{d_{\mathrm{in}}(d_{\mathrm{in}}+1)(d_{\mathrm{in}}+2)(d_{\mathrm{in}}+3)} \sum_{\alpha \in \mathfrak{S}_4} F(\alpha) \\ &\le \frac{d_{\mathrm{out}}^4 + 6d_{\mathrm{in}}^3 + 2d_{\mathrm{in}}^2 d_{\mathrm{out}} m^2 + 2d_{\mathrm{in}}^2 d_{\mathrm{out}}\eta^2 + 11 d_{\mathrm{in}}^2 + 10 d_{\mathrm{in}} d_{\mathrm{out}} m^2 + 10 d_{\mathrm{in}} d_{\mathrm{out}}\eta^2}{d_{\mathrm{out}}^2 d_{\mathrm{in}}(d_{\mathrm{in}}+1)(d_{\mathrm{in}}+2)(d_{\mathrm{in}}+3)} \\ &+ \frac{6d_{\mathrm{in}} + d_{\mathrm{out}}^2 m^4 + 2d_{\mathrm{out}}^2\eta^2 + 12 d_{\mathrm{out}} m^2 + 40 d_{\mathrm{out}}^2 m\eta^3 + 81 d_{\mathrm{out}}^2\eta^4 + 12 d_{\mathrm{out}}\eta^2}{d_{\mathrm{out}}^2 d_{\mathrm{in}}(d_{\mathrm{in}}+1)(d_{\mathrm{in}}+2)(d_{\mathrm{in}}+3)}\end{aligned}$$

回顾一下，对于随机变量 $X = \text{迹}\left(\mathcal{N}(|\phi\rangle\langle\phi|) - \frac{\mathbb{I}}{d_{\mathrm{out}}}\right)^2 = \text{迹}\left(\mathcal{N}(|\phi\rangle\langle\phi|)\right)^2 - \frac{1}{d_{\mathrm{out}}}$，我们有：

$$\mathbb{E}(X) = \frac{\left(\mathrm{Tr}\left(\mathcal{N}(\mathbb{I}) - \frac{d_{\mathrm{in}}}{d_{\mathrm{out}}}\mathbb{I}\right)^2 + d_{\mathrm{in}}^2 \left\|\mathcal{J} - \frac{\mathbb{I}}{d_{\mathrm{in}} d_{\mathrm{out}}}\right\|_2^2\right)}{d_{\mathrm{in}}(d_{\mathrm{in}}+1)} = \frac{1}{d_{\mathrm{in}}(d_{\mathrm{in}}+1)}\left(\mathrm{Tr}(\mathcal{M}(\mathbb{I})^2) + \eta^2\right) = \frac{m^2 + \eta^2}{d_{\mathrm{in}}(d_{\mathrm{in}}+1)}.$$

排列 α	$F(\alpha)$ 的上界	参考文献
(13)	$\left(\frac{d_{\text{in}}}{d_{\text{out}}}+\eta^2\right)^2$	
id, (132), (314), (24)(13)	$\frac{d_{\text{in}}/d_{\text{out}}+\eta^2}{d_{\text{out}}}+\frac{\eta^2}{d_{\text{out}}}+5\eta^4$	(引理 C.8)
(312), (134)	$\left(\frac{d_{\text{in}}^2}{d_{\text{out}}}+m^2\right)\left(\frac{d_{\text{in}}}{d_{\text{out}}}+\eta^2\right)$	
(1234)	$\left(\frac{d_{\text{in}}^2}{d_{\text{out}}}+m^2\right)^2$	
(24), (1432)	$\frac{d_{\text{in}}^2}{d_{\text{out}}^2}+\frac{2m^2}{d_{\text{out}}}+25\eta^4$	(引理 C.9)
(142), (243)	$\frac{d_{\text{in}}/d_{\text{out}}+\eta^2}{d_{\text{out}}}+\frac{\eta^2}{d_{\text{out}}}+5\eta^4$	(引理 C.7)
(14)、(12)、(23)、(34)、(1324)、(1423)，(1243)，(1342)	$\frac{d_{\text{in}}^2}{d_{\text{out}}^2}+\frac{d_{\text{in}}}{d_{\text{out}}}\eta^2+\frac{m^2}{d_{\text{out}}}+5m\eta^3$	(引理 C.11)
(12)(34)，(14)(23)，(234)，(124)	$\frac{d_{\text{in}}^3}{d_{\text{out}}^2}+2\frac{d_{\text{in}}}{d_{\text{out}}}m^2+m^2\eta^2$	(引理 C.10)

由于 $\text{Var}(X)=\text{Var}\left(X+\frac{1}{d_{\text{out}}}\right)$，它可以用以下上界表示:

$$
\begin{aligned}
&\text{Var}(X)=\mathbb{E}\left(\left(\text{Tr}(\mathcal{N}(|\phi\rangle\langle\phi|)^2)\right)^2\right)-\left(\mathbb{E}\left(\text{Tr}(\mathcal{N}(|\phi\rangle\langle\phi|)^2)\right)\right)^2\\
&\leq\frac{d_{\text{out}}^4+6d_{\text{in}}^3+2d_{\text{in}}^2d_{\text{out}}m^2+2d_{\text{in}}^2d_{\text{out}}\eta^2+11d_{\text{in}}^2+10d_{\text{in}}d_{\text{out}}m^2+10d_{\text{in}}d_{\text{out}}\eta^2}{d_{\text{out}}^2d_{\text{in}}(d_{\text{in}}+1)(d_{\text{in}}+2)(d_{\text{in}}+3)}\\
&+\frac{6d_{\text{in}}+d_{\text{out}}^2m^4+2d_{\text{out}}^2\eta^2+12d_{\text{out}}m^2+40d_{\text{out}}^2m\eta^3+81d_{\text{out}}^2\eta^4+12d_{\text{out}}\eta^2}{d_{\text{out}}^2d_{\text{in}}(d_{\text{in}}+1)(d_{\text{in}}+2)(d_{\text{in}}+3)}-\left(\frac{m^2+\eta^2}{d_{\text{in}}(d_{\text{in}}+1)}+\frac{1}{d_{\text{out}}}\right)^2\\
&\leq\left(\frac{80d_{\text{in}}^2\eta^4+10d_{\text{in}}^2m^2\eta^2+40d_{\text{in}}^2\eta^3m}{d_{\text{in}}^2(d_{\text{in}}+1)^2(d_{\text{in}}+2)(d_{\text{in}}+3)}\right).
\end{aligned}
$$

因此，利用不等式 $(m^2+\eta^2)^2\geq 4m^2\eta^2$ 和 $(m^2+\eta^2)^2\geq 2m\eta^3$（连续应用算术-几何平均不等式），方差的上界变为:

$$
\begin{aligned}
\frac{\text{Var}(X)}{\mathbb{E}(X)^2}&\leq\left(\frac{80d_{\text{in}}^2\eta^4+10d_{\text{in}}^2m^2\eta^2+40d_{\text{in}}^2\eta^3m}{(d_{\text{in}}+2)(d_{\text{in}}+3)(\eta^2+m^2)^2}\right)\\
&\leq 80\frac{d_{\text{in}}^2\eta^4}{d_{\text{in}}^2\eta^4}+10\frac{d_{\text{in}}^2m^2\eta^2}{4d_{\text{in}}^2m^2\eta^2}+40\frac{d_{\text{in}}^2\eta^3m}{2d_{\text{in}}^2m\eta^3}\leq 105.
\end{aligned}
$$

□

定理 C.13。存在一种非相干无辅助系统算法，其所需测量次数满足

$$N=\mathcal{O}\left(\frac{d_{\text{in}}^2d_{\text{out}}^{1.5}}{\varepsilon^2}\right)$$

*to d*以至少为 $2/3$ 的成功概率区分 $\mathcal{N}=\mathcal{D}$ or $d_\diamond(\mathcal{N},\mathcal{D})>\varepsilon$.

证明。复杂度。我们首先证明算法 2 使用 $\mathcal{O}(d_{\text{in}}^2d_{\text{out}}^{1.5}/\varepsilon^2)$ 次测量。注意，算法 3 需要 $\mathcal{O}(\sqrt{d_{\text{out}}}\log(3M)/\eta^2)$ 次测量，以检验一个 d_{out} 维量子态 ρ 是否满足 $\rho=\frac{\mathbb{I}}{d_{\text{out}}}$ 或 $\left\|\rho-\frac{\mathbb{I}}{d_{\text{out}}}\right\|_2\geq\eta$，且错误概率为 $1/(3M)$。我们对量子态 $\mathcal{N}(|\phi\rangle\langle\phi|)$ 应用此测试，该态是一个 d_{out} 维量子态，并且 $\eta=\frac{\varepsilon}{2\sqrt{d_{\text{out}}d_{\text{in}}}}$。因此，量子态恒等性测试算法将使用 $\mathcal{O}(d_{\text{in}}^2d_{\text{out}}^{1.5}\log(3M)/\varepsilon^2)$ 次测量。由于我们重复此测试 $M=\mathcal{O}(1)$ 次，总测量次数为 $\mathcal{O}(d_{\text{in}}^2d_{\text{out}}^{1.5}/\varepsilon^2)$。

正确性。接下来需要证明算法 2 是 1/3-正确的。为此，我们需要控制两个错误概率。第一个是在零假设 H_0 下，量子信道 $\mathcal{N} = \mathcal{D}$，因此对于所有 $k \in [M]$,$\mathcal{N}(|\phi_k\rangle\langle\phi_k|) = \frac{\mathbb{I}}{d_{\text{out}}}$。因此，对于所有量子态测试，我们都处于零假设 h_0 下。因此

$$\begin{aligned}\mathbb{P}_{H_0}(\text{error}) &= \mathbb{P}_{H_0}(\exists k \in [M] : i_k = 1) \\ &\leq \sum_{k=1}^{M} \mathbb{P}_{h_0}(i_k = 1) \leq \sum_{k=1}^{M} \frac{1}{3M} = \frac{1}{3}.\end{aligned}$$

第二个错误概率涉及备择假设 H_1。在这种情况下，量子信道 $\mathcal{N}$ 与去极化信道 $\mathcal{D}$相差 ε。对于给定的 $k \in [M]$，我们来给出在算法第 k步处于 h_1 下的概率下界。令 $X_k = \left\|\mathcal{N}(|\phi_k\rangle\langle\phi_k|) - \frac{\mathbb{I}}{d_{\text{out}}}\right\|_2^2$。回顾定理 4.3，其表述如下:

$$\text{Var}(X_k) \leq 105\mathbb{E}\left(X_k\right)^2$$

因此，Paley-Zygmund 不等式意味着

$$\mathbb{P}\left(X_k \geq \frac{1}{2}\mathbb{E}\left(X_k\right)\right) \geq 1 - \frac{1}{\frac{1}{4}\frac{\mathbb{E}(X_k)^2}{\text{Var}(X_k)} + 1} \geq 1 - \frac{1}{\frac{1}{8\times 105} + 1} \geq 10^{-3}.$$

还要回顾 $\mathrm{E}\left(X_k\right) = \mathrm{E}\left(\left\|\mathcal{N}(|\phi_k\rangle\langle\phi_k|) - \frac{\mathbb{I}}{d}\right\|_2^2\right) \geq \frac{\varepsilon^2}{2d_{\text{in}}^2 d_{\text{out}}}$(不等式 1)。因此，以至少 10^{-3}的概率，我们有 $\left\|\mathcal{N}(|\phi_k\rangle\langle\phi_k|) - \frac{\mathbb{I}}{d_{\text{out}}}\right\|_2 \geq \frac{\varepsilon}{2d_{\text{in}}\sqrt{d_{\text{out}}}}$，这意味着我们处于备择假设$h_1$下。将 $E_k = \left\{\left\|\mathcal{N}(|\phi_k\rangle\langle\phi_k|) - \frac{\mathbb{I}}{d_{\text{out}}}\right\|_2 \geq \frac{\varepsilon}{2d_{\text{in}}\sqrt{d_{\text{out}}}}\right\}$的良事件记为，$H_1$ 下的错误概率可如下控制:

$$\begin{aligned}\mathbb{P}_{H_1}(\text{error}) = \mathbb{P}_{H_1}(\forall k \in [M] : i_k = 0) &= \prod_{k=1}^{M} \mathbb{P}_{H_1}(i_k = 0) \\ &\leq \prod_{k=1}^{M} \left(\mathbb{P}_{H_1}(i_k = 0|E_k)\mathbb{P}\left(E_k\right) + \mathbb{P}_{H_1}(i_k = 0|\bar{E}_k)\mathbb{P}\left(\bar{E}_k\right)\right) \\ &\leq \prod_{k=1}^{M} \left(\mathbb{P}_{h_1}(i_k = 0)\mathbb{P}\left(E_k\right) + \mathbb{P}\left(\bar{E}_k\right)\right) \\ &\leq \prod_{k=1}^{M} \left(\mathbb{P}_{H_1}(i_k = 0|E_k)\mathbb{P}\left(E_k\right) + 1 - \mathbb{P}\left(E_k\right)\right) \\ &= \prod_{k=1}^{M} \left(1 - \mathbb{P}\left(E_k\right)\mathbb{P}_{h_1}(i_k = 1|E_k)\right) \\ &\leq \left(1 - 10^{-3} \cdot \left(1 - \frac{1}{3M}\right)\right)^M \leq \left(1 - \frac{10^{-3}}{2}\right)^M \leq \frac{1}{3}\end{aligned}$$

对于 $M = 2200 = \mathcal{O}(1)$。这就完成了算法 2 的正确性证明。 □

D 检验恒等量子信道与去极化信道的下界

D.1 定理 4.5 的证明

定理 D.1。设 $\varepsilon \leq 1/32$、 $d_{\text{in}} \geq 80$ 和 $d_{\text{out}} \geq 10$。 [2] 任何用于恒等信道到去极化信道测试的非相干辅助系统辅助的非自适应算法（无论采用迹距离还是菱形距离），在最坏情况下都需要进行一定次数的测量

$$N = \Omega\left(\frac{d_{\text{in}}^2 d_{\text{out}}^{1.5}}{\log(d_{\text{in}} d_{\text{out}}/\varepsilon)^2 \varepsilon^2}\right).$$

证明。构造。在零假设 H_0 下，量子信道为 $\mathcal{N}(\rho) = \mathcal{D}(\rho) = \text{Tr}(\rho)\frac{\mathbb{I}}{d_{\text{out}}}$。在备择假设 H_1下，我们选择如下形式的量子信道 $\mathcal{N} \sim \mathcal{P}$:

$$\mathcal{N}(\rho) = \text{Tr}(\rho)\frac{\mathbb{I}}{d_{\text{out}}} + \frac{\varepsilon}{d_{\text{out}}} \langle \bar{w}| \rho |\bar{w}\rangle U$$

其中 $|w\rangle = W|0\rangle$， $W \sim \text{Haar}(d_{\text{in}})$，且 U 满足

$$\begin{cases} U_{x,x} = 0 & \text{for all } x \in [d_{\text{out}}], \\ U_{y,x} = \bar{U}_{x,y} \sim \mathcal{N}_c(0,\sigma^2) = \mathcal{N}(0,\sigma^2/2) + i\mathcal{N}(0,\sigma^2/2) & \text{for all } x < y \in [d_{\text{out}}], \end{cases}$$

其中参数 σ 稍后确定，并且我们对事件

$$\mathcal{G} = \{\|U\|_1 \geq d_{\text{out}}, \|U\|_\infty \leq 32\}.$$

我们将此分布称为 $\mathcal{P}$，并采用记号 $(w,U) \sim \mathcal{P}$。若不对事件 $\mathcal{G}$进行条件化，则 U的分布记为 $\mathcal{P}_0$，并写作 $U \sim \mathcal{P}_0$。Chen 等人 [2022b,f]曾使用高斯随机变量进行随机构造，以证明下界。注意，$\mathcal{N}$是迹保持的，因为 $\text{Tr}(U) = 0$。为了证明 $\mathcal{N}$是一个量子信道，尚需证明 $\mathcal{N}$是完全正的，这等价于证明相应的 Choi 矩阵是半正定的。为此，我们可以将该量子信道 $\mathcal{N}$的 Choi 态表示为:

$$\begin{aligned} \mathcal{J}_{\mathcal{N}} &= \frac{\mathbb{I}}{d_{\text{in}} d_{\text{out}}} + \frac{\varepsilon}{d_{\text{in}} d_{\text{out}}} \sum_{i,j=1}^{d_{\text{in}}} |i\rangle\langle j| \otimes \langle 0| W^\top |i\rangle\langle j| \bar{W}|0\rangle U \\ &= \frac{\mathbb{I}}{d_{\text{in}} d_{\text{out}}} + \frac{\varepsilon}{d_{\text{in}} d_{\text{out}}} \sum_{i,j} |i\rangle\langle j| \otimes \langle i| W|0\rangle\langle 0| W^\dagger |j\rangle U \\ &= \frac{\mathbb{I}}{d_{\text{in}} d_{\text{out}}} + \frac{\varepsilon}{d_{\text{in}} d_{\text{out}}} W|0\rangle\langle 0| W^\dagger \otimes U \\ &= \frac{\mathbb{I}}{D} + \frac{\varepsilon}{D}|w\rangle\langle w| \otimes U \end{aligned}$$

其中 $D = d_{\text{in}} d_{\text{out}}$。
注意到 $\||w\rangle\langle w| \otimes U\|_\infty = \|U\|_\infty \leq 32$ 因此 $\mathcal{J}_{\mathcal{N}} \geq 0$ 当且仅当 $\varepsilon \leq 1/32$。所以在事件 $\mathcal{G}$ 下，映射 $\mathcal{N}$ 是一个量子信道。参数 σ 应选择为使得 $d_\diamond(\mathcal{N},\mathcal{D}) \geq \varepsilon$。回顾 $|w\rangle = W|0\rangle$，菱形距离的定义意味着

$$\begin{aligned} d_\diamond(\mathcal{N},\mathcal{D}) &\geq d_{\text{Tr}}(\mathcal{N},\mathcal{D}) = \max_\rho \|(\mathcal{N}-\mathcal{D})(\rho)\|_1 \\ &\geq \|(\mathcal{N}-\mathcal{D})(|\bar{w}\rangle\langle\bar{w}|)\|_1 = \frac{\varepsilon}{d_{\text{out}}}\|U\|_1 \geq \varepsilon \end{aligned}$$

[2]我们没有尝试优化这些条件。

其中我们使用了以下事实：在事件 $\mathcal{G}$ 下，我们有 $\|U\|_1 \geq d_{\text{out}}$。注意，我们在该定理中证明的下界对于由迹距离给出的更强条件同样成立。现在我们来证明事件 $\mathcal{G}$ 以高概率发生。

引理 D.2. 存在常数 $c > 0$，使得：

$$\mathbb{P}\left(\left|\|U\|_1 - \mathbb{E}\left(\|U\|_1\right)\right| > s\right) \leq \exp\left(-\frac{cs^2}{d_{\text{out}}\sigma^2}\right)$$

证明. 函数 $U \mapsto \|U\|_1$ 关于希尔伯特-施密特范数是 $\sqrt{d_{\text{out}}}$-Lipschitz 函数。事实上，根据三角不等式和柯西-施瓦茨不等式 $\left|\|U\|_1 - \|V\|_1\right| \leq \|U - V\|_1 \leq \sqrt{d_{\text{out}}}\|U - V\|_2$。高斯随机变量的 Lipschitz 函数的集中性 [Wainwright，2019年，定理 2.26] 恰好给出了所需结论。 □

接下来，我们需要给出 $\|U\|_1$ 期望的一个下界。根据霍尔德不等式：

$$\mathbb{E}\left(\|U\|_1\right) \geq \sqrt{\frac{\mathbb{E}\left(\|U\|_2^2\right)^3}{\mathbb{E}\left(\|U\|_4^4\right)}} \geq \sqrt{\frac{(d_{\text{out}}^2\sigma^2)^3}{4d_{\text{out}}^3\sigma^4}} = \frac{d_{\text{out}}\sqrt{d_{\text{out}}}\sigma}{2}.$$

只需选取 $\sigma = \frac{4}{\sqrt{d_{\text{out}}}}$，使得 $\mathbb{E}\left(\|U\|_1\right) \geq 2d_{\text{out}}$，根据引理 D.2，我们以 $1 - \exp(-\Omega(d_{\text{out}}^2))$ 的概率有 $\|U\|_1 \geq d_{\text{out}}$。还需证明，对于这个 $\sigma = \frac{4}{\sqrt{d_{\text{out}}}}$ 的选取，事件 $\{\|U\|_\infty \leq 32\}$ 也以高概率发生。事实上，令 $\mathcal{S}$ 为 $\mathbb{S}^{d_{\text{out}}}$ 的一个 $1/4$-网，其大小至多为 $8^{d_{\text{out}}}$。根据并合界：

$$\begin{aligned}
\mathbb{P}\left(\|U\|_\infty > 32\right) &= \mathbb{P}\left(\exists \phi \in \mathbf{S}^{d_{\text{out}}} : \langle\phi| U |\phi\rangle = \|U\|_\infty, \|U\|_\infty > 32\right) \\
&\leq \mathbb{P}\left(\exists \phi \in \mathcal{S} : \langle\phi| U |\phi\rangle > \frac{1}{2}\|U\|_\infty, \|U\|_\infty > 32\right) \\
&\leq |\mathcal{S}|\mathbb{P}\left(\langle\phi| U |\phi\rangle > 16\right) \leq 8^{d_{\text{out}}} e^{-8d_{\text{out}}} \leq e^{-4d_{\text{out}}}.
\end{aligned}$$

最后，以至少为 $1 - \exp(-\Omega(d_{\text{out}}^2)) - \exp(-\Omega(d_{\text{out}}))$ 的概率，事件 $\mathcal{G}$ is satisfied，并且我们有一个量子信道 $\mathcal{N}$，它与去极化信道 $\mathcal{D}$ 的菱形距离为 ε-far。一个 $1/3$-correct 算法 $\mathcal{A}$ 应以至多为 $1/3$ 的错误概率区分信道 $\mathcal{N}$ 和 $\mathcal{D}$。令 N 为完成此任务所需的足够测量次数，并令 I_1，...，I_N 为算法 $\mathcal{A}$ 的观测值。对全变差距离应用数据处理不等式，可得 Le Cam 方法 [Le Cam，1973]:

$$\begin{aligned}
\mathrm{TV}\left(\mathbb{P}_{H_0}^{I_1,\ldots,I_N} \middle\| \mathbb{P}_{H_1}^{I_1,\ldots,I_N}\right) &\geq \mathrm{TV}\left(\mathrm{Bern}(\mathbb{P}_{H_0}(\mathcal{A} = 1)) \| \mathrm{Bern}(\mathbb{P}_{H_1}(\mathcal{A} = 1))\right) \\
&\geq \mathrm{TV}(\mathrm{Bern}(1/3) \| \mathrm{Bern}(2/3)) = \frac{1}{3}.
\end{aligned}$$

现在，我们需要用一个涉及 N、d_{in}、d_{out} 和 ε 的表达式来给出这个全变差距离的上界。

全变差距离的上界。非自适应算法 $\mathcal{A}$ 会在步骤 t 选择输入 ρ_t 和测量装置 $\mathcal{M}_t = \{\lambda_i^t |\phi_i^t\rangle\langle\phi_i^t|\}_{i \in \mathcal{I}_t}$。注意，在不失一般性的情况下，我们总可以将问题约化为这样的正算子值测度。在零假设 H_0 下，量子信道 $\mathcal{N} = \mathcal{D}$，因此结果的概率分布恰好为：

$$\mathbb{P}_{H_0}^{I_1,\ldots,I_N} = \left\{\prod_{t=1}^{N} \lambda_{i_t}^t \left\langle \phi_{i_t}^t \right| \mathrm{id} \otimes \mathcal{D}(\rho_t) \left| \phi_{i_t}^t \right\rangle\right\}_{i_1,\ldots,i_N}.$$

在该　另一方面，在备择假设 H_1 下，结果的概率恰好为　:

$$\mathbb{P}_{H_1}^{I_1,\ldots,I_N} = \left\{ \prod_{t=1}^{N} \lambda_{i_t}^t \left\langle \phi_{i_t}^t \right| \mathrm{id} \otimes \mathcal{N}(\rho_t) \left| \phi_{i_t}^t \right\rangle \right\}_{i_1,\ldots,i_N}$$

回顾一下， $D = d_{\mathrm{in}} d_{\mathrm{out}}$ 以及

$$\mathcal{J}_{\mathcal{D}} = \frac{\mathbb{I}}{D} \quad \text{and} \quad \mathcal{J}_{\mathcal{N}} = \frac{\mathbb{I}}{D} + \frac{\varepsilon}{D} |w\rangle\langle w| \otimes U.$$

由于全变差距离的凸性，我们不妨假设每个输入态都是纯态。也就是说，对于 $t \in [N]$，我们写作 $\rho_t = |\psi_t\rangle\langle\psi_t|$。此外，我们可以将每个秩一输入态和测量向量写成如下形式:

$$|\psi_t\rangle = A_t \otimes \mathbb{I} |\Psi_{d_{\mathrm{in}}}\rangle \quad \text{and} \quad \left|\phi_{i_t}^t\right\rangle = B_{i_t}^t \otimes \mathbb{I} |\Psi_{d_{\mathrm{out}}}\rangle$$

其中 $|\Psi_d\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |ii\rangle$，且矩阵 $A_t \in \mathbb{C}^{d_{\mathrm{anc}} \times d_{\mathrm{in}}}$ 和 $B_{i_t}^t \in \mathbb{C}^{d_{\mathrm{anc}} \times d_{\mathrm{out}}}$ 满足:

$$\mathrm{Tr}(A_t A_t^\dagger) = d_{\mathrm{in}} \quad \text{and} \quad \mathrm{Tr}(B_{i_t}^t B_{i_t}^{t,\dagger}) = d_{\mathrm{out}}.$$

注意，对于所有 t 以及所有 $X \in \mathbb{C}^{d_{\mathrm{anc}} \otimes d_{\mathrm{anc}}}$，我们有 $\sum_{i_t} \lambda_{i_t}^t B^{t,}{}_{i_t}{}^{\dagger} X B_{i_t}^t = d_{\mathrm{out}} \mathbf{Tr}(X) \mathbb{I}_{d_{\mathrm{out}}}$。事实上，正算子值测度 $\mathcal{M}_t$ 的条件意味着:

$$X \otimes \mathbb{I} = X \otimes \mathbb{I} \sum_{i_t} \lambda_{i_t}^t \left|\phi_{i_t}^t\right\rangle\left\langle\phi_{i_t}^t\right| = \sum_{i_t} \lambda_{i_t}^t X B_{i_t}^t \otimes \mathbb{I} |\Psi_{d_{\mathrm{out}}}\rangle\langle\Psi_{d_{\mathrm{out}}}| B_{i_t}^{t,\dagger} \otimes \mathbb{I}$$

因此，取偏迹可得

$$\mathrm{Tr}(X)\mathbb{I} = \frac{1}{d_{\mathrm{out}}} \sum_{i_t,i,j} \lambda_{i_t}^t \langle j| B_{i_t}^{t,\dagger} X B_{i_t}^t |i\rangle |i\rangle \langle j|.$$

最后

$$\sum_{i_t} \lambda_{i_t}^t B_{i_t}^{t,\dagger} X B_{i_t}^t = d_{\mathrm{out}} \mathrm{Tr}(X) \mathbb{I}_{d_{\mathrm{out}}}.$$

取 $X = \mathbb{I}$ 并对第二个系统取偏迹，我们得到

$$\sum_{i_t} \lambda_{i_t}^t B_{i_t}^t B_{i_t}^{t,\dagger} = d_{\mathrm{out}}^2 \mathbb{I}_{d_{\mathrm{anc}}}.$$

现在，我们可以将零假设下观测值的分布重新写成如下形式:

$$\begin{aligned}
\mathbb{P}_{H_0}^{I_1,\ldots,I_N} &= \left\{ \prod_{t=1}^{N} \lambda_{i_t}^t \left\langle \phi_{i_t}^t \right| \mathrm{id} \otimes \mathcal{D}(\rho_t) \left| \phi_{i_t}^t \right\rangle \right\}_{i_1,\ldots,i_N} \\
&= \left\{ \prod_{t=1}^{N} \lambda_{i_t}^t \langle \Psi_{d_{\mathrm{out}}}| (B_{i_t}^{t,\dagger} A_t \otimes \mathbb{I}) \mathcal{J}_{\mathcal{D}} (A_t^\dagger B_{i_t}^t \otimes \mathbb{I}) |\Psi_{d_{\mathrm{out}}}\rangle \right\}_{i_1,\ldots,i_N} \\
&= \left\{ \prod_{t=1}^{N} \frac{\lambda_{i_t}^t}{D} \langle \Psi_{d_{\mathrm{out}}}| (B_{i_t}^{t,\dagger} A_t A_t^\dagger B_{i_t}^t \otimes \mathbb{I}) |\Psi_{d_{\mathrm{out}}}\rangle \right\}_{i_1,\ldots,i_N} \\
&= \left\{ \prod_{t=1}^{N} \frac{\lambda_{i_t}^t}{D d_{\mathrm{out}}} \mathrm{Tr}(B_{i_t}^{t,\dagger} A_t A_t^\dagger B_{i_t}^t) \right\}_{i_1,\ldots,i_N},
\end{aligned}$$

并在备择假设下如下：

$$\begin{aligned}
\mathbb{P}_{H_1}^{I_1,\ldots,I_N} &= \left\{\prod_{t=1}^{N}\lambda_{i_t}^t\left\langle\phi_{i_t}^t\right|\mathrm{id}\otimes\mathcal{N}(\rho_t)\left|\phi_{i_t}^t\right\rangle\right\}_{i_1,\ldots,i_N}\\
&= \left\{\prod_{t=1}^{N}\lambda_{i_t}^t\left\langle\Psi_{d_{\mathrm{out}}}\right|(B_{i_t}^{t,\dagger}A_t\otimes\mathbb{I})\mathcal{J}_{\mathcal{N}}(A_t^\dagger B_{i_t}^t\otimes\mathbb{I})\left|\Psi_{d_{\mathrm{out}}}\right\rangle\right\}_{i_1,\ldots,i_N}\\
&= \left\{\prod_{t=1}^{N}\lambda_{i_t}^t\left\langle\Psi_{d_{\mathrm{out}}}\right|(B_{i_t}^{t,\dagger}A_t\otimes\mathbb{I})\left(\frac{\mathbb{I}}{D}+\frac{\varepsilon}{D}|w\rangle\langle w|\otimes U\right)(A_t^\dagger B_{i_t}^t\otimes\mathbb{I})\left|\Psi_{d_{\mathrm{out}}}\right\rangle\right\}_{i_1,\ldots,i_N}\\
&= \left\{\prod_{t=1}^{N}\left(\frac{\lambda_{i_t}^t}{Dd_{\mathrm{out}}}\mathrm{Tr}(B_{i_t}^{t,\dagger}A_tA_t^\dagger B_{i_t}^t)+\frac{\varepsilon\lambda_{i_t}^t}{D}\left\langle\Psi_{d_{\mathrm{out}}}\right|(B_{i_t}^{t,\dagger}A_t|w\rangle\langle w|A_t^\dagger B_{i_t}^t\otimes U)\left|\Psi_{d_{\mathrm{out}}}\right\rangle\right)\right\}_{i_1,\ldots,i_N}
\end{aligned}$$

因此，我们可以将全变差距离表示如下：

$$\begin{aligned}
&2\,\mathrm{TV}\left(\mathbb{P}_{H_0}^{I_1,\ldots,I_N}\middle\|\mathbb{P}_{H_1}^{I_1,\ldots,I_N}\right)\\
&=\sum_{i_1,\ldots,i_N}\left|\mathbb{E}_{(w,U)\sim\mathcal{P}}\prod_{t=1}^{N}\left(\frac{\lambda_{i_t}^t}{Dd_{\mathrm{out}}}\mathrm{Tr}(B_{i_t}^{t,\dagger}A_tA_t^\dagger B_{i_t}^t)+\frac{\varepsilon\lambda_{i_t}^t}{D}\left\langle\Psi_{d_{\mathrm{out}}}\right|(B_{i_t}^{t,\dagger}A_t|w\rangle\langle w|A_t^\dagger B_{i_t}^t\otimes U)\left|\Psi_{d_{\mathrm{out}}}\right\rangle\right)\right.\\
&\qquad\left.-\prod_{t=1}^{N}\frac{\lambda_{i_t}^t}{Dd_{\mathrm{out}}}\mathrm{Tr}(B_{i_t}^{t,\dagger}A_tA_t^\dagger B_{i_t}^t)\right|\\
&=\mathbb{E}_{\le N}\left|\mathbb{E}_{(w,U)\sim\mathcal{P}}\prod_{t=1}^{N}\left(1+\varepsilon d_{\mathrm{out}}\frac{\left\langle\Psi_{d_{\mathrm{out}}}\right|(B_{i_t}^{t,\dagger}A_t|w\rangle\langle w|A_t^\dagger B_{i_t}^t\otimes U)\left|\Psi_{d_{\mathrm{out}}}\right\rangle}{\mathrm{Tr}(B_{i_t}^{t,\dagger}A_tA_t^\dagger B_{i_t}^t)}\right)-1\right|\\
&=\mathbb{E}_{\le N}\left|\mathbb{E}_{(w,U)\sim\mathcal{P}}\prod_{t=1}^{N}\left(1+\varepsilon\cdot\frac{\mathrm{Tr}(B_{i_t}^{t,\dagger}A_t|w\rangle\langle w|A_t^\dagger B_{i_t}^t U)}{\mathrm{Tr}(B_{i_t}^{t,\dagger}A_tA_t^\dagger B_{i_t}^t)}\right)_{\lambda_{i_t}^t}-1\right|
\end{aligned}$$

其中我们使用记号 $\mathbb{E}_{\le N}(X(i_1,\ldots,i_N))=\sum_{i_1,\ldots,i_N}\left(\prod_{t=1}^{N}\frac{\lambda_{i_t}^t}{Dd_{\mathrm{out}}}\mathrm{Tr}(B^{t}{}_{,i_t}{}^\dagger A_tA_t^\dagger B_{i_t}^t)\right)X(i_1,\ldots,i_N)$。令 u 为满足 $|w\rangle=\frac{|u\rangle}{\|u\|_2}$的标准高斯向量。我们对事件 $\mathcal{E}$ 进行条件化，其中 u 满足：

1. $\|u\|_2\ge\sqrt{\frac{1}{6}d_{\mathrm{in}}}$和 2.

$\forall t\in[N]:\quad P_u^t\le(7\log($

$N\quad^4))$

$d_{\mathrm{in}}^4d_{\mathrm{out}}$

其中 P_u^t 定义为

$$\begin{aligned}
P_w^t&=\sum_{i_t,j_t}\frac{\lambda_{i_t}^t\lambda_{j_t}^t}{D^2d_{\mathrm{out}}^2}\left(\frac{|\langle w|A_t^\dagger B_{i_t}^tB_{j_t}^{t,\dagger}A_t|w\rangle|^4}{\mathrm{Tr}(B_{i_t}^{t,\dagger}A_tA_t^\dagger B_{i_t}^t)\mathrm{Tr}(B_{j_t}^{t,\dagger}A_tA_t^\dagger B_{j_t}^t)}\right)\\
P_u^t&=\sum_{i_t,j_t}\frac{\lambda_{i_t}^t\lambda_{j_t}^t}{D^2d_{\mathrm{out}}^2d_{\mathrm{in}}^4}\left(\frac{|\langle u|A_t^\dagger B_{i_t}^tB_{j_t}^{t,\dagger}A_t|u\rangle|^4}{\mathrm{Tr}(B_{i_t}^{t,\dagger}A_tA_t^\dagger B_{i_t}^t)\mathrm{Tr}(B_{j_t}^{t,\dagger}A_tA_t^\dagger B_{j_t}^t)}\right).
\end{aligned}$$

注意，在事件 $\mathcal{E}$ 下，我们有 $P_w^t\le6^4P_u^t$。我们声称，对于 $d_{\mathrm{in}}\ge80$，事件 $\mathcal{E}$ 至少以 $9/10$ 的概率成立。该结论的证明见引理 D.3。

现在，我们可以通过全变差距离区分事件 $\mathcal{E}$ 是否成立。令

$$\Psi_{i,w,U}=\prod_{t=1}^{N}\left(1+\varepsilon\cdot\Phi_{w,U}^{t,i_t}\right)\quad\text{where}\quad\Phi_{w,U}^{t,i_t}=\frac{\mathrm{Tr}(B_{i_t}^{t,\dagger}A_t\left|w\right\rangle\!\left\langle w\right|A_t^\dagger B_{i_t}^tU)}{\mathrm{Tr}(B_{i_t}^{t,\dagger}A_tA_t^\dagger B_{i_t}^t)}.$$

根据三角不等式:

$$\begin{aligned}
&\mathbb{E}_{\le N}\left|\mathbb{E}_{(w,U)\sim\mathcal{P}}\prod_{t=1}^{N}\left(1+\varepsilon\cdot\frac{\mathrm{Tr}(B_{i_t}^{t,\dagger}A_t\left|w\right\rangle\!\left\langle w\right|A_t^\dagger B_{i_t}^tU)}{\mathrm{Tr}(B_{i_t}^{t,\dagger}A_tA_t^\dagger B_{i_t}^t)}\right)-1\right|\\
&\le\mathbb{E}_{\le N}\left|\mathbb{E}_{(w,U)\sim\mathcal{P}}\left[\mathbf{1}\{\mathcal{E}\}(\Psi_{i,w,U}-1)\right]\right|+\mathbb{E}_{\le N}\left|\mathbb{E}_{(w,U)\sim\mathcal{P}}\left[\mathbf{1}\{\bar{\mathcal{E}}\}(\Psi_{i,w,U}-1)\right]\right|\\
&\le\mathbb{E}_{\le N}\left|\mathbb{E}_{(w,U)\sim\mathcal{P}}\left[\mathbf{1}\{\mathcal{E}\}(\Psi_{i,w,U}-1)\right]\right|+\mathbb{E}_{\le N}\mathbb{E}_{(w,U)\sim\mathcal{P}}\left[\mathbf{1}\{\bar{\mathcal{E}}\}(\Psi_{i,w,U}+1)\right]\\
&=\mathbb{E}_{\le N}\left|\mathbb{E}_{(w,U)\sim\mathcal{P}}\left[\mathbf{1}\{\mathcal{E}\}(\Psi_{i,w,U}-1)\right]\right|+2\mathbb{P}\left(\bar{\mathcal{E}}\right)
\end{aligned}$$

其中我们利用了以下事实: $\sum_{i_t}\lambda_{i_t}^tB^{t,\ i_t\ \dagger}XB_{i_t}^t=d_{\text{out}}$迹$(X)\mathbb{I}$ 以及

$$\begin{aligned}
\mathbb{E}_{\le N}\Psi_{i,w,U}&=\sum_{i_1,\ldots,i_N}\left(\prod_{t=1}^{N}\frac{\lambda_{i_t}^t}{Dd_{\text{out}}}\cdot\mathrm{Tr}(B_{i_t}^{t,\dagger}A_tA_t^\dagger B_{i_t}^t)\right)\prod_{t=1}^{N}\left(1+\varepsilon\cdot\frac{\mathrm{Tr}(B_{i_t}^{t,\dagger}A_t\left|w\right\rangle\!\left\langle w\right|A_t^\dagger B_{i_t}^tU)}{\mathrm{Tr}(B_{i_t}^{t,\dagger}A_tA_t^\dagger B_{i_t}^t)}\right)\\
&=\prod_{t=1}^{N}\sum_{i_t}\left(\frac{\lambda_{i_t}^t}{Dd_{\text{out}}}\cdot\mathrm{Tr}(B_{i_t}^{t,\dagger}A_tA_t^\dagger B_{i_t}^t)+\frac{\varepsilon\lambda_{i_t}^t}{Dd_{\text{out}}}\cdot\mathrm{Tr}(B_{i_t}^{t,\dagger}A_t\left|w\right\rangle\!\left\langle w\right|A_t^\dagger B_{i_t}^tU)\right)\\
&=\prod_{t=1}^{N}\left(1+\frac{\varepsilon}{D}\cdot\mathrm{Tr}(A_t\left|w\right\rangle\!\left\langle w\right|A_t^\dagger)\mathrm{Tr}(U)\right)=1.
\end{aligned}$$

剩下的工作是为期望 $\mathbb{E}_{\le N}\left|\mathbb{E}_{(w,U)\sim\mathcal{P}}\left[\mathbf{1}\{\mathcal{E}\}(\Psi_{i,\ w,\ U}-1)\right]\right|$给出上界。为此，我们沿用[Bubeck 等人 2020]的方法，并应用柯西-施瓦茨不等式和霍尔德不等式:

$$\begin{aligned}
&\left(\mathbb{E}_{\le N}\left|\mathbb{E}_{(w,U)\sim\mathcal{P}}\left[\mathbf{1}\{\mathcal{E}\}(\Psi_{i,w,U}-1)\right]\right|\right)^2+\mathbb{P}\left(\mathcal{E}\right)^2\\
&\le\mathbb{E}_{\le N}\left(\mathbb{E}_{(w,U)\sim\mathcal{P}}\left[\mathbf{1}\{\mathcal{E}(w)\}(\Psi_{i,w,U}-1)\right]\right)^2+\mathbb{P}\left(\mathcal{E}\right)^2\\
&=\mathbb{E}_{\le N}\mathbb{E}_{(w,U)\sim\mathcal{P}}\mathbb{E}_{(z,V)\sim\mathcal{P}}\mathbf{1}\{\mathcal{E}(w)\}\Psi_{i,w,U}\mathbf{1}\{\mathcal{E}(z)\}\Psi_{i,z,V}\\
&\le\mathbb{E}_{(w,U)\sim\mathcal{P}}\mathbf{1}\{\mathcal{E}(w)\}\mathbb{E}_{(z,V)\sim\mathcal{P}}\mathbf{1}\{\mathcal{E}(z)\}\prod_{t=1}^{N}\mathbb{E}_{i_t}\left(1+\varepsilon\cdot\Phi_{w,U}^{t,i_t}\right)\left(1+\varepsilon\cdot\Phi_{z,V}^{t,i_t}\right)\\
&=\mathbb{E}_{(w,U)\sim\mathcal{P}}\mathbf{1}\{\mathcal{E}(w)\}\mathbb{E}_{(z,V)\sim\mathcal{P}}\mathbf{1}\{\mathcal{E}(z)\}\prod_{t=1}^{N}\left(1+\varepsilon^2\cdot\mathbb{E}_{i_t}\Phi_{w,U}^{t,i_t}\Phi_{z,V}^{t,i_t}\right)\quad(\text{ because }\ \mathbb{E}_{i_t}\Phi_{w,U}^{t,i_t}=0)\\
&\le\max_{1\le t\le N}\mathbb{E}_{(w,U)\sim\mathcal{P}}\mathbf{1}\{\mathcal{E}(w)\}\mathbb{E}_{(z,V)\sim\mathcal{P}}\mathbf{1}\{\mathcal{E}(z)\}\left(1+\varepsilon^2\cdot\mathbb{E}_{i_t}\Phi_{w,U}^{t,i_t}\Phi_{z,V}^{t,i_t}\right)^N\\
&\le\frac{1}{\mathbb{P}\left(\mathcal{G}\right)^2}\max_{1\le t\le N}\mathbb{E}_{U,V\sim\mathcal{P}_0}\mathbb{E}_{w,z}\mathbf{1}\{\mathcal{E}(w)\}\mathbf{1}\{\mathcal{E}(z)\}\left(1+\varepsilon^2\cdot\left|\mathbb{E}_{i_t}\Phi_{w,U}^{t,i_t}\Phi_{z,V}^{t,i_t}\right|\right)^N\\
&\le\frac{1}{(1-e^{-\Omega(d_{\text{out}})})^2}\max_{1\le t\le N}\mathbb{E}_{U,V\sim\mathcal{P}_0}\mathbb{E}_{w,z}\mathbf{1}\{\mathcal{E}(w)\}\mathbf{1}\{\mathcal{E}(z)\}\left(1+\varepsilon^2\cdot\left|\mathbb{E}_{i_t}\Phi_{w,U}^{t,i_t}\Phi_{z,V}^{t,i_t}\right|\right)^N
\end{aligned}$$

注意，在最后两个不等式中，我们不再要求 U 满足 $\|U\|_\infty\le 32$ 和 $\|U\|_1\ge d_{\text{out}}$。这是可能的，因为被积函数为正且 $\mathrm{P}\left(\mathcal{G}\right)\ \ge 1-e^{-\Omega(d_{\text{out}})}$ 。

对于 $t \in [N]$，令 Z_t为 $\{U_{i,j}, V_{i,j}\}_i^{d_{\text{out}}}$，$j=1$ 中定义如下的多项式：

$$\begin{aligned}
Z_t &= \varepsilon^2 \mathbb{E}_{i_t} \Phi_{w,U}^{t,i_t} \Phi_{z,V}^{t,i_t} \\
&= \varepsilon^2 \sum_{i_t} \left(\frac{\lambda_{i_t}^t}{D d_{\text{out}}} \text{Tr}(B_{i_t}^{t,\dagger} A_t A_t^\dagger B_{i_t}^t) \right) \left(\frac{\text{Tr}(B_{i_t}^{t,\dagger} A_t \left|w\right\rangle\!\left\langle w\right| A_t^\dagger B_{i_t}^t U)}{\text{Tr}(B_{i_t}^{t,\dagger} A_t A_t^\dagger B_{i_t}^t)} \right) \left(\frac{\text{Tr}(B_{i_t}^{t,\dagger} A_t \left|z\right\rangle\!\left\langle z\right| A_t^\dagger B_{i_t}^t V)}{\text{Tr}(B_{i_t}^{t,\dagger} A_t A_t^\dagger B_{i_t}^t)} \right) \\
&= \varepsilon^2 \sum_{i_t} \left(\frac{\lambda_{i_t}^t}{D d_{\text{out}}} \right) \left(\frac{\text{Tr}(B_{i_t}^{t,\dagger} A_t \left|w\right\rangle\!\left\langle w\right| A_t^\dagger B_{i_t}^t U) \text{Tr}(B_{i_t}^{t,\dagger} A_t \left|z\right\rangle\!\left\langle z\right| A_t^\dagger B_{i_t}^t V)}{\text{Tr}(B_{i_t}^{t,\dagger} A_t A_t^\dagger B_{i_t}^t)} \right)
\end{aligned}$$

注意，Z_t 是一个期望为 0 的二次多项式。超收缩性 [Aubrun 和 Szarek，2017，命题 5.48] 对所有 $k \in \{1, \ldots, N\}$均成立：

$$\mathbb{E}\left(|Z_t|^k\right) \leq k^k \mathbb{E}\left(Z_t^2\right)^{k/2}.$$

这意味着我们只需控制 Z_t的二阶矩。我们有：

$$\begin{aligned}
\mathbb{E}_{U,V}(Z_t^2) = \varepsilon^4 \mathbb{E}_{U,V} \Bigg[\sum_{i_t, j_t} \frac{\lambda_{i_t}^t \lambda_{j_t}^t}{D^2 d_{\text{out}}^2} \left(\frac{\text{Tr}(B_{i_t}^{t,\dagger} A_t \left|w\right\rangle\!\left\langle w\right| A_t^\dagger B_{i_t}^t U) \text{Tr}(B_{i_t}^{t,\dagger} A_t \left|z\right\rangle\!\left\langle z\right| A_t^\dagger B_{i_t}^t V)}{\text{Tr}(B_{i_t}^{t,\dagger} A_t A_t^\dagger B_{i_t}^t)} \right) \\
\cdot \left(\frac{\text{Tr}(B_{j_t}^{t,\dagger} A_t \left|w\right\rangle\!\left\langle w\right| A_t^\dagger B_{j_t}^t U) \text{Tr}(B_{j_t}^{t,\dagger} A_t \left|z\right\rangle\!\left\langle z\right| A_t^\dagger B_{j_t}^t V)}{\text{Tr}(B_{j_t}^{t,\dagger} A_t A_t^\dagger B_{j_t}^t)} \right) \Bigg].
\end{aligned}$$

令$\Xi_{i_t,j_t}(w) = \mathbb{E}_U[\text{迹}(B^t{}_{,i_t}{}^\dagger A_t \left|w\right\rangle\!\left\langle w\right| A_t^\dagger B_{i_t}^t U) \text{迹}(B^t{}_{,j_t}{}^\dagger A_t \left|w\right\rangle\!\left\langle w\right| A_t^\dagger B_{j_t}^t U)]$，我们有：

$$\mathbb{E}_{U,V}(Z_t^2) = \varepsilon^4 \sum_{i_t, j_t} \frac{\lambda_{i_t}^t \lambda_{j_t}^t}{D^2 d_{\text{out}}^2} \left(\frac{\Xi_{i_t,j_t}(w) \Xi_{i_t,j_t}(z)}{\text{Tr}(B_{i_t}^{t,\dagger} A_t A_t^\dagger B_{i_t}^t) \text{Tr}(B_{j_t}^{t,\dagger} A_t A_t^\dagger B_{j_t}^t)} \right)$$

给定 i_t, j_t，我们可以对期望Ξ_{i_t,j_t}给出上界：

$$\begin{aligned}
\Xi_{i_t,j_t}(w) &= \mathbb{E}_U[\text{Tr}(B_{i_t}^{t,\dagger} A_t \left|w\right\rangle\!\left\langle w\right| A_t^\dagger B_{i_t}^t U) \text{Tr}(B_{j_t}^{t,\dagger} A_t \left|w\right\rangle\!\left\langle w\right| A_t^\dagger B_{j_t}^t U)] \\
&= \sum_{x,y,x',y'} \mathbb{E}\left(U_{x,y} U_{x',y'}\right) \text{Tr}(B_{i_t}^{t,\dagger} A_t \left|w\right\rangle\!\left\langle w\right| A_t^\dagger B_{i_t}^t \left|x\right\rangle\!\left\langle y\right|) \text{Tr}(B_{j_t}^{t,\dagger} A_t \left|w\right\rangle\!\left\langle w\right| A_t^\dagger B_{j_t}^t \left|x'\right\rangle\!\left\langle y'\right|) \\
&\leq \frac{16}{d_{\text{out}}} \sum_{x,y} \left\langle w\right| A_t^\dagger B_{i_t}^t \left|x\right\rangle\!\left\langle x\right| B_{j_t}^{t,\dagger} A_t \left|w\right\rangle \left\langle w\right| A_t^\dagger B_{j_t}^t \left|y\right\rangle\!\left\langle y\right| B_{i_t}^{t,\dagger} A_t \left|w\right\rangle \\
&= \frac{16}{d_{\text{out}}} \left\langle w\right| A_t^\dagger B_{i_t}^t B_{j_t}^{t,\dagger} A_t \left|w\right\rangle \left\langle w\right| A_t^\dagger B_{j_t}^t B_{i_t}^{t,\dagger} A_t \left|w\right\rangle \\
&= \frac{16}{d_{\text{out}}} |\left\langle w\right| A_t^\dagger B_{i_t}^t B_{j_t}^{t,\dagger} A_t \left|w\right\rangle|^2
\end{aligned}$$

因此，我们可以将 Z_t^2 的期望上界表示如下：

$$\begin{aligned}
\mathbb{E}_{U,V}(Z_t^2) &= \varepsilon^4 \sum_{i_t, j_t} \frac{\lambda_{i_t}^t \lambda_{j_t}^t}{D^2 d_{\text{out}}^2} \left(\frac{\Xi_{i_t,j_t}(w) \Xi_{i_t,j_t}(z)}{\text{Tr}(B_{i_t}^{t,\dagger} A_t A_t^\dagger B_{i_t}^t) \text{Tr}(B_{j_t}^{t,\dagger} A_t A_t^\dagger B_{j_t}^t)} \right) \\
&= \varepsilon^4 \left(\frac{16^2}{d_{\text{out}}^2} \right) \sum_{i_t, j_t} \frac{\lambda_{i_t}^t \lambda_{j_t}^t}{D^2 d_{\text{out}}^2} \left(\frac{|\left\langle w\right| A_t^\dagger B_{i_t}^t B_{j_t}^{t,\dagger} A_t \left|w\right\rangle|^2 |\left\langle z\right| A_t^\dagger B_{i_t}^t B_{j_t}^{t,\dagger} A_t \left|z\right\rangle|^2}{\text{Tr}(B_{i_t}^{t,\dagger} A_t A_t^\dagger B_{i_t}^t) \text{Tr}(B_{j_t}^{t,\dagger} A_t A_t^\dagger B_{j_t}^t)} \right)
\end{aligned}$$

这意味着每个矩都有一个上界，也就是说，对于 $k=1$、.....、 N，我们有：

$$
\begin{aligned}
&\mathbb{E}_{w,z}\mathbf{1}\{\mathcal{E}(w)\}\mathbf{1}\{\mathcal{E}(z)\}\mathbb{E}_{U,V}(|Z_t|^k)\\
&\leq \mathbb{E}_{w,z}\mathbf{1}\{\mathcal{E}(w)\}\mathbf{1}\{\mathcal{E}(z)\}k^k\left[\varepsilon^4\left(\frac{16^2}{d_{\text{out}}^2}\right)\sum_{i_t,j_t}\frac{\lambda_{i_t}^t\lambda_{j_t}^t}{D^2d_{\text{out}}^2}\left(\frac{|\langle w|\,A_t^\dagger B_{i_t}^tB_{j_t}^{t,\dagger}A_t\,|w\rangle\,|^2|\langle z|\,A_t^\dagger B_{i_t}^tB_{j_t}^{t,\dagger}A_t\,|z\rangle\,|^2}{\mathrm{Tr}(B_{i_t}^{t,\dagger}A_tA_t^\dagger B_{i_t}^t)\mathrm{Tr}(B_{j_t}^{t,\dagger}A_tA_t^\dagger B_{j_t}^t)}\right)\right]^{k/2}\\
&\leq k^k\mathbb{E}_{w,z}\mathbf{1}\{\mathcal{E}(w)\}\mathbf{1}\{\mathcal{E}(z)\}\left[\varepsilon^4\left(\frac{16^2}{d_{\text{out}}^2}\right)\sum_{i_t,j_t}\frac{\lambda_{i_t}^t\lambda_{j_t}^t}{D^2d_{\text{out}}^2}\left(\frac{|\langle w|\,A_t^\dagger B_{i_t}^tB_{j_t}^{t,\dagger}A_t\,|w\rangle\,|^4+|\langle z|\,A_t^\dagger B_{i_t}^tB_{j_t}^{t,\dagger}A_t\,|z\rangle\,|^4}{2\mathrm{Tr}(B_{i_t}^{t,\dagger}A_tA_t^\dagger B_{i_t}^t)\mathrm{Tr}(B_{j_t}^{t,\dagger}A_tA_t^\dagger B_{j_t}^t)}\right)\right]^{k/2}\\
&= k^k\mathbb{E}_{w,z}\mathbf{1}\{\mathcal{E}(w)\}\mathbf{1}\{\mathcal{E}(z)\}\left[\varepsilon^4\left(\frac{16^2}{d_{\text{out}}^2}\right)\frac{(P_w^t+P_z^t)}{2}\right]^{k/2}\\
&\leq k^k\mathbb{E}_{w,z}\mathbf{1}\{\mathcal{E}(w)\}\mathbf{1}\{\mathcal{E}(z)\}\left[\varepsilon^4\left(\frac{16^2\cdot 6^4}{d_{\text{out}}^2}\right)\frac{(P_u^t+P_v^t)}{2}\right]^{k/2}\\
&\leq k^k\mathbb{E}_{w,z}\mathbf{1}\{\mathcal{E}(w)\}\mathbf{1}\{\mathcal{E}(z)\}\left[\varepsilon^4\left(\frac{16^2\cdot 6^4}{d_{\text{out}}^2}\right)\left(\frac{(7\log(N))^4}{d_{\text{in}}^4d_{\text{out}}}\right)\right]^{k/2}\leq k^k\left[\frac{C\varepsilon^4\log(N)^4}{d_{\text{in}}^4d_{\text{out}}^3}\right]^{k/2}
\end{aligned}
$$

其中 $C>0$ 是一个通用常数，并且我们利用了事件 $\mathcal{E}(w)$ 和 $\mathcal{E}(z)$ 成立这一条件。现在，将全变差距离的下界和上界合并，可得：

$$
\begin{aligned}
(1-e^{-\Omega(d_{\text{out}})})^2\left(\frac{7^2}{15^2}+\frac{9^2}{10^2}\right)&\leq(1-e^{-\Omega(d_{\text{out}})})^2\left[\left(2\,\mathrm{TV}\left(\mathbb{P}_{H_0}^{I_1,\ldots,I_N}\middle\|\mathbb{P}_{H_1}^{I_1,\ldots,I_N}\right)-2\mathbb{P}\left(\bar{E}\right)\right)^2+\mathbb{P}\left(\mathcal{E}\right)^2\right]\\
&\leq(1-e^{-\Omega(d_{\text{out}})})^2\left[\left(\mathbb{E}_{\leq N}\left|\mathbb{E}_{(w,U)\sim\mathcal{P}}\left[\mathbf{1}\{\mathcal{E}\}(\Psi_{i,w,U}-1)\right]\right|\right)^2+\mathbb{P}\left(\mathcal{E}\right)^2\right]\\
&\leq\max_t\mathbb{E}\left((1+|Z_t|)^N\right)\\
&\leq\max_t\sum_{k=0}^N\binom{N}{k}k^k\left(\frac{C\varepsilon^4\log(N)^4}{d_{\text{in}}^4d_{\text{out}}^3}\right)^{k/2}\leq\sum_{k=0}^N\left(\frac{C'N\varepsilon^2\log(N)^2}{d_{\text{in}}^2d_{\text{out}}^{1.5}}\right)^k
\end{aligned}
$$

其中我们利用了 $\binom{N}{k}\leq\frac{N^ke^k}{k^k}$ 和 $C'=\sqrt{C}e$。若 $N\log(N)^2\leq\frac{d_{\text{in}}^2d_{\text{out}}^{1.5}}{101C'\varepsilon^2}$，则右端至多为 $\sum_{k\geq0}\frac{1}{101^k}=1.01$，但左端至少为 $(1-e^{-\Omega(d_{\text{out}})})^2\left(\frac{7^2}{15^2}+\frac{9^2}{10^2}\right)\geq1.02$，其中 $d_{\text{out}}\geq$ 为 $\Omega(1)$，这就矛盾了。因此， $N\log(N)^2\geq\frac{d_{\text{in}}^2d_{\text{out}}^{1.5}}{101C'\varepsilon^2}$，最终得到：

$$
N\geq\Omega\left(\frac{d_{\text{in}}^2d_{\text{out}}^{1.5}}{\log(d_{\text{in}}d_{\text{out}}/\varepsilon)^2\varepsilon^2}\right).
$$

□

下面证明我们的断言：

引理 D.3. 设 $d_{\text{in}}\geq80$。以至少 $9/10$ 的概率，事件 $\mathcal{E}$ 成立。

证明。固定 $t\in[N]$，记 $(i,j)=(i_t,j_t)$，$X_i=B_i^\dagger A_t$ 并回忆 $|w\rangle=\frac{|u\rangle}{\||u\rangle\|_2}$，使得 u 是一个标准高斯向量。回忆事件 $\mathcal{E}$ 满足 u：

1. $\|u\|_2\geq\frac{1}{2}\sqrt{\frac{2}{3}d_{\text{in}}}$ 且

2. $\forall t\in[N]$： $P_u^t\leq\frac{(7\log($
$N^{4}))}{d_{\text{in}}^4d_{\text{out}}}$

其中 P_u^t 定义为

$$P_u^t = \sum_{i_t,j_t} \frac{\lambda_{i_t}^t \lambda_{j_t}^t}{D^2 d_{\text{out}}^2 d_{\text{in}}^4} \left(\frac{|\langle u| A_t^\dagger B_{i_t}^t B_{j_t}^{t,\dagger} A_t |u\rangle|^4}{\text{Tr}(B_{i_t}^{t,\dagger} A_t A_t^\dagger B_{i_t}^t)\text{Tr}(B_{j_t}^{t,\dagger} A_t A_t^\dagger B_{j_t}^t)} \right) = \sum_{i,j} \frac{\lambda_i \lambda_j}{D^2 d_{\text{out}}^2 d_{\text{in}}^4} \left(\frac{|\langle u| X_i^\dagger X_j |u\rangle|^4}{\|X_i\|_2^2 \|X_j\|_2^2} \right)$$

首先注意到，以高概率有 $\|u\|_2 \geq \frac{1}{2}\sqrt{\frac{2}{3}d_{\text{in}}}$。事实上，函数 $u \mapsto \|u\|_2$ 是 Lipschitz 的，因此 $\mathbb{P}\left(\|u\|_2 \leq \mathbb{E}\left(\|u\|_2\right) - s\right) \leq e^{-s^2/2}$ [Wainwright, 2019年，定理 2.26]。另一方面，根据霍尔德不等式，我们有 $\mathbb{E}\left(\|u\|_2\right) \geq \sqrt{\mathbb{E}(\|u\|_2^2)^3 \mathbb{E}(\|u\|_2^4)} = \sqrt{\frac{d_{\text{in}}^3}{d_{\text{in}}^2+2d_{\text{in}}}} \geq \sqrt{\frac{2}{3}d_{\text{in}}}$，因此

$$\mathbb{P}\left(\|u\|_2 \leq \frac{1}{2}\sqrt{\frac{2}{3}d_{\text{in}}} \right) \leq \mathbb{P}\left(\|u\|_2 - \mathbb{E}\left(\|u\|_2\right) \leq -\frac{1}{2}\sqrt{\frac{2}{3}d_{\text{in}}} \right) \leq e^{-d_{\text{in}}/32}.$$

对于事件 $\mathcal{E}$ 中的第二个条件，我们可以看到 P_u 是关于 u 的各个元素的 8 次高斯多项式。因此，我们可以使用高斯多项式的集中不等式 [Aubrun 和 Szarek，2017，推论 5.49]，；对于任意 $s > (2e)^{1/4}$，有：

$$\mathbb{P}\left(|P - \mathbb{E}\left(P\right)| \geq s\sqrt{\text{Var}(P)} \right) \leq \exp\left(-\frac{4}{e} s^{1/4} \right)$$

因此，以至少 $1 - \frac{1}{N^2}$ 的概率，有：

$$P \leq \mathbb{E}\left(P\right) + (e\log(N)/2)^4 \sqrt{\text{Var}(P)} \leq 5\log^4(N)\sqrt{\mathbb{E}\left(P^2\right)}.$$

让我们控制 $P^2 = P_u^2$ 的期望，回顾一下，我们将 $(i,j) = (i_t, j_t)$ 和 $X_i = B_i^\dagger A_t$ 记作，

$$\begin{aligned}
&\mathbb{E}\left(P^2\right) = \mathbb{E}\left[\left(\sum_{i,j} \frac{\lambda_i \lambda_j}{D^2 d_{\text{out}}^2 d_{\text{in}}^4} \left(\|X_i\|_2^{-2} \|X_j\|_2^{-2} |\langle u| X_i^\dagger X_j |u\rangle|^4 \right) \right)^2 \right] \\
&= \mathbb{E}\left[\sum_{i,j,k,l} \frac{\lambda_i \lambda_j \lambda_k \lambda_l}{D^4 d_{\text{out}}^4 d_{\text{in}}^8} \left(\|X_i\|_2^{-2} \|X_j\|_2^{-2} \|X_k\|_2^{-2} \|X_l\|_2^{-2} |\langle w| X_i^\dagger X_j |w\rangle|^4 |\langle w| X_k^\dagger X_l |w\rangle|^4 \right) \right] \mathbb{E}\left(\|u\|_2^{16}\right) \\
&\leq \sum_{i,j,k,l} \frac{\lambda_i \lambda_j \lambda_k \lambda_l}{D^4 d_{\text{out}}^4 d_{\text{in}}^8} \cdot \frac{\sum_{\alpha \in \mathfrak{S}_8} \text{Tr}_\alpha(X_i^\dagger X_j, X_j^\dagger X_i, X_i^\dagger X_j, X_j^\dagger X_i, X_k^\dagger X_l, X_l^\dagger X_k, X_k^\dagger X_l, X_l^\dagger X_k)}{(d_{\text{in}}+7)!\left[(d_{\text{in}}-1)!\right]^{-1} \|X_i\|_2^2 \|X_j\|_2^2 \|X_k\|_2^2 \|X_l\|_2^2} \cdot d_{\text{in}}^8 \\
&\leq \max_{\alpha \in \mathfrak{S}_8} \sum_{i,j,k,l} \frac{8!\,\lambda_i \lambda_j \lambda_k \lambda_l}{D^4 d_{\text{out}}^4 d_{\text{in}}^8} \cdot \frac{|\text{Tr}_\alpha(X_i^\dagger X_j, X_j^\dagger X_i, X_i^\dagger X_j, X_j^\dagger X_i, X_k^\dagger X_l, X_l^\dagger X_k, X_k^\dagger X_l, X_l^\dagger X_k)|}{\|X_i\|_2^2 \|X_j\|_2^2 \|X_k\|_2^2 \|X_l\|_2^2}
\end{aligned}$$

那么我们断言：

引理 D.4. 设 $A = X_i^\dagger X_j$ 和 $B = X_k^\dagger X_l$，则对所有 $\alpha \in \mathfrak{S}_8$，有

$$\begin{aligned}
&|\text{Tr}_\alpha(A, A^\dagger, A, A^\dagger, B, B^\dagger, B, B^\dagger)|^{1/2} \\
&\leq \max\{|\text{Tr}(A)|^4, \text{Tr}(AA^\dagger)^2\} \max\{|\text{Tr}(B)|^4, \text{Tr}(BB^\dagger)^2\} \\
&\leq \|X_i\|_2^2 \|X_j\|_2^2 \|X_k\|_2^2 \|X_l\|_2^2.
\end{aligned}$$

Sket证明的开头。证明该引理的策略取决于 α，我们可以给出一个概要 :

• 迹中只含一个元素时保持不变。

• 如果迹项中有两个连续的 A （或 B），我们用 2-范数 $\mathrm{Tr}(AA^\dagger)$ 乘以其余元素的算子范数来给这个迹取上界。然后，我们可以用 2-范数给算子范数取上界。

• 否则，迹项中会出现连续的 (A, B)（可能带有伴随）。我们可以应用柯西-施瓦茨不等式，进而得到两个连续的 A 或 B，然后应用前述策略。

例如，对于 $\alpha = (1)(5372648)$，我们有：

$$\begin{aligned}\mathrm{Tr}(A)\mathrm{Tr}(BABA^\dagger B^\dagger A^\dagger B^\dagger) &\le |\mathrm{Tr}(A)|\mathrm{Tr}(BB^\dagger)\|ABA^\dagger B^\dagger A^\dagger\|_\infty \\ &\le |\mathrm{Tr}(A)|\mathrm{Tr}(BB^\dagger)\|BB^\dagger\|_\infty\|AA^\dagger\|_\infty^{3/2} \\ &\le |\mathrm{Tr}(A)|\mathrm{Tr}(BB^\dagger)\mathrm{Tr}(BB^\dagger)\mathrm{Tr}(AA^\dagger)^{3/2} \\ &\le \max\{|\mathrm{Tr}(A)|^4, \mathrm{Tr}(AA^\dagger)^2\}\max\{|\mathrm{Tr}(B)|^4, \mathrm{Tr}(BB^\dagger)^2\}.\end{aligned}$$

另一个关于 $\alpha = (15372648)$的例子：

$$\begin{aligned}\mathrm{Tr}(ABABA^\dagger B^\dagger A^\dagger B^\dagger) &\le \mathrm{Tr}(ABABB^\dagger A^\dagger B^\dagger A^\dagger)^{1/2}\mathrm{Tr}(BABAA^\dagger B^\dagger A^\dagger B^\dagger)^{1/2} \\ &\le \mathrm{Tr}(BB^\dagger)\|AA^\dagger\|_\infty^2\|BB^\dagger\|_\infty \le \mathrm{Tr}(BB^\dagger)^2\mathrm{Tr}(AA^\dagger)^2.\end{aligned}$$

利用引理 D.4，我们有：

$$\begin{aligned}\mathbb{E}\left(P^2\right) &\le \max_{\alpha\in\mathfrak{S}_8}\sum_{i,j,k,l}\frac{8!\,\lambda_i\lambda_j\lambda_k\lambda_l}{D^4 d_{\mathrm{out}}^4 d_{\mathrm{in}}^8}\cdot\frac{|\mathrm{Tr}_\alpha(X_i^\dagger X_j, X_j^\dagger X_i, X_i^\dagger X_j, X_j^\dagger X_i, X_k^\dagger X_l, X_l^\dagger X_k, X_k^\dagger X_l, X_l^\dagger X_k)|}{\|X_i\|_2^2\|X_j\|_2^2\|X_k\|_2^2\|X_l\|_2^2} \\ &\le \max_{\alpha\in\mathfrak{S}_8}\sum_{i,j,k,l}\frac{8!\,\lambda_i\lambda_j\lambda_k\lambda_l}{D^4 d_{\mathrm{out}}^4 d_{\mathrm{in}}^8}\cdot\sqrt{|\mathrm{Tr}_\alpha(X_i^\dagger X_j, X_j^\dagger X_i, X_i^\dagger X_j, X_j^\dagger X_i, X_k^\dagger X_l, X_l^\dagger X_k, X_k^\dagger X_l, X_l^\dagger X_k)|} \\ &\le \sum_{i,j,k,l}\frac{8!\,\lambda_i\lambda_j\lambda_k\lambda_l}{D^4 d_{\mathrm{out}}^4 d_{\mathrm{in}}^8}\cdot\max\{|\mathrm{Tr}(X_i^\dagger X_j)|^2, \mathrm{Tr}(X_i^\dagger X_j X_j^\dagger X_i)\}\max\{|\mathrm{Tr}(X_k^\dagger X_l)|^2, \mathrm{Tr}(X_k^\dagger X_l X_l^\dagger X_k)\}\end{aligned}$$

所以我们 需要考虑 4 种情况，其中两种情况相似。我们定义四个指标子集 ：

$$\begin{aligned}C_1 &= \{(i,j,k,l) : |\mathrm{Tr}(X_i^\dagger X_j)|^2 > \mathrm{Tr}(X_i^\dagger X_j X_j^\dagger X_i), |\mathrm{Tr}(X_k^\dagger X_l)|^2 > \mathrm{Tr}(X_k^\dagger X_l X_l^\dagger X_k)\}, \\ C_2 &= \{(i,j,k,l) : |\mathrm{Tr}(X_i^\dagger X_j)|^2 \le \mathrm{Tr}(X_i^\dagger X_j X_j^\dagger X_i), |\mathrm{Tr}(X_k^\dagger X_l)|^2 \le \mathrm{Tr}(X_k^\dagger X_l X_l^\dagger X_k)\}, \\ C_3 &= \{(i,j,k,l) : |\mathrm{Tr}(X_i^\dagger X_j)|^2 > \mathrm{Tr}(X_i^\dagger X_j X_j^\dagger X_i), |\mathrm{Tr}(X_k^\dagger X_l)|^2 \le \mathrm{Tr}(X_k^\dagger X_l X_l^\dagger X_k)\}, \\ C_4 &= \{(i,j,k,l) : |\mathrm{Tr}(X_i^\dagger X_j)|^2 \le \mathrm{Tr}(X_i^\dagger X_j X_j^\dagger X_i), |\mathrm{Tr}(X_k^\dagger X_l)|^2 > \mathrm{Tr}(X_k^\dagger X_l X_l^\dagger X_k)\}.\end{aligned}$$

对于第一种情况，当指标 $(i、\ j、\ k、\ l) \in C_1$ 时，我们有：

$$
\begin{aligned}
&\sum_{i,j,k,l\in C_1} \frac{8!\,\lambda_i\lambda_j\lambda_k\lambda_l}{D^4 d_{\text{out}}^4 d_{\text{in}}^8} \cdot \max\{|\text{Tr}(X_i^\dagger X_j)|^2, \text{Tr}(X_i^\dagger X_j X_j^\dagger X_i)\} \max\{|\text{Tr}(X_k^\dagger X_l)|^2, \text{Tr}(X_k^\dagger X_l X_l^\dagger X_k)\} \\
&\le \sum_{i,j,k,l} \frac{8!\,\lambda_i\lambda_j\lambda_k\lambda_l}{D^4 d_{\text{out}}^4 d_{\text{in}}^8} \cdot |\text{Tr}(X_i^\dagger X_j)|^2 \text{Tr}(X_k^\dagger X_l)|^2 \\
&= \sum_{i,j,k,l} \sum_{x,y,x',y'} \frac{8!\,\lambda_i\lambda_j\lambda_k\lambda_l}{D^4 d_{\text{out}}^4 d_{\text{in}}^8} \cdot \langle x| X_i^\dagger X_j |x\rangle \langle y| X_j^\dagger X_i |y\rangle \langle x'| X_k^\dagger X_l |x'\rangle \langle y'| X_l^\dagger X_k |y'\rangle \\
&= \sum_{x,y,x',y'} \frac{8!}{D^4 d_{\text{out}}^4 d_{\text{in}}^8} \cdot d_{\text{out}}^4 \text{Tr}[\text{Tr}(A_t |x\rangle \langle y| A_t^\dagger)\mathbb{I}_{d_{\text{out}}} \text{Tr}(A_t |y\rangle \langle x| A_t^\dagger)\mathbb{I}_{d_{\text{out}}}] \\
&\qquad\qquad \cdot \text{Tr}[\text{Tr}(A_t |x'\rangle \langle y'| A_t^\dagger)\mathbb{I}_{d_{\text{out}}} \text{Tr}(A_t |y'\rangle \langle x'| A_t^\dagger)\mathbb{I}_{d_{\text{out}}}] \\
&= \sum_{x,y,x',y'} \frac{8!}{D^4 d_{\text{out}}^4 d_{\text{in}}^8} \cdot d_{\text{out}}^6 \langle y| A_t^\dagger A_t |x\rangle \langle x| A_t^\dagger A_t |y\rangle \langle y'| A_t^\dagger A_t |x'\rangle \langle x'| A_t^\dagger A_t |y'\rangle \\
&= \frac{8!}{D^4 d_{\text{out}}^4 d_{\text{in}}^8} \cdot d_{\text{out}}^6 \text{Tr}(A_t^\dagger A_t A_t^\dagger A_t)^2 \le \frac{8!}{D^4 d_{\text{out}}^4 d_{\text{in}}^8} \cdot d_{\text{out}}^6 \text{Tr}(A_t^\dagger A_t)^4 \\
&= \frac{8!}{D^4 d_{\text{out}}^4 d_{\text{in}}^8} \cdot d_{\text{out}}^6 d_{\text{in}}^4 = \frac{8!}{d_{\text{in}}^8 d_{\text{out}}^2}
\end{aligned}
$$

因为 $\sum_i \lambda_i X_i M X_i^\dagger = \sum_i \lambda_i B_i^\dagger A_t M A_t^\dagger B_i = d_{\text{out}}$迹$(A_t M A_t^\dagger)\mathbb{I}_{d_{\text{out}}}$且迹$(A_t A_t^\dagger) = d_{\text{in}}$。对于第二种情形，当指标 $(i, j, k, l) \in C_2$ 时，我们有：

$$
\begin{aligned}
&\sum_{i,j,k,l\in C_2} \frac{8!\,\lambda_i\lambda_j\lambda_k\lambda_l}{D^4 d_{\text{out}}^4 d_{\text{in}}^8} \cdot \max\{|\text{Tr}(X_i^\dagger X_j)|^2, \text{Tr}(X_i^\dagger X_j X_j^\dagger X_i)\} \max\{|\text{Tr}(X_k^\dagger X_l)|^2, \text{Tr}(X_k^\dagger X_l X_l^\dagger X_k)\} \\
&\le \sum_{i,j,k,l} \frac{\lambda_i\lambda_j\lambda_k\lambda_l}{D^4 d_{\text{out}}^4 d_{\text{in}}^8} \cdot \text{Tr}(X_i^\dagger X_j X_j^\dagger X_i) \text{Tr}(X_k^\dagger X_l X_l^\dagger X_k) \\
&= \frac{8!}{D^4 d_{\text{out}}^4 d_{\text{in}}^8} \text{Tr}(A_t A_t^\dagger)^2 \text{Tr}(\mathbb{I}) \text{Tr}(A_t A_t^\dagger)^2 \text{Tr}(\mathbb{I}) d_{\text{out}}^4 \\
&= \frac{8!}{D^4 d_{\text{out}}^4 d_{\text{in}}^8} d_{\text{in}}^4 d_{\text{out}}^6 = \frac{8!}{d_{\text{in}}^8 d_{\text{out}}^2}.
\end{aligned}
$$

对于第三种情况，当指标 $(i, j, k, l) \in C_3$ 时，我们有：

$$
\begin{aligned}
&\sum_{i,j,k,l\in C_3} \frac{8!\,\lambda_i\lambda_j\lambda_k\lambda_l}{D^4 d_{\text{out}}^4 d_{\text{in}}^8} \cdot \max\{|\text{Tr}(X_i^\dagger X_j)|^2, \text{Tr}(X_i^\dagger X_j X_j^\dagger X_i)\} \max\{|\text{Tr}(X_k^\dagger X_l)|^2, \text{Tr}(X_k^\dagger X_l X_l^\dagger X_k)\} \\
&\le \sum_{i,j,k,l} \frac{\lambda_i\lambda_j\lambda_k\lambda_l}{D^4 d_{\text{out}}^4 d_{\text{in}}^8} \cdot |\text{Tr}(X_i^\dagger X_j)|^2 \text{Tr}(X_k^\dagger X_l X_l^\dagger X_k) \\
&= \sum_{i,j,k,l} \frac{\lambda_i\lambda_j\lambda_k\lambda_l}{D^4 d_{\text{out}}^4 d_{\text{in}}^8} \cdot \sum_{x,y} \langle x| X_i^\dagger X_j |x\rangle \langle y| X_j^\dagger X_i |y\rangle \text{Tr}(X_k^\dagger X_l X_l^\dagger X_k) \\
&= \sum_{i,j,k,l} \frac{\lambda_i\lambda_j\lambda_k\lambda_l}{D^4 d_{\text{out}}^4 d_{\text{in}}^8} \cdot \sum_{x,y} d_{\text{out}}^3 \langle y| A_t^\dagger A_t |x\rangle \langle x| A_t^\dagger A_t |y\rangle d_{\text{out}}^2 \text{Tr}(A_t A_t^\dagger)^2 \text{Tr}(\mathbb{I}) \\
&\le \sum_{i,j,k,l} \frac{\lambda_i\lambda_j\lambda_k\lambda_l}{D^4 d_{\text{out}}^4 d_{\text{in}}^8} \cdot d_{\text{out}}^6 \text{Tr}(A_t A_t^\dagger)^4 = \frac{8!}{D^4 d_{\text{out}}^4 d_{\text{in}}^8} d_{\text{out}}^6 d_{\text{in}}^4 = \frac{8!}{d_{\text{in}}^8 d_{\text{out}}^2}.
\end{aligned}
$$

第四种情况中，指标 $(i,j,k,l) \in C_4$，与前一种情况类似。综上，我们有

$$\begin{aligned}\mathbb{E}\left(P^2\right) &\leq \sum_{i,j,k,l} \frac{8!\,\lambda_i\lambda_j\lambda_k\lambda_l}{D^4 d_{\text{out}}^4 d_{\text{in}}^8} \cdot \max\{|\text{Tr}(X_i^\dagger X_j)|^2, \text{Tr}(X_i^\dagger X_j X_j^\dagger X_i)\} \max\{|\text{Tr}(X_k^\dagger X_l)|^2, \text{Tr}(X_k^\dagger X_l X_l^\dagger X_k)\} \\ &\leq \frac{4\times 8!}{d_{\text{in}}^8 d_{\text{out}}^2}.\end{aligned}$$

因此，根据并合界，以至少 $1-\frac{1}{N}-e^{-d_{\text{in}}/32} \geq \frac{9}{10}$ 的概率，对所有 $t \in [N]$:

$$P_u \leq 5\log^4(N)^4\sqrt{\mathbb{E}\left(P_u^2\right)} \leq 5\log^4(N)\sqrt{\frac{4\times 8!}{d_{\text{in}}^8 d_{\text{out}}^2}} \leq \frac{(7\log(N))^4}{d_{\text{in}}^4 d_{\text{out}}}$$

并且 $\|u\|_2 \geq \sqrt{d_{\text{in}}/6}$，也就是说，事件 $\mathcal{E}$ 已满足。

□

D.2 定理 4.6 的证明

定理 D.5。对于测试恒等信道到去极化信道的任何非相干辅助系统辅助的自适应算法，在最坏情况下都需要

$$N = \Omega\left(\frac{d_{\text{in}}^2 d_{\text{out}} + d_{\text{out}}^{1.5}}{\varepsilon^2}\right)$$

次测量。

证明。我们采用与定理 4.5 的证明中相同的构造。主要地，在零假设 H_0 下，量子信道为 $\mathcal{N}(\rho) = \mathcal{D}(\rho) = \text{Tr}(\rho)\frac{\mathbb{I}}{d_{\text{out}}}$。在备择假设 H_1 下，量子信道 $\mathcal{N} \sim \mathcal{P}$ 具有如下形式:

$$\mathcal{N}(\rho) = \text{Tr}(\rho)\frac{\mathbb{I}}{d_{\text{out}}} + \frac{\varepsilon}{d_{\text{out}}}\langle w|\,\rho\,|w\rangle\, U$$

其中 $|w\rangle = W|0\rangle$ 和 $W \sim \text{Haar}(d_{\text{in}})$，且对所有 $i,j \in [d_{\text{out}}]$, $U_{j,\ i} = U_{i,\ j} \sim \mathbf{1}\{i \neq j\}\mathcal{N}_c\left(0, \sigma^2 = \frac{16}{d_{\text{out}}}\right)$，我们以事件 $\mathcal{G} = \{\|U\|_1 \geq d_{\text{out}}, \|U\|_\infty \leq 32\}$为条件。我们将此分布称为 $\mathcal{P}$，并使用记号 $(w,U) \sim \mathcal{P}$。回忆一下，$\text{P}(\mathcal{G}) \geq 1 - \text{exp}(-\Omega(d_{\text{out}})) - \text{exp}(-\Omega(d_{\text{out}}^2)$，且在 $\mathcal{G}$下，映射 $\mathcal{N}$是一个与量子信道 $\mathcal{D}$相距 ε 的有效量子信道。

现在，给定一组观测值 $i_{<t} = (i_1, \ldots, i_{t-1})$。自适应算法 $\mathcal{A}$ 会在第 t 步选择输入 $\rho_t^{i_{<t}}$和测量装置 $\mathcal{M}_t^{i_{<t}} = \left\{\lambda^{t,\ i_{<t}}_{i_t}\left|\phi^{t,\ i_{<t}}_{i_t}\right\rangle\left\langle\phi^{t,\ i_{<t}}_{i_t}\right|\right\}_{i_t \in \mathcal{I}_t}$。

在原假设 hypothesis H_0 下，量子信道 $\mathcal{N} = \mathcal{D}$，因此结果的概率恰好为:

$$\mathbb{P}_{H_0}^{I_1,\ldots,I_N} = \left\{\prod_{t=1}^N \lambda_{i_t}^{t,i_{<t}}\left\langle\phi_{i_t}^{t,i_{<t}}\right|\text{id}\otimes\mathcal{D}(\rho_t^{i_{<t}})\left|\phi_{i_t}^{t,i_{<t}}\right\rangle\right\}_{i_1,\ldots,i_N}.$$

另一方面，在 H_1 下，测量结果的概率恰好为:

$$\mathbb{P}_{H_1,(w,U)}^{I_1,\ldots,I_N} = \left\{\prod_{t=1}^N \lambda_{i_t}^{t,i_{<t}}\left\langle\phi_{i_t}^{t,i_{<t}}\right|\text{id}\otimes\mathcal{N}_{(w,U)}(\rho_t^{i_{<t}})\left|\phi_{i_t}^{t,i_{<t}}\right\rangle\right\}_{i_1,\ldots,i_N}$$

回顾一下

$$\mathcal{J}_{\mathcal{D}} = \frac{\mathbb{I}}{D} \quad \text{and} \quad \mathcal{J}_{\mathcal{N}} = \frac{\mathbb{I}}{D} + \frac{\varepsilon}{D} |w\rangle\langle w| \otimes U.$$

由于 KL散度的凸性，不失一般性地，我们可以假设每个输入态都是纯态。对于 $t \in [N]$ 和 $i_{<t}$，令 $\rho_t^{i_{<t}} = \left|\psi_t^{i_{<t}}\right\rangle\left\langle\psi_t^{i_{<t}}\right|$。此外，我们可以将每个秩一输入态和测量向量写成如下形式：

$$\left|\psi_t^{i_{<t}}\right\rangle = A_t^{i_{<t}} \otimes \mathbb{I} |\Psi_{d_{\text{in}}}\rangle \quad \text{and} \quad \left|\phi_{i_t}^{t,i_{<t}}\right\rangle = B_{i_t}^{i_{<t}} \otimes \mathbb{I} |\Psi_{d_{\text{out}}}\rangle$$

其中 $|\Psi_d\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |ii\rangle$ 以及矩阵 $A_t^{i_{<t}} \in \mathbb{C}^{d_{\text{anc}} \times d_{\text{in}}}$ 和 $B_{i_t}^{i_{<t}} \in \mathbb{C}^{d_{\text{anc}} \times d_{\text{out}}}$ 满足：

$$\text{Tr}(A_t^{i_{<t}} A_t i_{<t}, \dagger) = d_{\text{in}} \quad \text{and} \quad \text{Tr}(B_{i_t}^{i_{<t}} B_{i_t} i_{<t}, \dagger) = d_{\text{out}}.$$

注意，对于所有 t、$\sum_{i_t} \lambda^{t,}{}_{i_t}{}^{i_{<t}} B^{i_{<t},}{}_{i_t}{}^{\dagger} X B_{i_t}^{i_{<t}} = d_{\text{out}} \mathbf{Tr}(X) \mathbb{I}$，我们都有。事实上，正算子值测度 $\mathcal{M}_t$的条件意味着：

$$X \otimes \mathbb{I} = X \otimes \mathbb{I} \sum_{i_t} \lambda_{i_t}^t \left|\phi_{i_t}^t\right\rangle\left\langle\phi_{i_t}^t\right| = \sum_{i_t} \lambda_{i_t}^t X B_{i_t}^t \otimes \mathbb{I} |\Psi_{d_{\text{out}}}\rangle\langle\Psi_{d_{\text{out}}}| B_{i_t}^{t,\dagger} \otimes \mathbb{I}$$

因此，取偏迹可得

$$\text{Tr}(X)\mathbb{I} = \frac{1}{d_{\text{out}}} \sum_{i_t,i,j} \lambda_{i_t}^t \langle j| B_{i_t}^{t,\dagger} X B_{i_t}^t |i\rangle |i\rangle \langle j|.$$

最后

$$\sum_{i_t} \lambda_{i_t}^t B_{i_t}^{t,\dagger} X B_{i_t}^t = d_{\text{out}} \text{Tr}(X) \mathbb{I}.$$

现在，我们可以重新写出零假设下观测值的分布 a s:

$$\begin{aligned}
\mathbb{P}_{H_0}^{I_1,\ldots,I_N} &= \left\{ \prod_{t=1}^{N} \lambda_{i_t}^t \left\langle \phi_{i_t}^t \right| \text{id} \otimes \mathcal{D}(\rho_t) \left| \phi_{i_t}^t \right\rangle \right\}_{i_1,\ldots,i_N} \\
&= \left\{ \prod_{t=1}^{N} \lambda_{i_t}^t \langle \Psi_{d_{\text{out}}}| (B_{i_t}^{t,\dagger} A_t \otimes \mathbb{I}) \mathcal{J}_{\mathcal{D}} (A_t^\dagger B_{i_t}^t \otimes \mathbb{I}) |\Psi_{d_{\text{out}}}\rangle \right\}_{i_1,\ldots,i_N} \\
&= \left\{ \prod_{t=1}^{N} \frac{\lambda_{i_t}^t}{D} \langle \Psi_{d_{\text{out}}}| (B_{i_t}^{t,\dagger} A_t A_t^\dagger B_{i_t}^t \otimes \mathbb{I}) |\Psi_{d_{\text{out}}}\rangle \right\}_{i_1,\ldots,i_N} \\
&= \left\{ \prod_{t=1}^{N} \frac{\lambda_{i_t}^t}{D d_{\text{out}}} \text{Tr}(B_{i_t}^{t,\dagger} A_t A_t^\dagger B_{i_t}^t) \right\}_{i_1,\ldots,i_N},
\end{aligned}$$

在备择假设下为:

$$\begin{aligned}
\mathbb{P}_{H_1}^{I_1,\ldots,I_N} &= \left\{\prod_{t=1}^{N}\lambda_{i_t}^t\left\langle\phi_{i_t}^t\right|\mathrm{id}\otimes\mathcal{N}(\rho_t)\left|\phi_{i_t}^t\right\rangle\right\}_{i_1,\ldots,i_N}\\
&= \left\{\prod_{t=1}^{N}\lambda_{i_t}^t\left\langle\Psi_{d_{\mathrm{out}}}\right|(B_{i_t}^{t,\dagger}A_t\otimes\mathbb{I})\mathcal{J}_{\mathcal{N}}(A_t^\dagger B_{i_t}^t\otimes\mathbb{I})\left|\Psi_{d_{\mathrm{out}}}\right\rangle\right\}_{i_1,\ldots,i_N}\\
&= \left\{\prod_{t=1}^{N}\lambda_{i_t}^t\left\langle\Psi_{d_{\mathrm{out}}}\right|(B_{i_t}^{t,\dagger}A_t\otimes\mathbb{I})\left(\frac{\mathbb{I}}{D}+\frac{\varepsilon}{D}|w\rangle\langle w|\otimes U\right)(A_t^\dagger B_{i_t}^t\otimes\mathbb{I})\left|\Psi_{d_{\mathrm{out}}}\right\rangle\right\}_{i_1,\ldots,i_N}\\
&= \left\{\prod_{t=1}^{N}\left(\frac{\lambda_{i_t}^t}{Dd_{\mathrm{out}}}\mathrm{Tr}(B_{i_t}^{t,\dagger}A_tA_t^\dagger B_{i_t}^t)+\frac{\varepsilon\lambda_{i_t}^t}{D}\left\langle\Psi_{d_{\mathrm{out}}}\right|(B_{i_t}^{t,\dagger}A_t|w\rangle\langle w|A_t^\dagger B_{i_t}^t\otimes U)\left|\Psi_{d_{\mathrm{out}}}\right\rangle\right)\right\}_{i_1,\ldots,i_N}
\end{aligned}$$

KL 散度可以表示如下:

$$\begin{aligned}
&\mathrm{KL}\left(\mathbb{P}_{H_0}^{I_1,\ldots,I_N}\middle\|\mathbb{P}_{H_1,(w,U)}^{I_1,\ldots,I_N}\right)\\
&=\sum_{i_1,\ldots,i_N}\prod_{t=1}^{N}\frac{\lambda_{i_t}^t}{Dd_{\mathrm{out}}}\mathrm{Tr}(B_{i_t}^{t,\dagger}A_tA_t^\dagger B_{i_t}^t)\\
&\qquad\times\log\left(\frac{\prod_{t=1}^{N}\frac{\lambda_{i_t}^t}{Dd_{\mathrm{out}}}\mathrm{Tr}(B_{i_t}^{t,\dagger}A_tA_t^\dagger B_{i_t}^t)}{\prod_{t=1}^{N}\left(\frac{\lambda_{i_t}^t}{Dd_{\mathrm{out}}}\mathrm{Tr}(B_{i_t}^{t,\dagger}A_tA_t^\dagger B_{i_t}^t)+\frac{\varepsilon\lambda_{i_t}^t}{D}\left\langle\Psi_{d_{\mathrm{out}}}\right|(B_{i_t}^{t,\dagger}A_t|w\rangle\langle w|A_t^\dagger B_{i_t}^t\otimes U)\left|\Psi_{d_{\mathrm{out}}}\right\rangle\right)}\right)\\
&=\sum_{t=1}^{N}\mathbb{E}_{\le N}(-\log)\left(1+\frac{\frac{\varepsilon\lambda_{i_t}^t}{D}\left\langle\Psi_{d_{\mathrm{out}}}\right|(B_{i_t}^{t,\dagger}A_t|w\rangle\langle w|A_t^\dagger B_{i_t}^t\otimes U)\left|\Psi_{d_{\mathrm{out}}}\right\rangle}{\frac{\lambda_{i_t}^t}{Dd_{\mathrm{out}}}\mathrm{Tr}(B_{i_t}^{t,\dagger}A_tA_t^\dagger B_{i_t}^t)}\right)\\
&=\sum_{t=1}^{N}\mathbb{E}_{\le N}(-\log)\left(1+\varepsilon\frac{\mathrm{Tr}((B_{i_t}^{t,\dagger}A_t|w\rangle\langle w|A_t^\dagger B_{i_t}^t U))}{\mathrm{Tr}(B_{i_t}^{t,\dagger}A_tA_t^\dagger B_{i_t}^t)}\right)
\end{aligned}$$

其中我们使用记号 $\mathbb{E}_{\le N}(X(i_1,\ldots,i_N))=\sum_{i_1,\ldots,i_N}\left(\prod_{t=1}^{N}\frac{\lambda_{i_t}^t}{Dd_{\mathrm{out}}}\mathrm{Tr}(B^t{}_{,i_t}{}^\dagger A_tA_t^\dagger B_{i_t}^t)\right)X(i_1,\ldots,i_N)$。利用不等式 $(-\log(1+x))\le -x+x^2$ 对 $x\ge -1/2$ 成立，且由于对于 $\varepsilon\le 64$，我们有$\varepsilon\,\mathrm{Tr}((B^t{}_{,i_t}{}^\dagger A_t|w\rangle\langle w|A_t^\dagger B_{i_t}^t U))\,\mathrm{Tr}(B^t{}_{,i_t}{}^\dagger A_tA_t^\dagger B_{i_t}^t)\ge -1/2$，因此可将前面的被积函数上界估计如下:

$$\begin{aligned}
&(-\log)\left(1+\varepsilon\frac{\mathrm{Tr}((B_{i_t}^{t,\dagger}A_t|w\rangle\langle w|A_t^\dagger B_{i_t}^t U))}{\mathrm{Tr}(B_{i_t}^{t,\dagger}A_tA_t^\dagger B_{i_t}^t)}\right)\\
&\le\varepsilon\frac{\mathrm{Tr}((B_{i_t}^{t,\dagger}A_t|w\rangle\langle w|A_t^\dagger B_{i_t}^t U))}{\mathrm{Tr}(B_{i_t}^{t,\dagger}A_tA_t^\dagger B_{i_t}^t)}+\varepsilon^2\frac{\mathrm{Tr}((B_{i_t}^{t,\dagger}A_t|w\rangle\langle w|A_t^\dagger B_{i_t}^t U))^2}{\mathrm{Tr}(B_{i_t}^{t,\dagger}A_tA_t^\dagger B_{i_t}^t)^2}.
\end{aligned}$$

注意，第一项在取期望后消失：

$$\begin{aligned}
&\mathbb{E}_{\le N}\left(\varepsilon\frac{\mathrm{Tr}((B_{i_t}^{t,\dagger}A_t\left|w\right\rangle\!\left\langle w\right|A_t^\dagger B_{i_t}^t U))}{\mathrm{Tr}(B_{i_t}^{t,\dagger}A_tA_t^\dagger B_{i_t}^t)}\right)\\
&=\mathbb{E}_{\le t-1}\sum_{i_t}\frac{\lambda_{i_t}^t}{Dd_{\mathrm{out}}}\mathrm{Tr}(B_{i_t}^{t,\dagger}A_tA_t^\dagger B_{i_t}^t)\cdot\varepsilon\frac{\mathrm{Tr}((B_{i_t}^{t,\dagger}A_t\left|w\right\rangle\!\left\langle w\right|A_t^\dagger B_{i_t}^t U))}{\mathrm{Tr}(B_{i_t}^{t,\dagger}A_tA_t^\dagger B_{i_t}^t)}\\
&=\mathbb{E}_{\le t-1}\sum_{i_t}\frac{\lambda_{i_t}^t}{Dd_{\mathrm{out}}}\cdot\varepsilon\mathrm{Tr}((B_{i_t}^{t,\dagger}A_t\left|w\right\rangle\!\left\langle w\right|A_t^\dagger B_{i_t}^t U))\\
&=\mathbb{E}_{\le t-1}\frac{\varepsilon}{D}\mathrm{Tr}(A_t\left|w\right\rangle\!\left\langle w\right|A_t^\dagger)\mathrm{Tr}(U)=0
\end{aligned}$$

其中我们使用了 $\sum_{i_t}\lambda_{i_t}^t B^{t,\ }_{i_t}{}^{\dagger}XB_{i_t}^t=d_{\mathrm{out}}\mathbf{Tr}(X)\mathbb{I}$. 对于第二项，我们将改为求其在 U 下期望的上界。注意到该项非负，因此可以安全地去掉事件 $\mathcal{G}$ 上的条件，然后计算 Haar 分布向量 w 和高斯随机变量 $\{U_{i,j}\}$下的期望。

$$\begin{aligned}
\mathbb{E}\left(\varepsilon^2\frac{\mathrm{Tr}((B_{i_t}^{t,\dagger}A_t\left|w\right\rangle\!\left\langle w\right|A_t^\dagger B_{i_t}^t U))^2}{\mathrm{Tr}(B_{i_t}^{t,\dagger}A_tA_t^\dagger B_{i_t}^t)^2}\right)&\le\frac{32}{d_{\mathrm{out}}}\varepsilon^2\mathbb{E}\left(\frac{\left\langle w\right|A_t^\dagger B_{i_t}^tB_{i_t}^{t,\dagger}A_t\left|w\right\rangle^2}{\mathrm{Tr}(B_{i_t}^{t,\dagger}A_tA_t^\dagger B_{i_t}^t)^2}\right)\\
&\le\frac{64\varepsilon^2}{d_{\mathrm{out}}d_{\mathrm{in}}^2}\cdot\frac{\mathrm{Tr}(A_t^\dagger B_{i_t}^tB_{i_t}^{t,\dagger}A_t)^2}{\mathrm{Tr}(B_{i_t}^{t,\dagger}A_tA_t^\dagger B_{i_t}^t)^2}=\frac{64\varepsilon^2}{d_{\mathrm{in}}^2d_{\mathrm{out}}}.
\end{aligned}$$

因此

$$\begin{aligned}
\mathbb{E}_{(w,U)\sim\mathcal{P}}\mathrm{KL}\left(\mathbb{P}_{H_0}^{I_1,\dots,I_N}\middle\|\mathbb{P}_{H_1,(w,U)}^{I_1,\dots,I_N}\right)&\le\sum_{t=1}^N\mathbb{E}_{\le N}\mathbb{E}_{(w,U)\sim\mathcal{P}}(-\log)\left(1+\varepsilon\frac{\mathrm{Tr}((B_{i_t}^{t,\dagger}A_t\left|w\right\rangle\!\left\langle w\right|A_t^\dagger B_{i_t}^t U))}{\mathrm{Tr}(B_{i_t}^{t,\dagger}A_tA_t^\dagger B_{i_t}^t)}\right)\\
&\le\sum_{t=1}^N\mathbb{E}_{\le N}\frac{64\varepsilon^2}{d_{\mathrm{in}}^2d_{\mathrm{out}}}=\frac{64N\varepsilon^2}{d_{\mathrm{in}}^2d_{\mathrm{out}}}.
\end{aligned}$$

另一方面，将数据处理不等式应用于 KL 散度（见命题 F.3）可得：

$$\begin{aligned}
\mathbb{E}_{(w,U)\sim\mathcal{P}}\mathrm{KL}\left(\mathbb{P}_{H_0}^{I_1,\dots,I_N}\middle\|\mathbb{P}_{H_1,(w,U)}^{I_1,\dots,I_N}\right)&\ge\mathbb{E}_{(w,U)\sim\mathcal{P}}\mathrm{KL}(\mathbb{P}_{H_0}(\mathcal{A}=0)\,\|\mathbb{P}_{H_1,(w,U)}(\mathcal{A}=0))\\
&\ge\mathrm{KL}(2/3\|1/3)=\frac{2}{3}\log(2)-\frac{1}{3}\log(2)=\frac{1}{3}\log(2).
\end{aligned}$$

将 KL 散度的下界和上界合并：

$$\frac{128N\varepsilon^2}{d_{\mathrm{in}}^2d_{\mathrm{out}}}\ge\mathbb{E}_{(w,U)\sim\mathcal{P}}\mathrm{KL}\left(\mathbb{P}_{H_0}^{I_1,\dots,I_N}\middle\|\mathbb{P}_{H_1,(w,U)}^{I_1,\dots,I_N}\right)\ge\frac{1}{3}\log(2)$$

由此得到下界：

$$N=\Omega\left(\frac{d_{\mathrm{in}}^2d_{\mathrm{out}}}{\varepsilon^2}\right).$$

□

量子态的 E 测试恒等式

本节将说明如何把量子态检验化归为离散分布检验。Chen 等人，2022a]给出了相同的结果，但证明方法不同。对于正算子值测度 $\mathcal{M}$ 和量子态 ρ，令$\rho(\mathcal{M})$ 表示经典概率分布 $\{\mathrm{Tr}(\rho M_i)\}_i$。以下引理概括了这一化归的主要要点：

引理 E.1. 对于所有 $\delta > 0$，令 $l = \frac{1}{4}\log(2/\delta)$，且令 U^1、U^2、...、$U^l \in \mathbb{C}^{d\times d}$ 为列数为 $\left\{\left|U_i^j\right\rangle\right\}_{1\le i\le d,\ 1\le j\le l}$、$\mathcal{M} = \left\{\frac{1}{l}\left|U_i^j\right\rangle\left\langle U_i^j\right|\right\}_{i,\ j}$ 的 Haar 随机酉矩阵，则其构成一个正算子值测度，并且对于所有量子态 ρ 和 σ，以至少 $1-\delta$ 的概率有：

$$\mathrm{TV}(\rho(\mathcal{M}),\sigma(\mathcal{M})) \ge \frac{\|\rho - \mathbb{I}/d\|_2}{20}.$$

在 [Matthews 等人的文献 2009] 中可以找到类似的论述，其中作者分析了均匀 POVM 以及由球面 4-设计定义的 POVM。然而，对于我们的归约而言，尽量减少 POVM 的测量结果数量十分重要。

证明。令 $\xi = \rho - \sigma$，我们有 $U|e_i\rangle = |U_i\rangle$ 并使用 Weingarten演算 F.1 和 F.2 进行计算 e

$$\begin{aligned}
\mathbb{E}\left[\langle U_i|\xi|U_i\rangle^2\right] &= \mathbb{E}\left[\langle U_i|\xi|U_i\rangle\langle U_i|\xi|U_i\rangle\right] = \mathbb{E}\left[\mathrm{Tr}(\xi|U_i\rangle\langle U_i|\xi|U_i\rangle\langle U_i|)\right] \\
&= \mathbb{E}\left[\mathrm{Tr}(\xi U|e_i\rangle\langle e_i|U^*\xi U|e_i\rangle\langle e_i|U^*)\right] = \mathbb{E}\left[\mathrm{Tr}(U^*\xi U|e_i\rangle\langle e_i|U^*\xi U|e_i\rangle\langle e_i|)\right] \\
&= \sum_{\alpha,\beta\in\mathcal{S}_2}\mathrm{Wg}(\beta\alpha^{-1},d)\mathrm{Tr}_{\beta^{-1}}(\xi,\xi)\mathrm{Tr}_\alpha(|e_i\rangle\langle e_i|,|e_i\rangle\langle e_i|) = \frac{1}{d(d+1)}\mathrm{Tr}(\xi^2).
\end{aligned}$$

类似地

$$\begin{aligned}
\mathbb{E}\left[\langle U_i|\xi|U_i\rangle^4\right] &= \mathbb{E}\left[\langle U_i|\xi|U_i\rangle\langle U_i|\xi|U_i\rangle\langle U_i|\xi|U_i\rangle\langle U_i|\xi|U_i\rangle\right] \\
&= \mathbb{E}\left[\mathrm{Tr}(\xi|U_i\rangle\langle U_i|\xi|U_i\rangle\langle U_i|\xi|U_i\rangle\langle U_i|\xi|U_i\rangle\langle U_i|)\right] \\
&= \mathbb{E}\left[\mathrm{Tr}(\xi U|e_i\rangle\langle e_i|U^*\xi U|e_i\rangle\langle e_i|U^*\xi U|e_i\rangle\langle e_i|U^*\xi U|e_i\rangle\langle e_i|U^*)\right] \\
&= \mathbb{E}\left[\mathrm{Tr}(U^*\xi U|e_i\rangle\langle e_i|U^*\xi U|e_i\rangle\langle e_i|U^*\xi U|e_i\rangle\langle e_i|U^*\xi U|e_i\rangle\langle e_i|)\right] \\
&= \sum_{\alpha,\beta\in\mathfrak{S}_4}\mathrm{Wg}(\beta\alpha^{-1},d)\mathrm{Tr}_{\beta^{-1}}(\xi,\xi,\xi,\xi)\mathrm{Tr}_\alpha(|e_i\rangle\langle e_i|,|e_i\rangle\langle e_i|,|e_i\rangle\langle e_i|,|e_i\rangle\langle e_i|) \\
&= \frac{1}{d(d+1)(d+2)(d+3)}(6\mathrm{Tr}(\xi^2)^2 + 6\mathrm{Tr}(\xi^4)). \\
&\le \frac{c'}{d(d+1)(d+2)(d+3)}\mathrm{Tr}(\xi^2)^2.
\end{aligned}$$

现在我们可以通过霍尔德不等式得出结论：

$$\begin{aligned}
2\mathbb{E}\left[\mathrm{TV}(\rho(\mathcal{M}),\sigma(\mathcal{M}))\right] &= \sum_{i=1}^d \mathbb{E}\left[|\langle U_i|\xi|U_i\rangle|\right] \ge \sum_{i=1}^d \sqrt{\frac{\left(\mathbb{E}\left[\langle U_i|\xi|U_i\rangle^2\right]\right)^3}{\mathbb{E}\left[\langle U_i|\xi|U_i\rangle^4\right]}} \\
&\ge \sum_{i=1}^d \sqrt{\frac{(d^{-1}(d+1)^{-1}\mathrm{Tr}(\xi^2))^3}{c'd^{-1}(d+1)^{-1}(d+2)^{-1}(d+3)^{-1}\mathrm{Tr}(\xi^2)^2}} \\
&\ge \sum_{i=1}^d c\frac{\sqrt{\mathrm{Tr}(\xi^2)}}{d} \ge c\sqrt{\mathrm{Tr}(\rho-\sigma)^2}.
\end{aligned}$$

设 $f(U) = \mathrm{TV}(\rho(\mathcal{M}), \sigma(\mathcal{M}))$，我们首先利用三角不等式和柯西-施瓦茨不等式证明 f 是利普希茨连续的：

$$\begin{aligned}
2|f(U) - f(V)| &= \left| \sum_{1\le i\le d, 1\le j\le l} \frac{1}{l} |\mathrm{Tr}(\left|U_i^j\right\rangle\left\langle U_i^j\right| \xi)| - |\mathrm{Tr}(\left|V_i^j\right\rangle\left\langle V_i^j\right| \xi)| \right| \\
&\le \sum_{1\le i\le d, 1\le j\le l} \frac{1}{l} \left| \mathrm{Tr}((\left|U_i^j\right\rangle\left\langle U_i^j\right| - \left|V_i^j\right\rangle\left\langle V_i^j\right|)\xi) \right| \\
&\le \sum_{1\le i\le d, 1\le j\le l} \frac{1}{l} \sqrt{\mathrm{Tr}(\xi^2)} \sqrt{\mathrm{Tr}((\left|U_i^j\right\rangle\left\langle U_i^j\right| - \left|V_i^j\right\rangle\left\langle V_i^j\right|)^2)} \\
&\le \sqrt{\frac{d}{l}} \sqrt{\mathrm{Tr}(\xi^2)} \sqrt{\sum_{1\le i\le d, 1\le j\le l} \mathrm{Tr}((\left|U_i^j\right\rangle\left\langle U_i^j\right| - \left|V_i^j\right\rangle\left\langle V_i^j\right|)^2)} \\
&\le \sqrt{\frac{d}{l}} \sqrt{\mathrm{Tr}(\xi^2)} \sqrt{\sum_{1\le j\le l} \mathrm{Tr}((U^j - V^j)^2)} \\
&\le \sqrt{\frac{d}{l}} \sqrt{\mathrm{Tr}(\xi^2)} \|U - V\|_{2,\mathrm{HS}},
\end{aligned}$$

因此，f 是 $L = \sqrt{\frac{d}{2l}}\sqrt{\mathrm{Tr}(\xi^2)}$-Lipschitz 函数，由定理 F.4 可得：

$$\mathbb{P}\left(|f(U) - \mathbb{E}\left(f(U)\right)| > \frac{c}{2}\sqrt{\mathrm{Tr}(\xi^2)}\right) \le e^{-\frac{dc^2\mathrm{Tr}(\xi^2)}{48L^2}} = e^{-lc^2/24} = \delta/2,$$

对于 $l = 24\log(2/\delta)/c^2$。最后，以高概率（至少 $1-\delta/2$），我们有

$$\begin{aligned}
\mathrm{TV}(\rho(\mathcal{M}), \sigma(\mathcal{M})) &\ge \mathbb{E}\left(\mathrm{TV}(\rho(\mathcal{M}), \sigma(\mathcal{M}))\right) - |\mathrm{TV}(\rho(\mathcal{M}), \sigma(\mathcal{M})) - \mathbb{E}\left(\mathrm{TV}(\rho(\mathcal{M}), \sigma(\mathcal{M}))\right)| \\
&\ge c\sqrt{\mathrm{Tr}(\xi^2)} - \frac{c}{2}\sqrt{\mathrm{Tr}(\xi^2)} \ge \frac{c}{2}\sqrt{\mathrm{Tr}(\xi^2)}.
\end{aligned}$$

□

设 $\eta = \|\rho - \mathbb{I}/d\|_2$。在备择假设 H_2 下，P 与 U_n 之间的全变差距离下界为 $\mathrm{TV}(P, U_n) \ge \frac{1}{20}\|\rho - \mathbb{I}/d\|_2$。因此，引理 E.1 给出了一个正算子值测度，使我们的问题归约为恒等性检验：$P = U_n$ 与 $\mathrm{TV}(P, U_n) \ge \frac{\eta}{20}$，且该结论以高概率成立，其中 $n = \frac{1}{4}d\log(2/\delta)$ 且 $P = \mathcal{M}(\rho)$。因此，我们可以应用 Diakonikolas 等人的经典均匀性检验结果 [Diakonikolas et al., 2017]，得到副本复杂度：

$$\mathcal{O}\left(\frac{\sqrt{d}\log(1/\delta)}{\eta^2}\right).$$

F 技术引理

本节汇总了对本文前述证明有用的技术引理。

算法 3：在 2-范数下进行量子态恒等性检验，使错误概率至多为 δ。

$l = \frac{1}{4}\log(2/\delta)$. 从 Haar($d$) 分布中抽取样本 $U^1, U^2, \ldots, U^l \in \mathbb{C}^{d\times d}$。令 $\left\{\left|U_i^j\right\rangle\right\}_{1\le i\le d, 1\le j\le l}$ 为酉矩阵 $U^1, U^2, \ldots, U^l$ 的列。使用正算子值测度 $\mathcal{M} = \left\{\frac{1}{l}\left|U_i^j\right\rangle\left\langle U_i^j\right|\right\}_{i,j}$测量量子态 ρ，并从 $\rho(\mathcal{M})$ 中观测到$\mathcal{O}\left(\sqrt{d}\log(1/\delta)/\eta^2\right)$ 个样本。使用 Diakonikolas 等人提出的离散分布恒等性检验，检验是 h_0：$\rho(\mathcal{M}) = U_{ld}$ 还是 h_1 : TV($\rho(\mathcal{M})$ U_{ld}) $\ge \eta/20$，错误概率为 δ，并据此作答。

F.1 Weingarten演算

由于我们通常使用均匀 POVM，它由对 Haar 酉矩阵进行采样构成，因此我们需要了解一些 Weingarten演算的事实，以便计算 Haar 酉积分。若 π a 是 $[n]$的一个排列，则 Wg(π, d) 表示维数为 d的 Weingarten 函数。以下引理对我们的结果至关重要。

引理 F.1. *[*Gu, *2013]* 设 U 是一个服从 Haar 分布的 $d \times d$ 酉矩阵，且 $\{A_i, B_i\}_i$ 是由$d \times d$ 复矩阵构成的序列。我们有以下公式

$$\begin{aligned}&\mathbb{E}\left(\mathrm{Tr}(UB_1U^*A_1U\ldots UB_nU^*A_n)\right)\\&= \sum_{\alpha,\beta\in\mathfrak{S}_n} \mathrm{Wg}(\beta\alpha^{-1}, d)\mathrm{Tr}_{\beta^{-1}}(B_1, \ldots, B_n)\mathrm{Tr}_{\alpha\gamma_n}(A_1, \ldots, A_n),\end{aligned}$$

其中 $\gamma_n =$(12 . . . n) 和 Tr$\sigma(M_1, \ldots, M_n)$ $= \Pi_j$Tr($\Pi_{i\in C_j} M_i$)，对于 $\sigma = \Pi_j C_j$和 C_j是循环。

我们还需要 Weingarten 函数的一些取值:

引理 F.2. • Wg((1) d) $= \frac{1}{d}$,

- $\mathrm{Wg}((12), d) = \frac{-1}{d(d^2-1)}$,
- $\mathrm{Wg}((1)(2), d) = \frac{1}{d^2-1}$,
- $\mathrm{Wg}((123), d) = \frac{2}{d(d^2-1)(d^2-4)}$,
- $\mathrm{Wg}((12)(3), d) = \frac{-1}{(d^2-1)(d^2-4)}$,
- $\mathrm{Wg}((1)(2)(3), d) = \frac{d^2-2}{d(d^2-1)(d^2-4)}$.

特别是，已知 Weingarten 函数的和有一个闭式表达:

引理 F.3。 *[*Collins 等人, *2012]* 令 d、 $k \in \mathbb{N}^*$。我们有

$$\sum_{\alpha\in\mathfrak{S}_k} \mathrm{Wg}(\alpha, d) = \frac{1}{d(d+1)\cdots(d+k-1)}.$$

F.2 Haar 随机酉矩阵的集中不等式

以下集中不等式对我们的结果至关重要。

定理 F.4. *[*Meckes 等人， *2013]* 设 $M = \mathbb{U}(d)^k$ 配备 Hilbert–Schmidt 度量的 L_2-范数。若F：$M \to \mathbb{R}$是 L-Lipschitz 的，则对于任意 $t > 0$

$$\mathbb{P}\left(|F(U_1, \ldots, U_k) - \mathbb{E}\left(F(U_1, \ldots, U_k)\right)| \geq t\right) \leq e^{-dt^2/12L^2},$$

其中 U_1、.....、 U_k 是相互独立且服从 Haar 分布的酉矩阵。

F.3 Kullback–Leibler散度

定义 F.5（Kullback–Leibler散度）。对于分布 P和 Q，其定义在 $[d]$ 上，Kullback–Leibler散度定义为

$$\mathrm{KL}(P\|Q) = \sum_{i=1}^{d} P_i \log\left(\frac{P_i}{Q_i}\right) .$$

我们将 KL($p\|q$) = KL(伯努利分布(p)||伯努利分布(q)) 记为。

Kullback-Leibler 散度是非负的，并满足数据处理性质：

命题 F.6（[Van Erven 和 Harremos， 2014]）。设 P、 P'、 Q和 Q'是 $[d]$上的概率分布，则有

- 非负性 KL($P\|Q$) ≥ 0。
- 数据处理 设 X 是一个随机变量， g 是一个函数。定义随机变量 $Y = g(X)$，则有

$$\mathrm{KL}\left(P^X\|Q^X\right) \geq \mathrm{KL}\left(P^Y\|Q^Y\right).$$