无限单向导引

Pavel Sekatski, [1], * Florian Giraud, [1] Roope Uola, [1] 和 Nicolas Brunner[1]
[1] *Department of Applied Physics, University of Geneva, Switzerland*

本研究探讨了在采用高维纠缠的方案中量子操控的不对称性。我们构造了具有以下性质的纠缠态：(*i*) 考虑最一般的测量时，一方（Alice）始终无法操控另一方（Bob）的量子态；(*ii*) Bob 则能强力操控 Alice 的量子态，展现出真正的高维操控。换言之，Bob 可以让 Alice 相信他们共享的纠缠态具有任意高的施密特数，而 Alice 却始终无法让 Bob 相信该量子态甚至是纠缠态。从这个意义上说，单向导引可以变得不受限制。我们构造中的一项关键结果，是给出了一个关于所有高维测量在噪声和损耗共同作用下的联合可测性条件；这一结果本身也具有独立意义。

arXiv:2304.03888v1 [quant-ph] 8 Apr 2023

I. 引言

非定域性是量子理论的核心特征之一。这种效应体现在不同层面。一方面，它通过纠缠[1, 2]这一概念，体现在理论的数学结构（即希尔伯特空间）中。另一方面，对纠缠态进行局域测量所得到的测量统计可能呈现出强烈的非定域关联，这与任何局域模型都不相容 [3]。起初，人们认为纠缠与量子贝尔非定域性是同一现象的两个方面；如今已明确，它们实际上本质不同，参见例如 [4, 5]。

量子非定域性的另一种视角来自量子操控这一概念，综述见 [6, 7] 。这种效应由 Wiseman、Jones 和 Doherty [8], 加以形式化，其根源可追溯至 Einstein- Podolsky-Rosen [9]和 Schr¨odinger [10, 11]的早期研究。在此，未受信任的一方（Bob）希望说服另一方（Alice），使其相信双方共享一个纠缠态。Bob 展示自己能够通过不同测量基远程操控 Alice 的局域量子态，便能说服 Alice。因此，操控本质上是一项不对称任务，这与纠缠和贝尔非定域性不同。

有趣的是，操控的不对称性在量子态层面也有所体现。具体而言，存在一些纠缠态，可以实现从 Bob 到 Alice 的导引，却无法实现反方向的导引 [12]；Bob 能让 Alice 相信共享态是纠缠态，而 Alice 却永远无法说服 Bob，即使她使用所有可能的局域测量也是如此。这种现象被称为“单向导引”，近年来受到广泛关注，相关例子包括低维系统（主要是双量子比特） [12–17]、连续变量高斯系统 [18, 19] 以及实验演示，参见例如 [20–23]。

一个相关问题是，是否存在不同形式的单向导引，以及其中某些形式是否比其他形式更强。迄今为止，由于缺乏适用于这一情境的恰当操控测度，这个问题尚未得到讨论。在此，我们借助近期提出的真正高维操控概念 [24]，（另见 [25, 26]），着手解决这一问题。该概念使我们能够对操控进行维数方面的量化，具体而言，可为操控情景中纠缠态的施密特数给出下界。接着，我们探讨是否存在具有以下性质的纠缠态：(i) Alice 无法操控 Bob 的量子态（即使允许使用所有可能的局域测量）；(ii) Bob 能够强力操控 Alice 的量子态，也就是说，确保存在高维纠缠（施密特数至少为 d）。我们构造了一族具有上述两种性质的纠缠态，证明这个问题的答案是肯定的；对于任意有限维数 d，该族纠缠态的维数为 $d\times(d+1)$。为此，我们利用操控与测量不相容性之间的联系 [27–30], ，以及这一联系近期在高维操控方面的推广 [31]，并运用测量的 n-可模拟性概念 [32]。值得注意的是，我们给出了一个充分条件，用以判定在噪声与损耗的共同作用下，所有 POVM 构成的集合是否具有联合可测性。

II. 问题与主要结果

我们考虑这样一种情形：两位相距遥远的参与方 Alice 和 Bob 共享一个纠缠态 ϱ_{AB}。双方各自进行局域测量，这些测量由正算子值测度（POVM）集合表示。具体而言，Alice 的测量由一组 POVM $\{A_{a|x}\}$ 描述，其中 x 表示测量选项，a 表示测量结果，并满足以下性质：$A_{a|x}\geq 0$ 和 $\sum_a A_{a|x}=\mathbb{1}$，对所有 a 和 x 均成立。类似地，我们将 Bob 的 POVM 集合定义为 $\{B_{b|y}\}$。

由于共享态是纠缠的，各方局域测量的效果是远程制备（操控）另一方的量子态。这通过两个所谓的态组装来描述：$\{\sigma^A_{b|y}\}$ 描述在给定 Bob 的测量结果时 Alice 系统的量子态，而 $\{\sigma^B_{a|x}\}$描述在给定 Alice 的测量结果时 Bob 的量子态。这些态组装

* pavel.sekatski@unige.ch

由下式给出

$$\sigma^A_{b|y} = \mathrm{tr}_B[(\mathbb{1}\otimes B_{b|y})\varrho_{AB}]\,, \tag{1}$$
$$\sigma^B_{a|x} = \mathrm{tr}_A[(A_{a|x}\otimes \mathbb{1})\varrho_{AB}]\,. \tag{2}$$

我们在此探讨的核心问题是，这两个态组装之间可能存在多大差异，换言之，操控的效果可能有多不对称。粗略地说，我们要寻找一种纠缠态 ϱ_{AB}，使得其中一个态组装（比如 $\{\sigma^A_{b|y}\}$）是经典的（即绝不会导致操控），而另一个态组装 $\{\sigma^B_{a|x}\}$ 则高度非经典（即表现出强烈操控，能够证明其具有很高的纠缠维数）。

在更精确地定义问题之前，我们先指出，我们要寻找的是具有高维且不对称的某些纠缠态。显然，如果量子态 ϱ_{AB} 在交换 Alice 和 Bob 后保持对称，那么沿一个方向可获得的任意系综，也可以沿相反方向获得。此外，量子态 ϱ_{AB} 应具有较高的纠缠维数，这里通过施密特数 [33, 34]来量化：量子态 ϱ_{AB} 的施密特数是满足以下条件的最小值 n：存在一种分解$\varrho_{AB} = \sum_j p_j \left|\psi_j\right\rangle\left\langle\psi_j\right|$，其中所有 $\left|\psi_j\right\rangle$ 都是施密特秩至多为 n 的纯纠缠态。

更正式地说，我们要寻找满足以下两个性质的纠缠态：

1. The assemblage $\{\sigma^A_{b|y}\}$ admits a local hidden state (LHS) model [8]:

$$\sigma^A_{b|y} = p(b|y)\sum_\lambda p(\lambda|b,y)\sigma_\lambda \quad \forall b,y\,. \tag{3}$$

重要的是，对于 Bob 的任意一组测量，这一结论都应成立 $\{B_{b|y}\}$。因此，不可能发生从 Bob 到 Alice 的操控，这意味着 Bob 永远无法让 Alice 相信共享态 ϱ_{AB} 是纠缠态。

2. 系综 $\{\sigma^B_{a|x}\}$不能由（$d-1$）预备 [24]，即

$$\sigma^B_{a|x} \neq \sum_\lambda p(\lambda)\mathrm{tr}_A[(M^\lambda_{a|x}\otimes\mathbb{1})\rho^\lambda_{AB}] \tag{4}$$

其中，p（λ）是任意概率分布，$M^\lambda_{a|x}$ 是（在 $\mathbb{C}^d$中的）任意测量，并且所有 ρ^λ_{AB}都是施密特数至多为 $d-1$的任意量子态。因此，这证明了真正的 d 维操控，因而 Alice 可以让 Bob 相信共享态 ϱ_{AB} 具有较大的施密特数 d。简而言之，我们称 ϱ_{AB} 是 d-可操控的。

下文中，对于任意 d，我们将构造一族具有上述两种性质、维数为 $d\times(d+1)$ 的纠缠态。这表明，单向导引可以变得无限，即达到最大程度的不对称。具体而言，我们从一个最大纠缠的双量子位态$\left|\phi^+_d\right\rangle = \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\left|k,k\right\rangle$（记作 $\Phi^+_d = \left|\phi^+_d\right\rangle\!\left\langle\phi^+_d\right|$）出发，依次施加白噪声（退极化）信道和损失信道，其定义如下：

$$\mathcal{W}_p : \rho \mapsto p\,\rho + (1-p)\mathrm{tr}[\rho]\frac{\mathbb{1}_d}{d}\,, \tag{5}$$
$$\mathcal{L}_\eta : \rho \mapsto \eta\,\rho + (1-\eta)\mathrm{tr}[\rho]\left|\,\text{ø}\,\right\rangle\!\left\langle\,\text{ø}\,\right|. \tag{6}$$

退极化（损耗）信道以概率 $1-p$ $(1-\eta)$ 将原始量子态替换为最大混合态（真空态 $\left|\,\text{ø}\,\right\rangle\!\left\langle\,\text{ø}\,\right|$）。注意，真空态表示一个与输入希尔伯特空间正交的附加“能级”，因此输出态的维数为 $d+1$。经过这两个信道后，我们得到最终态

$$\begin{aligned}\varrho^{(\eta,p)}_{AB} &= \mathrm{id}\otimes(\mathcal{L}_\eta\circ\mathcal{W}_p)[\Phi^+] \\ &= \eta p\,\Phi^+_d + \eta(1-p)\frac{\mathbb{1}_d\otimes\mathbb{1}_d}{d^2} + (1-\eta)\frac{\mathbb{1}_d}{d}\otimes\left|\,\text{ø}\,\right\rangle\!\left\langle\,\text{ø}\,\right|,\end{aligned} \tag{7}$$

其维数为 $d\times(d+1)$。

结果 1。 量子态 $\varrho^{(\eta,p)}_{AB}$ 在公式 (7) 中定义，满足以下性质

(i) $\varrho^{(\eta,p)}_{AB}$ *is d-steerable from Alice to Bob if*

$$p > \frac{d\sqrt{\frac{d}{d+1}}-1}{d-1}. \tag{8}$$

(ii) $\varrho^{(\eta,p)}_{AB}$ 在从 *Bob* 到 *Alice* 的方向上不可操控，当且仅当

$$\eta \leq (1-p)^{d-1}. \tag{9}$$

因此，对于任意 d，存在一组参数值 (η,p)，使条件 (i) 和 (ii) 同时成立，从而证明了无限制单向导引。这种情形对应于低噪声和高损耗。

III. 证明概要

A. 陈述 (i)

第一步是证明可以移除损失信道，因为损失信道作用于可信方时，不会影响底层系综的操控性质。以下引理将这一结论形式化。

引理 1。 考虑一个系综 $\{\sigma_{a|x}\}_{a,x}$ 以及一个针对 $\eta > 0$ 的损失信道 $\mathcal{L}_\eta$。系综 $\left\{\sigma'_{a|x} = \mathcal{L}_\eta[\sigma_{a|x}]\right\}_{a,x}$ 是 n- 可导的，当且仅当$\{\sigma_{a|x}\}_{a,x}$ 是。

完整证明见附录A。思路是证明：如果系综 $\left\{\sigma'_{a|x}\right\}_{a,x}$ 是 n-可预备的，就可以为 $\{\sigma_{a|x}\}_{a,x}$构造一个 n-可预备的模型。反向结论显然成立（通过应用损失信道）。

因此，要证明 $\rho_{AB}^{(\eta,p)}$ 是 d从 Bob 到 Alice 的-可导引态，只需证明各向同性量子态$\rho_{AB}^{(1,p)} = p\,\Phi_d^+ + (1-p)\frac{\mathbb{1}_d\otimes\mathbb{1}_d}{d^2}$具有该性质；对于足够弱的噪声，这也在预期之中。事实上，文献 [31] 已证明，对于满足方程（ p 8）的，该结论成立，从而完成了命题（i）的证明。请注意，上述 d-可导引性是在使用所有测量构成的集合时得到证明的。也可以改用基于一对互为无偏基的较简单（且实用的）见证，从而验证 d-可导引性，适用于 $\rho_{AB}^{(1,p)}$ [24] 当

$$p \geq \frac{(d+\sqrt{d}-1)\sqrt{d-1}-1}{(d-1)(\sqrt{d-1}+1)}. \tag{10}$$

接下来，通过引理 2 证明中讨论的滤波过程，可以证明对于任意 $\eta > 0$， $\rho_{AB}^{(\eta,p)}$ 具有 d-可导引性；该过程会去除真空分量 $|\varnothing\rangle$。

B. 陈述 (ii)

这里我们利用 [29] 操控与测量相容性这两个概念之间的联系；这一联系将在下一节中正式引入。特别地，对于任意 CPTP 映射 $\mathcal{E}$，已知由算子$\sigma_{b|y} = \mathrm{tr}\left[(\mathbb{1}\otimes M_{b|y})(\mathrm{id}\otimes\mathcal{E}[\Phi^+])\right]$给出的量子态系综具有 LHS 模型，当且仅当测量集合$\{\mathcal{E}^*[M_{b|y}]\}$ 是联合可测的。因此，当且仅当通道$\mathcal{E}$ 是相容性破坏型 [35], 时，量子态 $(\mathrm{id}\otimes\mathcal{E}[\Phi^+])$ 才是不可操控的；也就是说，对于任意测量系综 $\{M_{b|y}\}$，所得系综$\{\mathcal{E}^*[M_{b|y}]\}$ 都是联合可测的。因此，命题（ii）可由以下引理推出。

引理 2 当 $\eta \leq (1-p)^{d-1}$时，通道 $\mathcal{E} = \mathcal{L}_\eta \circ \mathcal{W}_p$ 是相容性破坏型。

一旦我们解决了给定有限维数下所有测量在白噪声和损耗作用下的联合可测性问题，这个引理的证明就相当直接了当 d。这是一个本身也颇具研究价值的问题，我们将在下一节展开讨论。随后，我们将在附录C中利用这些结果给出引理 2 的形式化证明。

IV. 所有测量在损耗和噪声作用下的相容性

测量不相容性是指一组测量无法在同一个系统副本上同时进行的性质。形式上，一组测量 $\{M_{a|x}\}$ 称为不相容的，当且仅当不存在一个“母”POVM $\{E_\lambda\}$ 以及经典后处理$\{p(a|x,\lambda)\}$ 使得

$$M_{a|x} = \sum_\lambda p(a|x,\lambda)E_\lambda. \tag{11}$$

允许这种模型的测量集合称为联合可测；综述可参见例如 [36, 37] 。

我们关注含噪且有损测量的（不）相容性。对于任意一个具有m 个输出 $a = 1,\ldots,m$、作用于维数为d的系统上的 POVM $\{M_a\}$，我们将其非理想版本 $\{\bar{M}_a^{(\eta,p)}\}$ 定义为一个具有 $m+1$ 个元素的 POVM，具体如下：

$$\bar{M}_a^{(\eta,p)} = \begin{cases} \eta p\, M_a + \eta(1-p)(\mathrm{tr}\, M_a)\frac{\mathbb{1}_d}{d} & a = 1,\ldots,m \\ (1-\eta)\mathbb{1}_d & a = \varnothing \end{cases}. \tag{12}$$

含噪声的测量装置以概率 ηp表现得如同理想装置，以概率 $\eta(1-p)$产生随机结果，并以概率 $1-\eta$ 不发生点击（形式上，这对应于无点击结果 $a = \varnothing$）。我们关注在给定维数 d下，所有测量在何种 (η, p) 取值下会变得相容。以下结果给出了一个充分条件。

结果 2. 当满足以下条件时，所有 *POVM* 的集合 $\{\bar{M}_{a|U}^{(\eta,p)}\}_U$ 在 $\mathbb{C}^d$ 上是联合可测的

$$\eta \leq (1-p)^{d-1}. \tag{13}$$

证明： 为证明该结果，我们给出一个显式构造，其灵感来自 [38], 能够模拟所有噪声参数满足式（13）的不完美 POVM。注意，只需证明它能够模拟所有秩一 POVM $\{M_a = \alpha_a |\varphi_a\rangle\langle\varphi_a|\}$ 且满足 $\sum\alpha_a = d$，因为通过后处理即可用它们模拟所有其他测量。后处理通过混合 POVM 元素来完成，即对相应输出进行粗粒化。根据线性，该处理与式（12）中定义的测量噪声化相一致。

我们取协变 POVM 作为父 POVM——一种连续取值的测量，其密度为

$$E_{\boldsymbol{z}} = d\,|\boldsymbol{z}\rangle\langle\boldsymbol{z}| \tag{14}$$

其中 $|\boldsymbol{z}\rangle = \sum_{k=0}^{d-1} z_k |k\rangle$ 满足 $\boldsymbol{z}\in\mathbb{C}^d$，且 $|\boldsymbol{z}|^2 = 1$; $\mathrm{d}\boldsymbol{z}$ 是纯量子态 $|\boldsymbol{z}\rangle$ 上的酉变换不变测度，使得 $\int \mathrm{d}\boldsymbol{z}\,|\boldsymbol{z}\rangle\langle\boldsymbol{z}| = \frac{1}{d}\mathbb{1}_d$。

为定义模拟已通知的一阶 POVM 的响应函数 $p(a|\boldsymbol{z})$ $\{\alpha_a|\varphi_a\rangle\langle\varphi_a|\}_a$，我们分两步进行。首先，从概率分布 $\frac{\alpha_a}{d}$ 中抽取一个可能的输出 a。给定 a 及相应的量子态 $|\varphi_a\rangle$，通过使用确定性响应函数来模拟一个二结果 POVM$\{N_{(a)a},\ N^{(a)}{}_\varnothing\}$

$$p^{(a)}(a|\boldsymbol{z}) = \begin{cases} 1 & |\langle\varphi_a|\boldsymbol{z}\rangle|^2 \geq t \\ 0 & \text{otherwise} \end{cases} \tag{15}$$

以及 $p^{(a)}(\varnothing|\boldsymbol{z}) = 1-p^{(a)}(a|\boldsymbol{z})$，其参数为 $t\in[0,1]$。现在来计算由此得到的算子

$$N_a^{(a)} = \int \mathrm{d}\boldsymbol{z}\, p^{(a)}(a|\boldsymbol{z}) E_{\boldsymbol{z}} \tag{16}$$

且 $N_{(a)\varnothing} = \mathbb{1}_d - N_{(a)a}$。注意到 $N_{(a}^{a} = U N_a^{(a)} U^\dagger)$ 在所有保持量子态 $|\varphi_a\rangle$ 不变 $U|\varphi_a\rangle = |\varphi_a\rangle$ 的酉变换 U 下均保持不变，因为测度 $\mathrm{d}\boldsymbol{z}$ 和响应函数 $p^{(a)}(a|\boldsymbol{z})$ 在此类变换下都保持不变。换言之，任何此类酉变换都与我们的算符 $[U, N_a^{(a)}] = 0$ 对易。因此，$N_a^{(a)}$ 以 $|\varphi_a\rangle$ 为本征态，并且在正交子空间上与恒等算符成比例。也就是说，它具有如下形式

$$N_a^{(a)} = \bar{A}_d(t)\,|\varphi_a\rangle\langle\varphi_a| + \bar{B}_d(t)\frac{\mathbb{1}_d - |\varphi_a\rangle\langle\varphi_a|}{d-1}, \tag{17}$$

其中可计算的标量函数为

$$\begin{aligned}\bar{A}_d(t) &= \operatorname{tr} N_a^{(a)}\,|\varphi_a\rangle\langle\varphi_a| = d\int \mathrm{d}\boldsymbol{z}\, p^{(a)}(a|\boldsymbol{z})|\,\langle\varphi_a|\boldsymbol{z}\rangle\,|^2\\ \bar{A}_d(t) + \bar{B}_d(t) &= \operatorname{tr} N_a^{(a)} = d\int \mathrm{d}\boldsymbol{z}\, p^{(a)}(a|\boldsymbol{z}).\end{aligned} \tag{18}$$

这些积分很容易计算。在附录 B 中我们证明它们等于 $\bar{A}_d(t) = (1-t)^{d-1}((d-1)t+1)$ 以及 $\bar{T}_d(t) \equiv \bar{A}_d(t) + \bar{B}_d(t) = d(1-t)^{d-1}$。

最后，对抽样值 a 取平均后，我们看到该策略模拟了 $N_a = \frac{\alpha_a}{d} N_a^{(a)}$ 和 $N_\varnothing = \sum_a \frac{\alpha_a}{d} N^{(a)}{}_\varnothing$，从而得到

$$N_a = \frac{\alpha_a}{d}\left(\bar{A}_d(t)\,|\varphi_a\rangle\langle\varphi_a| + \bar{B}_d(t)\frac{\mathbb{1}_d - |\varphi_a\rangle\langle\varphi_a|}{d-1}\right) \tag{19}$$

且 $N_\varnothing = \mathbb{1}_d - \sum_a N_a$。另一方面，由式 (12) 可得 $\bar{M}_a^{(\eta,p)} = \frac{\alpha_d}{d}\left(d\,\eta p\,|\varphi_a\rangle\langle\varphi_a| + \eta(1-p)\mathbb{1}_d\right)$。将其与式 (19) 比较，我们得出结论，对于

$$\begin{aligned}\eta &= \frac{\bar{T}_d(t)}{d} = (1-t)^{d-1},\\ p &= \frac{d\bar{A}_d(t) - \bar{T}_d(t)}{(d-1)\bar{T}_d(t)} = t\end{aligned} \tag{20}$$

并且 $t\in[0,1]$ 可以模拟任意 POVM $\{\bar{M}_a^{(\eta,p)}\}$。要重现噪声更大的测量，只需在上述构造中加入噪声即可。因此，对于任意噪声水平 $p = t$，若 $\eta \le (1-t)^{d-1} = (1-p)^{d-1}$，我们的构造就能模拟所有 POVM $\{\bar{M}_a^{(\eta,p)}\}$。□

V. 讨论与结论

考虑基于高维纠缠的双体操控场景，我们研究了操控效应可以变得多么不对称。我们给出了纠缠态 ϱ_{AB}，使得 Alice 能让 Bob 相信 ϱ_{AB} 具有较高的施密特数，而 Bob 却始终无法让 Alice 相信该量子态甚至是纠缠的。因此，单向导引可以达到无限程度。

具体而言，我们构造了若干族纠缠态，它们在一个方向上表现出真正的 d 维操控，而在另一方向上则不可操控（即使采用最一般的测量）。我们指出，这一构造可以直接推广到这样的量子态：在一个方向上表现出真正的 n 维操控，而在另一方向上不可操控，其中 $1 < n \le d$ [1] 可取任意值。原则上，这类量子态的实际实现是可行的，例如可利用文献 [39, 40] 中的实验装置来演示无限单向导引。

最后，我们的工作还促进了对高维测量中联合可测性的刻画。特别是，我们得到了一个判据，用于判断同时受到噪声和损耗影响的任意测量是否兼容。这一结果本身也具有研究价值，并可能有其他应用。

致谢。— 我们感谢瑞士国家科学基金会（项目 192244、Ambizione PZ00P2-202179 和 NCCR SwissMAP）的资助。

[1] R. Horodecki、P. Horodecki、M. Horodecki 和 K. Horodecki，《现代物理评论》**81**，865（2009）。[2] O. G¨uhne 和 G. T´oth，《物理学报告》**474**，1（2009）。[3] N. Brunner、D. Cavalcanti、S. Pironio、V. Scarani 和 S. Wehner，《现代物理评论》**86**，419（2014）。

[4] R. F. Werner，《物理评论 A》**40**，4277（1989）。[5] J. Barrett，《物理评论 A》**65**，042302（2002）。[6] D. Cavalcanti 和 P. Skrzypczyk，《物理学进展报告》**80**，024001（2016）。[7] R. Uola、A. C. S. Costa、H. C. Nguyen 和 O. G¨uhne，《现代物理学评论》**92**（2020），10.1103/revmod- phys.92.015001。[8] H. M. Wiseman、S. J. Jones 和 A. C. Do- herty，《物理评论快报》**98**（2007），10.1103/phys- revlett.98.140402。

[1] 为此，只需调整方程（8）和（10）中的界限，只要求 n–可操控性，分别依据 [31] 关于（8）以及 [24]关于（10）的结果。

[9] A. 爱因斯坦、B. Podolsky 和 N. Rosen，Phys. Rev. 47, 777 1935( )。[10] E. Schr¨odinger，《剑桥哲学学会数学论文集》31，555–563（1935）。[11] E. Schr¨odinger，《剑桥哲学学会数学论文集》32，446–452（1936）。[12] J. Bowles、T. V´ertesi、M. T. Quintino 和 N. Brunner，Phys. Rev. Lett. 112, 200402（2014）。[13] P. Skrzypczyk、M. Navascu´es 和 D. Cavalcanti，Phys. Rev. Lett. 112, 180404（2014）。[14] M. T. Quintino、T. V´ertesi、D. Cavalcanti、R. Augusiak、M. Demianowicz、A. Ac´ın 和 N. Brunner，Phys. Rev. A 92, 032107（2015）。[15] J. Bowles、F. Hirsch、M. T. Quintino 和 N. Brunner，Phys. Rev. A 93, 022121 （ 2016 ）。[16] Q. Zeng，Phys. Rev. A 106, 032202（2022）。[17] I. M´arton、S. Nagy、E. Bene 和 T. V´ertesi，Phys. Rev. Res. 3, 043100（2021）。[18] S. L. W. Midgley、A. J. Ferris 和 M. K. Olsen, Phys. Rev. A 81, 022101（2010）。[19] M. K. Olsen，Phys. Rev. A 88, 051802（2013）。[20] V. H¨andchen、T. Eberle、S. Steinlechner、A. Samblowski、T. Franz、R. F. Werner 和 R. Schnabel，Nature Photonics 6, 596（2012）。[21] S. Wollmann、N. Walk、A. J. Bennet、H. M. Wiseman 和 G. J. Pryde，Phys. Rev. Lett. 116, 160403（2016）。[22] K. Sun、X.-J. Ye、J.-S. Xu、X.-Y. Xu、J.-S. Tang、Y.-C. Wu、J.-L. Chen、C.-F. Li 和 G.-C. Guo，Phys. Rev. Lett. 116, 160404（2016）。[23] N. Tischler、F. Ghafari、T. J. Baker、S. Slussarenko、R. B. Patel、M. M. Weston、S. Wollmann、L. K. Shalm、V. B. Verma、S. W. Nam、H. C. Nguyen、H. M. Wiseman 和 G. J. Pryde，Phys. Rev. Lett. 121, 100401（2018）。[24] S. Designolle、V. Srivastav、R. Uola、N. H. Valencia、W. McCutcheon、M. Malik 和 N. Brunner，Phys. Rev. Lett. 126, 200404（2021）。[25] S. Designolle，Phys. Rev. A 105, 032430（2022）。[26] C. de Gois、M. Pl´avala、R. Schwonnek 和 O. G¨uhne，“高维操控认证的完整层级—化”，（2022），arXiv:2212.12544 [quant-ph]。[27] M. T. Quintino、T. V´ertesi 和 N. Brunner，《Physical Review Letters》113（2014），10.1103/phys- revlett.113.160402。[28] R. Uola、T. Moroder 和 O. G¨uhne，《Physical Review Letters》113（2014），10.1103/physrevlett.113.160403。[29] R. Uola、C. Budroni、O. G¨uhne 和 J.-P. Pellonp¨a¨a，《Physical Review Letters》115（2015），10.1103/phys- revlett.115.230402。[30]J. Kiukas、C. Budroni、R. Uola 和 J.-P. Pel- lonp¨a¨a，《Physical Review A》96（2017），10.1103/phys- reva.96.042331。[31] B. D. Jones、R. Uola、T. Cope、M. Ioannou、S. De- signolle、P. Sekatski 和 N. Brunner，arXiv 预印本 arXiv:2207.04080（2022）。[32] M. Ioannou、P. Sekatski、S. Designolle、B. D. M. Jones、R. Uola 和 N. Brunner，《Phys. Rev. Lett.》129，190401（2022）。[33] B. M. Terhal 和 P. Horodecki，《Phys. Rev. A》61，040301（2000）。[34] A. Sanpera、D. Bruß 和 M. Le wenstein，《Phys. Rev. A》63，050301（2001）。[35] T. Heinosaari、J. Kiukas、D. Reitzner 和 J. Schultz，《Journal of Physics A: Mathematical and Theoretical》48，435301（2015）。[36] T. Heinosaari、T. Miyadera 和 M. Ziman，《Journal of Physics A: Mathematical and Theoretical》49，123001（2016）。[37] O. G¨uhne、E. Haapasalo、T. Kraft、J.-P. Pellonp¨a¨a 和 R. Uola，《Rev. Mod. Phys.》95，011003（2023）。[38] F. Hirsch、M. T. Quintino、J. Bowles 和 N. Brunner，《Physical Review Letters》111，160402（2013）。[39] Q. Zeng、B. Wang、P. Li 和 X. Zhang，《Phys. Rev. Lett.》120，030401（2018）。[40] V. Srivastav、N. H. Valencia、W. McCutcheon、S. Lee- dumrongwatthanakun、S. Designolle、R. Uola、N. Brun- ner 和 M. Malik，《Phys. Rev. X》12，041023（2022）。[41] M. Hayashi，《Journal of Physics A: Mathematical and General》31，4633（1998）。

附录 A：引理 1 的证明

引理 1：考虑一个系综 $\{\sigma_{a|x}\}_{a,\,x}$ 以及一个作用于 $\eta > 0$ 的损失信道 $\mathcal{L}_\eta$。系综 $\left\{\sigma'_{a|x} = \mathcal{L}_\eta[\sigma_{a|x}]\right\}_{a,\,x}$是 n-可操控的，当且仅当 $\{\sigma_{a|x}\}_{a,\,x}$ 也是。

首先证明，如果 $\{\sigma_{a|x}\}_{a,\,x}$ 不是 n-可操控的，那么 $\{\sigma'_{a|x}\}_{a,\,x}$ 也不是。这里，$\{\sigma_{a|x}\}_{a,\,x}$ 不是 n-可操控的，意指存在一个秩为-n 的隐量子态（RnHS）模型，可以模拟该系综。该模型由定义在量子态 $\psi_{AB}(\lambda)$ 上的概率密度 $p(\lambda)$ 构成，其中这些量子态的施密特秩均不超过 n；此外，Alice 还实施一组 “ 响应 POVM” $A_{a|x,\,\lambda}$，使得

$$\sigma_{a|x} = \int \mathrm{d}\lambda p(\lambda)\,\mathrm{tr}_A\,\psi_{AB}(\lambda)A_{a|x,\lambda}. \tag{A1}$$

只需将损失信道作用于每个量子态 $\psi'_{AB}(\lambda) = \mathrm{id}_A \otimes \mathcal{L}_\eta[\psi_{AB}(\lambda)]$，即可直接为系综 $\{\sigma'_{a|x}\}_{a,\,x}$ 定义 RnHS 模型。请注意，损失信道（与任何局域映射一样）不会增加量子态的施密特秩，且

$$\int \mathrm{d}\lambda p(\lambda)\,\mathrm{tr}_A(\mathrm{id}_A \otimes \mathcal{L}_\eta[\psi_{AB}(\lambda)])A_{a|x,\lambda} = \mathcal{L}_\eta\left[\int \mathrm{d}\lambda p(\lambda)\,\mathrm{tr}_A\,\psi_{AB}(\lambda)A_{a|x,\lambda}\right] = \mathcal{L}[\sigma_{a|x}] = \sigma'_{a|x}. \tag{A2}$$

接下来，我们证明反方向：如果 $\{\sigma'_{a|x}\}_{a,\ x}$ 不是 n-可转向的，那么 $\{\sigma_{a|x}\}_{a,\ x}$ 也不是。现在，我们从系综 model $p'(\lambda)$、(λ) 和 $A_{a|x,\ \lambda}$ 的一个 RnHS 模型开始。

$$\sigma'_{a|x} = \int \mathrm{d}\lambda p'(\lambda)\,\mathrm{tr}_A\,\psi'_{AB}(\lambda)A_{a|x,\lambda}. \tag{A3}$$

这里将量子态 $\sigma'_{a|x}$ 和 $\phi'_{AB}(\lambda)$定义在一个 $(d+1)$ 维系统上，其中包含损失信道引入的额外能级 $|\text{ø}\rangle$。我们定义这些量子态在与 $|\psi\rangle$ 正交、由 $\Pi_{[1,d]}$ 投影得到的子空间上的限制。对于隐藏量子态，我们得到

$$\psi_{AB}(\lambda) \equiv \frac{(\mathrm{id}_A \otimes \Pi_{[1,d]})\psi'_{AB}(\lambda)(\mathrm{id}_A \otimes \Pi_{[1,d]})}{q_{[1,d]}(\lambda)} \qquad \text{with} \qquad q_{[1,d]}(\lambda) = \mathrm{tr}\big(\mathrm{id}_A \otimes \Pi_{[1,d]}\big)\psi'_{AB}(\lambda) \tag{A4}$$

它们的施密特秩也至多为 n，并定义新的概率密度

$$p(\lambda) \equiv \frac{p'(\lambda)q_{[1,d]}(\lambda)}{\int \mathrm{d}\lambda p'(\lambda)q_{[1,d]}(\lambda)}. \tag{A5}$$

这里的分母为

$$\int \mathrm{d}\lambda p'(\lambda)q_{[1,d]}(\lambda) = \mathrm{tr}\big(\mathrm{id}_A \otimes \Pi_{[1,d]}\big)\int \mathrm{d}\lambda p'(\lambda)\psi'_{AB}(\lambda) = \mathrm{tr}\,\Pi_{[1,d]}\sum_a \sigma'_{a|x} = \eta \tag{A6}$$

N现在计算新颖的 RnHS 模型 $(p(\lambda)\ \psi_{AB}(\lambda)A_{a|x,\lambda})$ 所模拟的系综

$$\begin{aligned}
\tilde{\sigma}_{a|x} &= \int \mathrm{d}\lambda p(\lambda) tr_A \psi_{AB}(\lambda)(\mathrm{id}_A \otimes \Pi_{[1,d]})A_{a|x,\lambda} \\
&= \frac{\int \mathrm{d}\lambda p'(\lambda) tr_A(\mathrm{id}_A \otimes \Pi_{[1,d]})\psi'_{AB}(\lambda)(\mathrm{id}_A \otimes \Pi_{[1,d]})A_{a|x,\lambda}}{\int \mathrm{d}\lambda p'(\lambda)q_{[1,d]}(\lambda)} \\
&= \frac{\Pi_{[1,d]}\left(\int \mathrm{d}\lambda p'(\lambda) tr_A \psi'_{AB}(\lambda)A_{a|x,\lambda}\right)\Pi_{[1,d]}}{\eta} \\
&= \frac{1}{\eta}\Pi_{[1,d]}\sigma'_{a|x}\ \Pi_{[1,d]} \\
&= \sigma_{a|x}
\end{aligned} \tag{A7}$$

为证明最后一个等式，考虑损失信道对 $\sigma_{a|x}$ 的作用

$$\sigma'_{a|x} = \mathcal{L}_\eta(\sigma_{a|x}) = \eta\,\sigma_{a|x} + (1-\eta)\,|\,\text{ø}\,\rangle\langle\,\text{ø}\,|\ \implies\ \sigma_{a|x} = \frac{1}{\eta}\Pi_{[1,d]}\sigma'_{a|x}\Pi_{[1,d]}. \tag{A8}$$

证明至此完成。 □

附录 B：计算结果 2 证明中的积分

这里我们计算这些积分

$$\begin{aligned}
\bar{A}_d(t) &= d\int \mathrm{d}\boldsymbol{z}\, p_t^{(a)}(a|\boldsymbol{z})\ |\langle\varphi_a|\boldsymbol{z}\rangle|^2 \\
\bar{T}_d(t) &= d\int \mathrm{d}\boldsymbol{z}\, p_t^{(a)}(a|\boldsymbol{z}),
\end{aligned} \tag{B1}$$

其中，$\mathrm{d}\boldsymbol{z}$ 是量子态 $|\boldsymbol{z}\rangle$ 上的酉不变测度，且 $p_t^{(a)}(a|\boldsymbol{z}) = \begin{cases} 1 & |\langle\varphi_a|\boldsymbol{z}\rangle|^2 \geq t \\ 0 & \text{否则} \end{cases}$。由于测度具有不变性，在 $|\varphi_a\rangle = |0\rangle$的基底下进行计算会更方便，因此可直接得到

$$\begin{aligned}
\bar{A}_d(t) &= d\int \mathrm{d}\boldsymbol{z}\,\Xi[\boldsymbol{z}]\ |\langle 0|\boldsymbol{z}\rangle|^2 \\
\bar{T}_d(t) &= d\int \mathrm{d}\boldsymbol{z}\,\Xi[\boldsymbol{z}],
\end{aligned} \tag{B2}$$

且 $\Xi_t(\boldsymbol{z}) = \begin{cases} 1 & |\langle 0|\boldsymbol{z}\rangle|^2 \geq t \\ 0 \end{cases}$ 否则。为计算这些积分，我们将量子态 $|\boldsymbol{z}\rangle = \sum_{k=0}^{d-1} z_k |k\rangle$参数化为

$$\boldsymbol{z} = \begin{pmatrix} z_0 \\ z_1 \\ \vdots \\ z_{d-2} \\ z_{d-1} \end{pmatrix} = \begin{pmatrix} \cos(\theta_1) \\ e^{\mathrm{i}\phi_2}\sin(\theta_1)\cos(\theta_2) \\ \vdots \\ e^{\mathrm{i}\phi_{d-1}}\sin(\theta_1)\ldots\sin(\theta_{d-2})\cos(\theta_{d-1}) \\ e^{\mathrm{i}\phi_d}\sin(\theta_1)\ldots\sin(\theta_{d-2})\sin(\theta_{d-1}) \end{pmatrix} \tag{B3}$$

对于 $\phi_i \in [0, 2\pi]$ 和 $\theta_i \in [0, \frac{\pi}{2}]$，不变测度具有如下形式： [41]

$$\mathrm{d}\boldsymbol{z} = \frac{(d-1)!}{\pi^{d-1}} \Pi_{i=1}^{d-1} \sin^{2d-2i-1}(\theta_i)\cos(\theta_i)\mathrm{d}\theta_i \, \Pi_{j=2}^{d}\mathrm{d}\phi_j. \tag{B4}$$

采用这种参数化方式，我们得到 $|\langle 0|\boldsymbol{z}\rangle|^2 = |z_0|^2 = \cos^2(\theta_1)$ 和

$$\Xi_t(\boldsymbol{z}) \equiv \Xi_t(\theta_1) = \begin{cases} 1 & \cos^2(\theta_1) \geq t \\ 0 & \text{otherwise.} \end{cases} \tag{B5}$$

被积函数仅依赖于角度 θ_1，因此我们可以写成

$$\begin{aligned} \bar{T}_d(t) &= \frac{d}{N}\int_0^{\pi/2} \sin^{2d-3}(\theta_1)\cos(\theta_1)\mathrm{d}\theta_1 \Xi_t(\theta_1) \\ \bar{A}_d(t) &= \frac{d}{N}\int_0^{\pi/2} \sin^{2d-3}(\theta_1)\cos(\theta_1)\mathrm{d}\theta_1 \Xi_t(\theta_1)\cos^2(\theta_1). \end{aligned} \tag{B6}$$

其中归一化常数为 $N = \int_0^{\pi/2} \sin^{2d-3}(\theta_1)\cos(\theta_1)\mathrm{d}\theta_1$。进行变量代换 $x = \sin^2(\theta_1)$，其中 $\mathrm{d}\theta_1 = \mathrm{d}2 \quad {}^{x}_{\theta_1}\sin()\cos(\theta_1)$，即可得到正文中使用的表达式

$$\begin{aligned} N &= \frac{1}{2}\int_0^1 x^{d-2}\mathrm{d}x = \frac{1}{2(d-1)} \\ \bar{T}_d(t) &= \frac{d}{2N}\int_0^{1-t} x^{d-2}\mathrm{d}x = d(1-t)^{d-1} \\ \bar{A}_d(t) &= \frac{d}{2N}\int_0^{1-t} x^{d-2}(1-x)\mathrm{d}x = (1-t)^{d-1}((d-1)t+1). \end{aligned} \tag{B7}$$

附录 C：引理 2 的证明

引理 2 当 $\eta \leq (1-p)^{d-1}$. 时，信道 $\mathcal{E} = \mathcal{L}_\eta \circ \mathcal{W}_p$ 具有不相容性破坏性质

证明： 由结果 3 可知，当 $\eta \leq (1-p)^{d-1}$ 时，维数为 d、受到白噪声和损耗影响的所有 POVM $\{\bar{M}_{a|U}^{(\eta,p)}\}_U$ 均为联合可测。因此，引理 2 可由以下结果推出。

引理 2.1 当且仅当所有受到损耗和白噪声影响的 *POVM* $\{\bar{M}_{a|x}^{(\eta,p)}\}$ 构成的集合为联合可测时，信道 $\mathcal{E} = \mathcal{L}_\eta \circ \mathcal{W}_p$ 才是相容性破坏信道。

证明： 乍看之下，这一论断似乎是同义反复；但仔细考察便会发现，信道 $\mathcal{E}^-$的输出 $(d+1)$ 维，而 $M_{a|x}$ 描述的是对维数为 d 的系统进行的测量。因此，该谓词所指的并非同一组 POVM。

更准确地说，令集合 $\{M'_{a|x}\}$ 表示所有作用于维数为 $d+1$ 的 POVM。那么，当且仅当测量系综

$$\{\hat{M}_{a|x}^{(\eta,p)} \equiv \mathcal{E}^*[M'_{a|x}]\} \tag{C1}$$

是联合可测的。集合 $\{\bar{M}_{a|x}^{(\eta,p)}\}$ 包含这些 POVM

$$\bar{M}_a^{(\eta,p)} = \begin{cases} \eta p\, M_a + \eta(1-p)(\operatorname{tr} M_a)\frac{\mathbb{1}_d}{d} & a = 1,\dots,m \\ (1-\eta)\mathbb{1}_d & a = \varnothing \end{cases} \tag{C2}$$

其中， $M_{a|x}$ 遍历维数为 d的所有 POVM。我们要证明，系综 $\{\hat{}M_{a|x}^{(\eta,p)}\}$ 相容当且仅当 $\{\bar{M}_{a|x}^{(\eta,p)}\}$ 相容，其中两组测量都作用于一个 d维量子系统。

首先，我们仔细考察系综 $\{\hat{}M_{a|x}\}$。损失信道 $\mathcal{L}_\eta$ 有 $d+1$ 个 Kraus算子

$$\begin{aligned} K_\checkmark &= \sqrt{\eta}\underbrace{\sum_{k=1}^{d}|k\rangle\langle k|}_{\equiv\Pi_\checkmark} \\ K_k &= \sqrt{1-\eta}\,|\varnothing\rangle\langle k| \qquad k = 0,\dots,d-1 \end{aligned} \tag{C3}$$

因此，对于希尔伯特空间 span,,,ø 上的任意测量 M_a' $\mathcal{H}_{d+1} = \{|0\rangle\ \dots\ |d-1\rangle\ |\ \rangle\}$ $\mathcal{E}^*[M_a'] = \mathcal{W}_p^*\circ$，我们有 and $\mathcal{L}_\eta^*[M_a']$

$$\begin{aligned} \mathcal{L}_\eta^*[M_a'] &= K_\checkmark^\dagger M_a' K_\checkmark + \sum_{k=0}^{d-1} K_k^\dagger M_a' K_k \\ &= \eta\,\Pi_\checkmark M_a'\Pi_\checkmark + (1-\eta)\mathbb{1}_d\underbrace{\langle\varnothing|\,M_a'\,|\varnothing\rangle}_{\equiv q(a)}, \end{aligned} \tag{C4}$$

其中， $q(a)$ 是一个概率分布，因为 $q(a) = \mathsf{tr}\,|\varnothing\rangle\langle\varnothing|\,M_a' \geq 0$且 $\sum_a q(a) = \mathsf{tr}\,|\varnothing\rangle\langle\varnothing|\sum_a M_a' = 1$。此外，在发生损耗之前，算子 $M_a \equiv \Pi_\checkmark M_a'\Pi_\checkmark$ 在 d维子空间 $\mathcal{H}_d = \mathsf{span}\{|0\rangle,\dots,|d-1\rangle\}$ 上定义了一个有效的 POVM。因此，我们有

$$\mathcal{L}_\eta^*[M_a'] = \eta M_a + (1-\eta)q(a)\mathbb{1}_d. \tag{C5}$$

最后加入噪声信道，我们得到

$$\begin{aligned} \hat{M}_a^{(\eta,p)} &= \mathcal{W}_p^*\circ\mathcal{L}_\eta^*[M_a'] \\ &= \eta\mathcal{W}_p^*[M_a] + (1-\eta)q(a)\mathcal{W}_p^*[\mathbb{1}_d] \\ &= \eta M_a^{(1,p)} + (1-\eta)q(a)\mathbb{1}_d \\ &= \eta p M_a + \eta(1-p)(\operatorname{tr} M_a)\frac{\mathbb{1}_d}{d} + (1-\eta)q(a)\mathbb{1}_d \\ &= \bar{M}_a^{(\eta,p)} + q(a)\bar{M}_\varnothing^{(\eta,p)}. \end{aligned} \tag{C6}$$

我们看到，如果 POVM $\bar{M}_{(\eta,\ p)a}$可以被模拟，那么只需以概率 $q(a)$ 将输出 ø 重新标记为 a ，也可以用它来模拟 $\hat{}M_a^{(\eta,p)}$。因此，如果所有 POVM $\{\bar{M}_{a|x}^{(\eta,p)}\}$ 组成的集合相容，那么$\{\hat{}M_{a|x}^{(\eta,p)}\}$也相容。

为证明逆命题，考虑 $(d+1)$ 维空间上的所有 POVM，其元素形式为$\{M_1,\dots,M_a,\dots,M_\varnothing = |\varnothing\rangle\langle\varnothing|\}$，其中 $\langle\varnothing|\,M_a\,|\varnothing\rangle = 0$，而 $\{M_1,\dots,M_a,\dots\}$（不含 $M_\varnothing$ 元素）遍历 d 维子空间 $\mathcal{H}_d = \mathsf{span}\{|0\rangle,\dots,|d-1\rangle\}$ 上的所有 POVM。对于这种形式的 POVM，我们有$q(a) = 0$, $q(\varnothing) = 1$，根据方程

$$\begin{aligned} \hat{M}_a^{(\eta,p)} &= \bar{M}_a^{(\eta,p)} \\ \hat{M}_\varnothing^{(\eta,p)} &= (1-\eta)\bar{M}_\varnothing^{(\eta,p)}. \end{aligned} \tag{C7}$$

This 如果任何测量 $\hat{}M^{(\eta,p)a}$都可以被模拟，那么任何测量 $\bar{M}_a^{(\eta,p)}$也同样可以。 □