arXiv:2302.00974v2 [quant-ph] 8 Jul 2023

所有实射影测量都可以自检验

Ranyiliu Chen LauraMan˘cinska Jurij Vol˘ci˘c

摘要

自检验是量子功能验证中最强的形式，它使经典用户能够推断出用于产生测量统计的量子态和测量。虽然量子态的自检验已得到充分理解，但测量的自检验，尤其是在高维情形下，仍难以实现。我们通过证明每个实投影测量都可以自检验，展示了这一方向上的首个一般性结果。自检验的标准定义只允许认证实测量。因此，我们的工作实际上将可自检验的投影测量范围扩展到了其全部潜力。为获得这一结果，我们采用了这样一种思路：扩展现有的自检验，以验证额外的不可信测量。这种方法称为“事后自检验”。我们对事后自检验的方法进行了形式化，并确立了其适用的充分条件。利用这一条件，我们构造了适用于所有实投影测量的自检验。受这一构造启发，我们提出了一种新的迭代自检技术，即依次运用事后自检验。从任意一个已有的自检验出发，我们全面刻画了可通过迭代自检验验证的测量集合。这为基于现有自检验构造新的自检验提供了清晰的方法。

1 引言

1.1 背景

设想这样一种情形：经典用户 Victor 向量子设备提出问题 x并接收答案 a。由于对设备的内部运作一无所知，Victor 将其行为建模为态制备 $|\psi\rangle$，并伴有量子测量 $\{M_{a|x}, \sum_a M_{a|x} = I\}$。对于问题 x，设备会对量子态 $|\psi\rangle$ 执行测量 $\{M_{a|x}\}_a$，并输出相应的测量结果 a。利用玻恩规则 [Bor26] $p(a|x) = \langle\psi|M_{a|x}|\psi\rangle$，从 $|\psi\rangle$ 和 $\{M_{a|x}\}$ 预测设备的输出统计量是很直接的；但仅凭统计量 $p(a|x)$，无法推断出 $|\psi\rangle$ 和$\{M_{a|x}\}$。事实上，不同的量子态 $|\psi\rangle$ 和 $\{M_{a|x}\}$ 可能产生相同的$p(a|x)$。在这种情况下，只要不限制运行时间，经典计算机总能模拟这一量子过程。

有趣的是，在所谓的“二部贝尔场景” [BCP+14、Bel64] 中（见图 1），可以从由此得到的经典统计数据推断出量子功能。Victor 与两个空间上分离的量子设备交互，这两个设备分别称为爱丽丝和鲍勃。他向爱丽丝和鲍勃分别提出问题 $x \in \mathcal{I}_A$和 $y \in \mathcal{I}_B$，而他们则分别给出答案 $a \in \mathcal{O}_A$ 和 $b \in \mathcal{O}_B$。在这次交互过程中，爱丽丝和鲍勃不能相互通信，但他们可以共享一个纠缠量子态 $|\psi\rangle_{AB}$，并使用测量 $\{M_{a|x}: \ a \in \mathcal{O}_A、\ x \in \mathcal{I}_A\}$ 和$\{N_{b|y}: \ b \in \mathcal{O}_B、\ y \in \mathcal{I}_B\}$ 在本地进行测量，从而得到输出 a 和 b。Victor 观察到的统计数据因此服从分布 $p(a,b|x,y) = \langle\psi|M_{a|x} \otimes N_{b|y}|\psi\rangle$。事实证明，某些统计数据 $p(a,b|x,y)$只能由特定纠缠量子态 $|\psi\rangle_{AB}$ 上的一组特定测量 $\{M_{a|x}\}$ 和 $\{N_{b|y}\}$ 产生（局域参考系的变化除外）。这种现象称为“自检验” [MY04]，它依赖于量子理论的关键特征，例如纠缠 [GP92] 和测量不相容性[WPGF09]。自检验是最强形式的验证，因为它所需的假设最少，即爱丽丝和鲍勃的测量设备之间不存在通信，且量子理论成立。具体而言，在自检验中，我们不要求能够使用任何可信或经过全面表征的量子设备；这一条件也称为“设备无关性” [ABG+07]。

我们将二部贝尔场景中设备的量子力学描述称为策略。形式上，这样的策略 $\mathcal{S}$ 是一个元组

$$\mathcal{S} = (|\psi\rangle_{AB}, \{M_{a|x}: a \in \mathcal{O}_A, x \in \mathcal{I}_A\}, \{N_{b|y}: b \in \mathcal{O}_B, y \in \mathcal{I}_B\}),$$

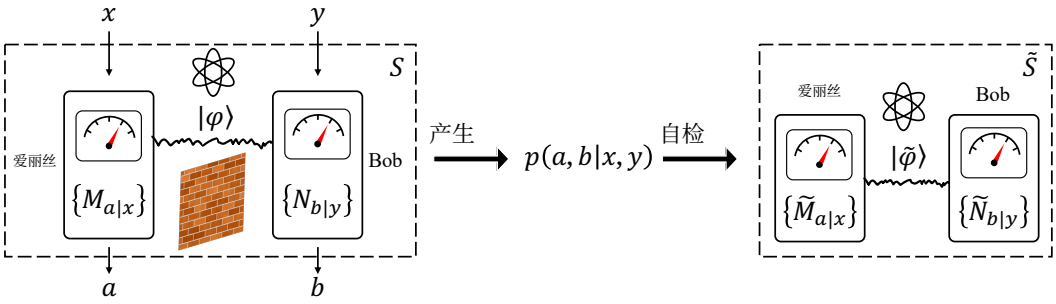

图 1：贝尔场景中的自检验。空间上分离的爱丽丝和鲍勃在共享态（由 $\mathcal{S}$ 描述）上进行局域测量，从而产生关联 $p(a,\ b|x,\ y)$。在自检验的情形下，Victor 可以通过经典方式验证爱丽丝和鲍勃：爱丽丝和鲍勃产生正确关联的唯一方式，就是遵循规定的规范 $\mathcal{S}$。

其中，$|\psi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ 是共享态，$\mathcal{M}_x = \{M_{a|x}\} \subseteq \mathcal{L}(\mathcal{H}_A)$ 和 $\mathcal{N}_b = \{N_{b|y}\} \subseteq \mathcal{L}(\mathcal{H}_B)$ 分别是爱丽丝和鲍勃的 POVM（正算子值测度）。由此得到的测量统计

$$p(a,b|x,y) = \langle\psi|M_{a|x} \otimes N_{b|y}|\psi\rangle$$

通常称为关联。在自检验中，我们仅凭观察其产生的测量统计 p，便能恢复构成 $\mathcal{S}$ 的量子态和测量的描述。因此，只要自检验成立，我们就能验证其中涉及的态制备和测量功能，而无需预先了解所用量子设备的内部运作方式。这引出了自检验中的一个根本问题：

问题： 哪些量子态和测量可以自检验？

换言之，上述问题是在问：经典用户在无法使用可信量子设备的情况下，能够验证哪些态制备和测量功能？要验证（自检验）给定的态制备或测量功能，我们需要构造一个包含该功能的策略 $\mathcal{S}$，并且该策略还能由其产生的关联确定（即经过自检验）。

在双体场景中，关于哪些量子态可自检验的问题，已有一项里程碑式结果 [CGS17], ，它表明任何纯双体纠缠态都可以自检验。近期研究表明，在网络场景中 [TPKLR22] ，任何多方纠缠态都可以自检验 [ŠBR+23]。与量子态自检验相对完善的图景相比，一般测量的自检验仍未得到解决。首先，在二部贝尔场景中，任何复测量（即在共享态的施密特基下具有复矩阵元素的测量）都可以由实测量模拟 [PV08、MMG09、RTW+21]。因此，任何经过自检验的测量都必须是实测量，因为测量及其复共轭总会产生相同的统计结果：

$$\langle\psi|M_{a|x} \otimes N_{b|y}|\psi\rangle = \overline{\langle\psi|M_{a|x} \otimes N_{b|y}|\psi\rangle} = \langle\psi|\overline{M}_{a|x} \otimes \overline{N}_{b|y}|\psi\rangle\,.$$

现有协议主要关注低维量子系统或特定的高维测量。对于二能级系统，已知如何对泡利测量进行自检验 [MY04],，后续研究表明，任意二维投影测量都可以自检验 [YN13]。在 [McK17, Col17] 泡利矩阵的张量积可以自检验，而 [SSKA21] 则为一对特定的 d输出测量提出了一种自检验方案。在 [MPS21, Fu22], 提出了一种常数规模自检验，用于满足某些特殊性质的测量。然而，迄今为止，任意高维测量的自检验仍未能实现。

1.2 结果

在这项工作中，我们以全面（而非基于示例）的方式研究测量的自检验。我们首次给出了一般测量自检验方面的结果。我们的具体贡献包括以下内容：

(i) 我们提出了一种完全明确的自检协议，适用于任意实投影测量。我们的构造所用的问题集大小为 d 的三次方，其中 d 是待自检验测量的维数；答案集大小则为常数。此外，我们的自检验对噪声具有鲁棒性。

(ii) 我们将事后自检的方法形式化，并确定了其适用的充分条件。当我们能够扩展一个先前已自检验的策略，使其包含一项额外测量时，就会发生事后自检。尽管文献中零星出现过这种方法的实例，但人们尚未全面理解这一现象及其发生条件。为此，我们确定了一个充分条件，在该条件下，给定策略的初始自检 $\mathcal{S}$ 可以扩展为包含一项额外测量 $\mathcal{M}$。将这一判据应用于近期研究 [MPS21] 中的初始策略后，我们得以获得 (i) 中的自检构造。

(iii) 我们提出了一种新的迭代自检技术，它涉及按顺序应用事后自检。从任意一个已确立的自检出发，我们利用约当代数刻画可通过迭代自检验证的测量集合。迭代自检的灵感源自 (ii) 中的自检构造，并为基于现有自检开发新自检提供了一种便捷方法。

1.3 论文结构

我们在第2节介绍本文所需的预备知识和常用符号。在第3 节中，我们形式化定义事后自检，并给出一个判据，用于判断某个投影测量是否为事后自检的。接着，在第 4 节中，我们研究迭代自检，并据此展示如何对任意实射影测量进行自检。在第 5 节中，我们阐述迭代自检的一般理论。我们在第6节总结研究结果并提出一些开放问题。附录 A 包含事后自检的示例、反例和一般障碍。附录 B 给出了我们稳健自检策略中可观测量的构造，并附有 Mathematica 代码。

2 预备知识与符号

2.1 测量的可观测量图景

在许多情况下，尤其是当测量为投影测量时（*i.e.*，即 POVM 中的所有算子都是投影），使用广义观测量 而非 POVM 算子会更加方便。给定一个 POVM $\{M_{a|x}\}$，其广义观测量定义为

$$A_x^{(j)} := \sum_{a=0}^{|\mathcal{O}_A|-1} \omega^{aj} M_{a|x},$$

其中 $\omega = e^{i2\pi/|\mathcal{O}_A|}$。注意， $A_x^{(0)} = I$ 根据定义。由于该变换可逆， $\{M_{a|x}\}$可以由 $\{A_x^{(j)}\}$ 通过 $M_a = \frac{1}{|\mathcal{O}_A|}\sum_{j=0}^{|\mathcal{O}_A|-1} \omega^{-aj} A_x^{(j)}$恢复。因此， $\{A_x^{(j)}\}$ 为测量提供了一种替代但完整的描述。广义观测量具有以下性质：（证明见 [KŠT+19] ）

- For any POVM $\{M_{a|x}\}$, $A_x^{(j)} A_x^{(j)\dagger} \leq I$, $A_x^{(j)\dagger} A_x^{(j)} \leq I$, *i.e.*, $A_x^{(j)}$ are contractions.
- 当且仅当相应的 POVM $\{M_{a|x}\}$ 是投影的，此时 $A_x := A_{(1)x}$ 是一个 $|\mathcal{O}_A|$阶酉矩阵。在这种情况下，我们称 A_x 为 $\{M_{a|x}\}$的可观测量，并且有 $A_{(j)x} = A_x^j$。因此，
- 投影的测量完全由其可观测量刻画：

$$M_a = \frac{1}{|\mathcal{O}_A|} \sum_{j=0}^{|\mathcal{O}_A|-1} \omega^{-aj} A_x^j,$$

而一般来说，可能无法从A_x中恢复测量的 POVM元素。

在本研究中，我们用以下元组来指定量子策略

$$\mathcal{S}=(|\psi\rangle_{AB},\{A_x^{(j)}:x\in\mathcal{I}_A,j\in\mathcal{O}_A\},\{B_y^{(k)}:y\in\mathcal{I}_B,k\in\mathcal{O}_B\}),$$

其中 $A_x^{(j)}=\sum_{a=0}^{|\mathcal{O}_A|-1}\omega_A^{aj}M_{a|x}$, $\omega_A=e^{i2\pi/|\mathcal{O}_A|}$, $B_y^{(k)}=\sum_{b=0}^{|\mathcal{O}_B|-1}\omega_B^{bk}N_{b|y}$, $\omega_B=e^{i2\pi/|\mathcal{O}_B|}$。关联也可以方便地通过以下方式指定：

$$\{\langle\psi|A_x^{(j)}\otimes B_y^{(k)}|\psi\rangle\}_{j,k,x,y}=\{\sum_{a,b}\omega_A^{aj}\omega_B^{bk}p(ab|xy)\}_{j,k,x,y}.$$

此外，如果 $\mathcal{S}$ 中的所有测量都是投影的，我们就称 $\mathcal{S}$ 为投影的，并为简便起见将其记作 $\mathcal{S}=(|\psi\rangle_{AB},\ \{A_x:\ x\in\mathcal{I}_A\},\ \{B_y:\ y\in\mathcal{I}_B\})$。本文将以可观测量的形式给出结果。

2.2 局部扩张与自检验

在自检协议中，验证者 Victor 希望根据自己观察到的关联推断其背后的量子策略，因此，人们期望生成给定关联的策略在某种程度上是唯一的。然而，至少有两种对策略的操作不会影响关联。首先，如果我们只选择不同的基，那么对于任意局部酉算子 U_A，U_B，策略 $\mathcal{S}=(|\psi\rangle_{AB}$，$\{A_x^{(j)}\}$，$\{B_y^{(k)}\})$ 和 $\mathcal{S}'=(U_A\otimes U_B|\psi\rangle_{AB}$，$\{U_AA_x^{(j)}U_A^\dagger\}$，$\{U_BB_y^{(k)}U_B^\dagger\})$ 会产生相同的关联。其次，如果我们附加一个双部辅助态 $|\text{aux}\rangle_{A'B'}$，且测量在其上平凡作用，那么策略 $\mathcal{S}=(|\psi\rangle_{AB}$，$\{A_x^{(j)}\}$，$\{B_y^{(k)}\})$ 和 $\mathcal{S}'=(|\text{aux}\rangle_{A'B'}\otimes|\psi\rangle_{AB}$，$\{I\otimes A_x^{(j)}\}$，$\{I\otimes B_y^{(k)}\})$ 会产生相同的关联。受上述两种操作的启发，如果在局部基变换下，$\mathcal{S}$ 等于 $\mathcal{S}$ 加上某个平凡的辅助态，我们就称“$\tilde{\mathcal{S}}$ 是 $\mathcal{S}$ 的局部扩张”。具体而言，我们称

定义 2.1（局部扩张）局部算子 $M_{\tilde{A}}\otimes N_{\tilde{B}}$ 和双部态 $|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}}$ 是算子 $M_A\otimes N_B$ 和量子态 $|\psi\rangle_{AB}$ 的局部扩张，其辅助态为 $|\text{aux}\rangle_{A'B'}\in\mathcal{H}_{A'}\otimes\mathcal{H}_{B'}$，局部等距映射为 $\Phi=\Phi_A\otimes\Phi_B$，其中 $\Phi_A:\ \mathcal{H}_A\to\mathcal{H}_{A'}\otimes\mathcal{H}_{\tilde{A}}$，$\Phi_B:\ \mathcal{H}_B\to\mathcal{H}_{B'}\otimes\mathcal{H}_{\tilde{B}}$，若

$$\Phi[M_A\otimes N_B|\psi\rangle_{AB}]=|\text{aux}\rangle_{A'B'}\otimes(\tilde{M}_{\tilde{A}}\otimes\tilde{N}_{\tilde{B}}|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}}).$$

我们将局部扩张记为

$$(|\psi\rangle_{AB},M_A\otimes N_B)\xhookrightarrow{\Phi,|\text{aux}\rangle}(|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}},\tilde{M}_{\tilde{A}}\otimes\tilde{N}_{\tilde{B}}),$$

如果根据上下文可以明确其含义，则省略箭头上方的 Φ、$|\text{aux}\rangle$。

策略 $\tilde{\mathcal{S}}=(|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}},\{\tilde{A}_x^{(j)}\}\ \{\tilde{B}_y^{(k)}\})$ 是策略 $\mathcal{S}=(|\psi\rangle_{AB},\{A_x^{(j)}\}\ \{B_y^{(k)}\})$的局部扩张，其辅助态为 $|\text{aux}\rangle_{A'B'}$，局部等距映射为 $\Phi=\Phi_A\otimes\Phi_B$，其中 $\Phi_A:\ \mathcal{H}_A\to\mathcal{H}_{A'}\otimes\mathcal{H}_{\tilde{A}}$，$\Phi_B:\ \mathcal{H}_B\to\mathcal{H}_{B'}\otimes\mathcal{H}_{\tilde{B}}$，若

$$(|\psi\rangle_{AB},A_x^{(j)}\otimes I_B)\xhookrightarrow{\Phi,|\text{aux}\rangle}(|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}},\tilde{A}_x^{(j)}\otimes I_{\tilde{B}}),$$
$$(|\psi\rangle_{AB},I_A\otimes B_y^{(k)})\xhookrightarrow{\Phi,|\text{aux}\rangle}(|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}},I_{\tilde{A}}\otimes\tilde{B}_y^{(k)})$$

对所有 $j\in\mathcal{O}_A$，$k\in\mathcal{O}_B$，$x\in\mathcal{I}_A$，$y\in\mathcal{I}_B$。我们用 $\mathcal{S}\xhookrightarrow{\Phi,|\text{aux}\rangle}\tilde{\mathcal{S}}$ 表示策略的局部扩张

我们还使用钩箭头记号表示近似局部扩张：

定义 2.2（局部 ε-扩张）局部算子 $M_{\tilde{A}}\otimes N_{\tilde{B}}$ 和双部态 $|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}}$ 是算子 $M_A\otimes N_B$ 和量子态 $|\psi\rangle_{AB}$ 的局部 ε-扩张，其辅助态为 $|\text{aux}\rangle_{A'B'}\in\mathcal{H}_{A'}\otimes\mathcal{H}_{B'}$，局部等距映射为 $\Phi=\Phi_A\otimes\Phi_B$，其中 $\Phi_A:\ \mathcal{H}_A\to\mathcal{H}_{A'}\otimes\mathcal{H}_{\tilde{A}}$，$\Phi_B:\ \mathcal{H}_B\to\mathcal{H}_{B'}\otimes\mathcal{H}_{\tilde{B}}$，如果

$$\|\Phi[M_A\otimes N_B|\psi\rangle_{AB}]-|\text{aux}\rangle_{A'B'}\otimes(\tilde{M}_{\tilde{A}}\otimes\tilde{N}_{\tilde{B}}|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}})\|\le\varepsilon.$$

我们将局部 ε-扩张记作

$$(|\psi\rangle_{AB},M_A\otimes N_B)\xhookrightarrow[\varepsilon]{\Phi,|\text{aux}\rangle}(|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}},\tilde{M}_{\tilde{A}}\otimes\tilde{N}_{\tilde{B}}).$$

策略 $\tilde{\mathcal{S}} = (|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}}, \{\tilde{A}_x^{(j)}\}\ \{\tilde{B}_y^{(k)}\})$ 是策略 $\mathcal{S} = (|\psi\rangle_{AB}, \{A_x^{(j)}\}\ \{B_y^{(k)}\})$的局部 ε-扩张，其中辅助态为 $|$辅$\rangle_{A'B'}$，局部等距映射为 $\Phi = \Phi_A \otimes \Phi_B$，其中 $\Phi_A : \mathcal{H}_A \to \mathcal{H}_{A'} \otimes \mathcal{H}_{\tilde{A}}$,$\Phi_B : \mathcal{H}_B \to \mathcal{H}_{B'} \otimes \mathcal{H}_{\tilde{B}}$，若

$$(|\psi\rangle_{AB}, A_x^{(j)} \otimes I_B) \xhookrightarrow[\varepsilon]{\Phi, |\mathrm{aux}\rangle} (|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}}, \tilde{A}_x^{(j)} \otimes I_{\tilde{B}}),$$
$$(|\psi\rangle_{AB}, I_A \otimes B_y^{(k)}) \xhookrightarrow[\varepsilon]{\Phi, |\mathrm{aux}\rangle} (|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}}, I_{\tilde{A}} \otimes \tilde{B}_y^{(k)})$$

对所有 $j \in \mathcal{O}_A$、$k \in \mathcal{O}_B$、$x \in \mathcal{I}_A$、$y \in \mathcal{I}_B$ 均成立。我们用 $\mathcal{S} \overset{\Phi,\ |\ \rangle}{\hookrightarrow} \tilde{\mathcal{S}}^{\text{辅助态}}$ 表示策略的局部 ε-扩张。

现在我们可以定义策略的精确自检验和鲁棒自检验 $\mathcal{S}$:

定义 2.3（策略的自检验）如果任意生成相同关联的策略 $\mathcal{S}$ 都满足 $\mathcal{S} \overset{\Phi,\ |\ \rangle}{\hookrightarrow} \tilde{\mathcal{S}}^{\text{辅助态}}$，则策略 $\tilde{\mathcal{S}} = (|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}}, \{\tilde{A}_x^{(j)}\}\ \{\tilde{B}_y^{(k)}\})$ 被其生成的关联 $\{\langle\tilde{\psi}|\tilde{A}_x^{(j)} \otimes \tilde{B}_y^{(k)}|\tilde{\psi}\rangle\}$（精确地）自检验，其中 Φ 为某个局部等距映射，$|$辅助态$\rangle$ 为某个辅助态。

如果策略 $\tilde{\mathcal{S}} = (|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}}, \{\tilde{A}_x^{(j)}\}\ \{\tilde{B}_y^{(k)}\})$ 是自检验的，且满足以下条件，则称其由所生成的关联鲁棒自检验：对于任意 $\varepsilon > 0$，都存在 $\delta > 0$，使得任何以$\mathcal{S}$ δ近似生成该关联的策略（即，对于所有 x, y, j, k，均有 $|\langle\psi|A_x^{(j)} \otimes B_y^{(k)}|\psi\rangle - \langle\tilde{\psi}|\tilde{A}_x^{(j)} \otimes \tilde{B}_y^{(k)}|\tilde{\psi}\rangle| < \delta$）都满足 $\mathcal{S} \overset{\Phi,\ |\ \rangle}{\underset{\varepsilon}{\hookrightarrow}} \tilde{\mathcal{S}}^{\text{辅助态}}$，其中某个局部等距映射为 Φ，辅助态为 $|$辅助态$\rangle$。

在自检验的语境中，$\mathcal{S}$ 通常称为参考策略，而 $\mathcal{S}$ 称为物理策略。本文作出以下假设。首先，鉴于自检测量存在复共轭问题（详见 [ŠB20] 中的第 3.7.1 节），我们考虑“实数”参考策略。这里的“实数”是指，在 $|\psi\rangle$ 的施密特基下，$\mathcal{S}$ 中 POVM 的矩阵元素均为实数。其次，我们考虑投影参考策略。请回想，这类策略完全由其可观测量刻画。从这个意义上说，我们所说的“对可观测量进行自检验”，实质上是“对其对应的投影测量进行自检验”。我们注意到，尽管一些先前的自检验结果也假设物理策略是投影的，但我们并不要求物理策略是投影的或实数的。最后，我们不失一般性地假设“辅助”量子态 $|\mathrm{aux}\rangle$ 的左、右局部维数相同，即 *i.e.*, $\mathcal{H}_{A'} \cong \mathcal{H}_{B'}$，因为总可以通过局部等距映射扩充较小的边缘空间。我们还假设参考量子态 $|\psi\rangle$具有满施密特秩；请注意，这是自检验文献中非常常见的假设。因此，我们可以取 $\mathcal{H}_{\tilde{A}} \cong \mathcal{H}_{\tilde{B}}$。

3 投影测量的鲁棒事后自检

事后自检的概念已在先前的研究中得到隐含运用，例如图态的自检 [McK16], 随机性认证 [ABDC18、WKB+20]以及单边自检验[SBJ+23]。综述论文 [ŠB20] 首次总结了这项技术，并将其称为“事后自检”。本节将形式化地阐述事后自检的思想，并为其应用确立一个充分条件。

3.1 定义

在事后自检中，我们考虑这样一种情形：已有一个自检验的策略 $\tilde{\mathcal{S}} = (|\tilde{\psi}\rangle,\ \{\tilde{A}_x^{(j)}\}_x,\ \{\tilde{B}_y^{(k)}\}_y)$，并希望对一个额外的测量 $\{\tilde{O}^{(\ell)}\}$进行自检。我们想要探讨的是，何时可以通过扩展 $\{\tilde{O}^{(\ell)}\}$ 来对其进行自检 $\tilde{\mathcal{S}}$。具体而言，何时可以根据 $\tilde{\mathcal{S}}' = (|\tilde{\psi}\rangle,\ \{\tilde{A}_x^{(j)}\}_x,\ \{\tilde{B}_y^{(k)}, \tilde{O}^{(\ell)}\}_y)$所产生的关联对其进行自检（图2）？

由于参考策略 $\tilde{\mathcal{S}} = (|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}}, \{\tilde{A}_x^{(j)}\}\ \{\tilde{B}_y^{(k)}\})$ 可根据关联进行鲁棒自检验，爱丽丝必须如实执行某种测量，该测量是 $\{\tilde{A}_x^{(j)}\}$ 的近似局部扩张：

$$(|\psi\rangle_{AB}, A_x^{(j)} \otimes I_B) \xhookrightarrow[\varepsilon]{\Phi, |\mathrm{aux}\rangle} (|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}}, \tilde{A}_x^{(j)} \otimes I_{\tilde{B}}) \tag{1}$$

那么，针对附加可观测量 $\tilde{O}^{(l)}$ 的事后自检会要求：同一个 Φ 和 $|$辅助$\rangle$ 也在 同一个 共享态上，将 $O^{(l)}$ 和 $\tilde{O}^{(l)}$ 连接起来，对于任意生成的、与 $\tilde{O}^{(l)}$的关联接近的 $O^{(l)}$。

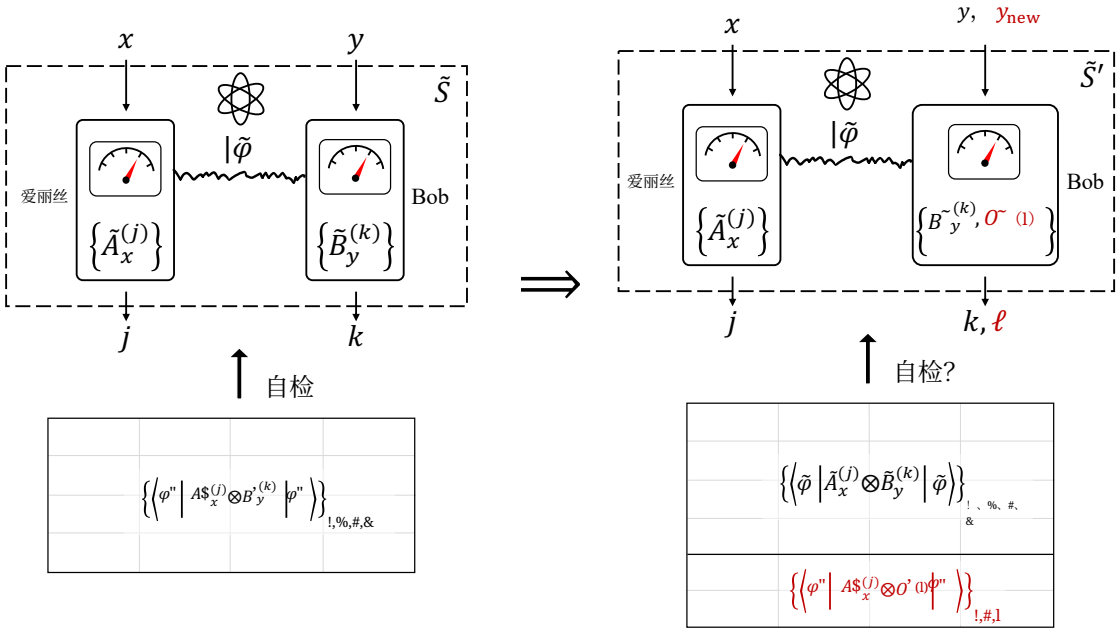

图 2：事后自检：从一个已自检验的策略 $\mathcal{S}$（左侧）出发，若能够根据关联 $\{\langle\psi|A_x^{(j)}\otimes O^{(\ell)}|\psi\rangle\}$ 推断出输入为 y_{new}、输出为 ℓ 的新测量$\tilde{O}^{(\ell)}$，则扩展策略 $\mathcal{S}'$（右侧）仍然是自检验的。

定义 3.1（鲁棒事后自检）给定量子态 $|\psi\rangle=|\psi\rangle_{\tilde{A}\tilde{B}}$和广义观测量$\{\tilde{A}_x^{(j)}\}$，如果满足以下条件，则称 L输出广义观测量 $\{\tilde{O}^{(l)}\}$ 基于关联$\{\langle\tilde{\psi}|\tilde{A}_x^{(j)}\otimes\tilde{O}^{(l)}|\tilde{\psi}\rangle\}$被鲁棒事后自检 （基于 $(|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}},\{\tilde{A}_x^{(j)}\})$ ）：对于任意 $\varepsilon'>0$，存在 $\varepsilon>0$ 和 $\delta>0$，使得：

若 $(|\psi\rangle_{AB}、A_x^{(j)}\otimes I_B)\xrightarrow[\varepsilon]{\Phi|\quad\rangle}$，辅助 $(|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}}、\tilde{A}_x^{(j)}\otimes I_{\tilde{B}}\}$对于量子态$|\psi\rangle_{AB}$、广义观测量 $\{A_x^{(j)}\}$、局部等距映射$\Phi=\Phi_A\otimes\Phi_B$以及量子态$|$辅助$\rangle_{A'B'}$，则任何以近似方式生成该关联的广义观测量$\{O^{(l)}\}$ δ（即 $|\langle\psi|A_x^{(j)}\otimes O^{(l)}|\psi\rangle-\langle\tilde{\psi}|\tilde{A}_x^{(j)}\otimes\tilde{O}_y^{(l)}|\tilde{\psi}\rangle|<\delta$）都满足

$$(|\psi\rangle_{AB},I_A\otimes O^{(l)})\xrightarrow[\varepsilon']{\Phi,|\text{aux}\rangle}(|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}},I_{\tilde{A}}\otimes\tilde{O}^{(l)}),$$

对所有 $l\in[0,L-1]$。

那么，事后自检在以下意义上扩展了自检协议：

命题 3.2 如果关联 $\{\langle\tilde{\psi}|\tilde{A}_x^{(j)}\otimes\tilde{B}_y^{(k)}|\tilde{\psi}\rangle\}$ 稳健地自检验 $\tilde{\mathcal{S}}=(|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}},\{\tilde{A}_x^{(j)}\}\ \{\tilde{B}_y^{(k)}\})$，且关联 $\{\langle\tilde{\psi}|\tilde{A}_x^{(j)}\otimes\tilde{O}^{(k)}|\tilde{\psi}\rangle\}$ 基于 $(|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}},\{\tilde{A}_x^{(j)}\})$ 稳健地进行事后自检 $\{\tilde{O}^{(l)}\}$，那么扩展相关性 $\{\langle\tilde{\psi}|\tilde{A}_x^{(j)}\otimes\tilde{B}_y^{(k)}|\tilde{\psi}\rangle\}\cup\{\langle\tilde{\psi}|\tilde{A}_x^{(j)}\otimes\tilde{O}^{(l)}|\tilde{\psi}\rangle\}$ 将稳健地自检验扩展策略 $\tilde{\mathcal{S}}^{Extend}=(|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}},\{\tilde{A}_x^{(j)}\},\{\tilde{B}_y^{(k)},\tilde{O}^{(l)}\})$。

证明。 根据鲁棒事后自检，对于任意 ε_1，存在 ε_2 和 δ_1，使得

$$(|\psi\rangle_{AB},I_A\otimes O^{(l)})\xrightarrow[\varepsilon_1]{\Phi,|\text{aux}\rangle}(|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}},I_{\tilde{A}}\otimes\tilde{O}^{(l)}),$$

如果 $|\langle\psi|A_x^{(j)}\otimes O^{(l)}|\psi\rangle-\langle\tilde{\psi}|\tilde{A}_x^{(j)}\otimes\tilde{O}_y^{(l)}|\tilde{\psi}\rangle|<\delta_1$。由于 $\tilde{\mathcal{S}}=(|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}},\{\tilde{A}_x^{(j)}\},\{\tilde{B}_y^{(k)}\})$ 是鲁棒自检的，对于 ε_2，存在 δ_2 使得

$$(|\psi\rangle_{AB},A_x^{(j)}\otimes I_B)\xrightarrow[\varepsilon_2]{\Phi,|\text{aux}\rangle}(|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}},\tilde{A}_x^{(j)}\otimes I_{\tilde{B}}),$$
$$(|\psi\rangle_{AB},I_A\otimes B_y^{(k)})\xrightarrow[\varepsilon_2]{\Phi,|\text{aux}\rangle}(|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}},I_{\tilde{A}}\otimes\tilde{B}_y^{(k)}),$$

如果 $|\langle\psi|A_x^{(j)}\otimes B_y^{(k)}|\psi\rangle-\langle\tilde{\psi}|\tilde{A}_x^{(j)}\otimes\tilde{B}_y^{(k)}|\tilde{\psi}\rangle|<\delta_2$。取 $\delta=$ 最小值$\{\delta_1,\delta_2\}$和 $\varepsilon=$ 最大值$\{\varepsilon_1,\varepsilon_2\}$，可得扩展策略 $\tilde{\mathcal{S}}^{Extend}=(|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}},\{\tilde{A}_x^{(j)}\},\{\tilde{B}_y^{(k)},\tilde{O}^{(l)}\})$ 是鲁棒自检的。■

我们将关联表的扩展可视化，以便更好地理解事后自检。为简单起见，考虑二元可观测量 A_x,B_y,O。由 $\mathcal{S}$ 生成的关联可以写成如表1所示的$(|\mathcal{I}_A|+1)\times(|\mathcal{I}_B|+1)$表。于是我们称表1自检验策略 $\mathcal{S}$。以 $\mathcal{S}$ 为初始策略，然后在鲍勃一侧添加一个额外的二元可观测量 O；这将扩展关联表，如表2所示。直观地说，给定自检验的 $\{A_x\}$，那么对于某个 O，可能会出现这样的情况：O 完全由 $\langle I\otimes O\rangle$ 和 $\{\langle A_x\otimes O\rangle\}_x$ 刻画。若如此，我们称 O 基于 $\{A_x\}$ 和 $|\tilde{\psi}\rangle$得到事后自检验。于是扩展后的表2自检验 $\tilde{\mathcal{S}}^{Extend}$，因为本质上表2的白色部分检验 $\mathcal{S}$，而黄色部分检验 O。

	I	$\tilde{B}_0$	...	$\tilde{B}_{Y-1}$
I	$\langle A_0,$	$\langle I, B_0\rangle_{\tilde{\psi}}$ $\langle A_0,$	...	$\langle I, B_{Y-1}\rangle_{\tilde{\psi}}$ $\langle A_0,$
$\tilde{A}_0$	$I\rangle_{\tilde{\psi}}$	$B_0\rangle_{\tilde{\psi}}$	...	$B_{Y-1}\rangle_{\tilde{\psi}}$
...	$\langle A_{X-1},$	...	...	... ...
$\tilde{A}_{X-1}$	$I\rangle_{\tilde{\psi}}$	$\langle A_{X-1}, B_0\rangle_{\tilde{\psi}}$	...	$\langle A_{X-1}, B_{Y-1}\rangle_{\tilde{\psi}}$

表1：初始关联表。这里 $\langle A,\ B\rangle_{\tilde{\psi}}$ 是 $\langle\psi|A\otimes B|\psi\rangle$的简写，并且我们取 $X=|\mathcal{I}_A|,Y=|\mathcal{I}_B|$。

	I	$\tilde{B}_0$	...	$\tilde{B}_{Y-1}$	$\tilde{O}$
I	$\langle A_0,$	$\langle I, B_0\rangle_{\tilde{\psi}}$ $\langle A_0,$	...	$\langle I, B_{Y-1}\rangle_{\tilde{\psi}}\langle A_0,$	$\langle I, O\rangle_{\tilde{\psi}}$
$\tilde{A}_0$	$I\rangle_{\tilde{\psi}}$	$B_0\rangle_{\tilde{\psi}}$	...	$B_{Y-1}\rangle_{\tilde{\psi}}$	$\langle A_0,\ O\rangle_{\tilde{\psi}}$
...	$\langle A_{X-1},$	...	...	... ...	...
$\tilde{A}_{X-1}$	$I\rangle_{\tilde{\psi}}$	$\langle A_{X-1},\ B_0\rangle_{\tilde{\psi}}$	...	$\langle A_{X-1},\ B_{Y-1}\rangle_{\tilde{\psi}}$	$\langle A_{X-1},\ O\rangle_{\tilde{\psi}}$

表2：扩展相关表。

从现在起，我们分别将 $\tilde{\mathcal{S}}$，$|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}}$，$\{\tilde{A}_x^{(j)}\}$ 称为初始策略、初始态和初始广义观测量，并将 $\tilde{O}^{(l)}$ 称为额外广义观测量。

3.2 投影策略的鲁棒事后自检判据

给定初始广义观测量 $\{A_x\}$ 以及初始态 $|\psi\rangle$，什么样的广义观测量 $\tilde{O}$ 能够基于 $(|\tilde{\psi}\rangle,\ \tilde{A}_x)$ 进行事后自检？直观地说，如果 $\{\langle\tilde{\psi}|(\tilde{A}_x^{(j)}\otimes\tilde{O}^{(\ell)})|\tilde{\psi}\rangle\}_x$ 能够为所有 ℓ 完整刻画 $\{\tilde{O}^{(\ell)}\}$，那么鲍勃也别无选择，只能诚实地对 $\tilde{O}^{(\ell)}$ 在 $|\tilde{\psi}\rangle$上执行局部扩张。这就给出了一个事后自检判据。在证明这一判据时，以下民间常识的一个版本很有用："任意向量都由其与基向量的内积唯一确定。"具体而言，

引理 3.3 设 $\tilde{v}_0,\ldots,\tilde{v}_{n-1}$ 是希尔伯特空间中的线性无关向量。设 $v_0,\ldots,v_{n-1}$ 是一组相近的向量（以内积 $\|a\|=\sqrt{\langle a,a\rangle}$ 所诱导的范数度量），

$$\forall x\in[0,n-1],\|v_x-\tilde{v}_x\|<\varepsilon.$$

对于任意一对向量 v 和 $\tilde{v}$，使得 $\langle v,v\rangle\leq\langle\tilde{v},\tilde{v}\rangle$ 和 $\tilde{v}\in$张成空间$_{\mathbb{C}}\{v_0,\ldots,v_{n-1}\}$，若

$$\forall x\in[0,n-1],|\langle v_x,v\rangle-\langle\tilde{v}_x,\tilde{v}\rangle|<\delta$$

then

$$\|v-\tilde{v}\|\leq\left(\frac{4n}{\lambda_{\min}(G)}\right)^{\frac{1}{4}}(\varepsilon\|\tilde{v}\|+\delta)^{\frac{1}{2}}\|\tilde{v}\|^{\frac{1}{2}},$$

其中，G 是 $\tilde{v}_0$、.....、$\tilde{v}_{n-1}$ 的格拉姆矩阵，其元素为 $g_{jk}=\langle\tilde{v}_j,\ \tilde{v}_k\rangle$，而 $\lambda_{\min}(G)$ 是 G的最小特征值。

证明。 由于 $\tilde{v} \in$ 张成$_{\mathbb{C}}\{\tilde{v}_0, \ldots, \tilde{v}_{n-1}\}$，令 $\tilde{v} = \sum_x \alpha_x \tilde{v}_x = W\alpha$，其中

$$W = \begin{pmatrix} | & & | \\ \tilde{v}_0 & \cdots & \tilde{v}_{n-1} \\ | & & | \end{pmatrix},$$

then

$$\begin{aligned}
\|v - \tilde{v}\|^2 =& \|v\|^2 + \|\tilde{v}\|^2 - 2\,\mathrm{Re}\,\langle v, \tilde{v}\rangle \\
=& \|v\|^2 + \|\tilde{v}\|^2 - 2\|\tilde{v}\|^2 - 2\,\mathrm{Re}\,\langle v - \tilde{v}, \tilde{v}\rangle \\
\leq& -2\,\mathrm{Re}\,\langle v - \tilde{v}, \tilde{v}\rangle \\
\leq& 2|\,\langle v - \tilde{v}, \tilde{v}\rangle\,| \\
=& 2|\sum_{x=0}^{n-1} \alpha_x \,\langle v - \tilde{v}, \tilde{v}_x\rangle\,| \\
\leq& 2\sum_{x=0}^{n-1} |\alpha_x| \cdot |\,\langle v, \tilde{v}_x\rangle - \langle \tilde{v}, \tilde{v}_x\rangle\,| \\
=& 2\sum_{x=0}^{n-1} |\alpha_x| \cdot |\,\langle v, \tilde{v}_x\rangle - \langle v, v_x\rangle + \langle v, v_x\rangle - \langle \tilde{v}, \tilde{v}_x\rangle\,| \\
\leq& 2\sum_{x=0}^{n-1} |\alpha_x| \cdot (\varepsilon\|v\| + \delta) \\
\leq& 2\|\alpha\|_1(\varepsilon\|\tilde{v}\| + \delta),
\end{aligned}$$

其中，$\|\cdot\|_1$ 是向量1-范数。利用向量范数不等式，我们有

$$\begin{aligned}
\|\alpha\|_1 \leq& \sqrt{n}\|\alpha\| \\
=& \sqrt{n}\|(W^\dagger W)^{-1}W^\dagger W\alpha\| \\
\leq& \sqrt{n}\|(W^\dagger W)^{-1}W^\dagger\|_\infty\|W\alpha\|,
\end{aligned}$$

其中，$\|\cdot\|_\infty$ 是算子的谱范数（Schatten ∞-范数）。

注意，W 存在奇异值分解 $W = V\Sigma U^\dagger$，其中 V 是等距变换，U 是酉算子，而 $\Sigma = \mathrm{diag}(\sigma_0, \ldots, \sigma_{n-1})$ 是正定的。于是 $G = W^\dagger W = U\Sigma^2 U^\dagger$。因此

$$\|(W^\dagger W)^{-1}W^\dagger\|_\infty = \|(U\Sigma^2U^\dagger)^{-1}U\Sigma V^\dagger\|_\infty = \|U\Sigma^{-1}V^\dagger\|_\infty = \sigma_{\max}(U\Sigma^{-1}V^\dagger) = \frac{1}{\sqrt{\lambda_{\min}(G)}}.$$

最后，

$$\begin{aligned}
\|v - \tilde{v}\|^2 \leq& 2\|\alpha\|_1(\varepsilon\|\tilde{v}\| + \delta) \\
\leq& 2\sqrt{n}\|(W^\dagger W)^{-1}W^\dagger\|_\infty\|W\alpha\|(\varepsilon\|\tilde{v}\| + \delta) \\
=& \frac{2\sqrt{n}}{\sqrt{\lambda_{\min}(G)}}(\varepsilon\|\tilde{v}\| + \delta)\|\tilde{v}\| \\
\Longrightarrow \quad \|v - \tilde{v}\| \leq& \left(\frac{4n}{\lambda_{\min}(G)}\right)^{\frac{1}{4}} (\varepsilon\|\tilde{v}\| + \delta)^{\frac{1}{2}}\,\|\tilde{v}\|^{\frac{1}{2}}.
\end{aligned}$$

■

引理3.3 关于酉算子的类似结论对下述命题至关重要。从现在起，我们假设参考策略的量子态是在施密特基下给出的。

命题 3.4 设 $|\psi\rangle_{\tilde{A}\tilde{B}} \in \mathcal{H}_{\tilde{A}} \otimes \mathcal{H}_{\tilde{B}}$ 是一个量子态，$\{A_x\}$、$x \in [0, n-1]$ 是 $\mathcal{L}(H_{\tilde{A}})$ 中的酉算子。假设 $O \in \mathcal{L}(H_{\tilde{B}})$ 是一个酉算子，使得

$$\bar{\tilde{O}}P \in \mathrm{span}_{\mathbb{C}}\{D\tilde{A}_x D\}$$

其中 P是正定的，且 $D=\mathrm{vec}^{-1}(|\tilde{\psi}\rangle)$ =对角矩阵(λ_0, ..., λ_{d-1})，其中 λ_j 是 $|\psi\rangle$的施密特系数。

若量子态 $|\psi\rangle_{AB}\in\mathcal{H}_A\otimes\mathcal{H}_B$、|辅助$\rangle\in\mathcal{H}_{A'}\otimes\mathcal{H}_{B'}$、压缩算子 $\{A_x\}$ *in* $\mathcal{L}(H_A)$、压缩算子 $O\in\mathcal{L}(\mathcal{H}_B)$以及局部等距映射 $\Phi=\Phi_A\otimes\Phi_B$： $\mathcal{H}_A\otimes\mathcal{H}_B\to(\mathcal{H}_{\tilde{A}}\otimes\mathcal{H}_{A'})\otimes(\mathcal{H}_{\tilde{B}}\otimes\mathcal{H}_{B'})$ 满足

$$\begin{aligned}
&\forall x,\ (|\psi\rangle_{AB},A_x\otimes I_B)\xhookrightarrow[\varepsilon]{\Phi,|\mathrm{aux}\rangle}(|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}},\tilde{A}_x\otimes I_{\tilde{B}}),\\
&|\psi\rangle_{AB}\xhookrightarrow[\varepsilon]{\Phi,|\mathrm{aux}\rangle}|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}},\\
&|\langle\psi|A_x\otimes O|\psi\rangle-\langle\tilde{\psi}|\tilde{A}_x\otimes\tilde{O}|\tilde{\psi}\rangle|<\delta,
\end{aligned}$$

则 $(|\psi\rangle_{AB}$、 $I_A\otimes O)\xhookrightarrow[\varepsilon']{\Phi|\quad\rangle}$, 辅助$(|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}}$、 $I_{\tilde{A}}\otimes\tilde{O})$，其中

$$\varepsilon'=\left(\frac{n}{\lambda_{\min}(G)}\right)^{\frac{1}{4}}\left(2\frac{\mathrm{Tr}\,Q}{\lambda_{\min}(Q)}\kappa(D)\right)^{\frac{1}{2}}\left(\left(2\left(\frac{\mathrm{Tr}\,Q}{\lambda_{\min}(Q)}\right)^{\frac{1}{2}}\lambda_{\max}(D)+1\right)\varepsilon+\delta\right)^{\frac{1}{2}}+\varepsilon. \quad (2)$$

这里， $Q=D^{-1}PD^{-1}$、 G 是 $\{\tilde{A}_x\}$ 的格拉姆矩阵，其元素为 $g_{jk}=\mathrm{Tr}[\tilde{A}_j^\dagger\tilde{A}_k]$； $\kappa(D)$ 是 D 的~条件数，即 $|\psi\rangle$的最大与最小施密特系数之比。

证明。定义

$$\begin{aligned}
\tilde{v}_x&:=D'\otimes\sqrt{P}^{-1}D\tilde{A}_x^\dagger D,\\
v_x&:=(I\otimes\sqrt{P^{-1}}D)(\Phi_A A_x^\dagger\Phi_A^\dagger)(D'\otimes D),\\
\tilde{v}&:=(D'\otimes\sqrt{P})(I_{B'}\otimes\tilde{O}^\intercal)=D'\otimes\sqrt{P}\tilde{O}^\intercal,\\
v&:=(D'\otimes\sqrt{P})(\Phi_B O\Phi_B^\dagger)^\intercal.
\end{aligned}$$

其中 $D'=\mathrm{vec}^{-1}$(|aux$\rangle$)。我们还考虑以施密特基表示的 |aux$\rangle$，因此 D' 是对角矩阵（但不一定是满秩的）。注意，$\mathrm{Tr}[D'^2]=\mathrm{Tr}[\rho_A]=1$。格拉姆矩阵 G'中对应于 $\{\tilde{v}_x\}$ 的元素为 $g'_{jk}=$Tr $[\tilde{v}_j^\dagger\tilde{v}_k]=Tr[(D^{-1}PD^{-1})^{-1}\tilde{A}_k^\dagger D^2\tilde{A}_j]=Tr[(Q)^{-1}\tilde{A}_k^\dagger D^2\tilde{A}_j]$。比较 G 和 G' 的最小特征值，可得

$$\lambda_{\min}(G')\geq\lambda_{\min}(G)\lambda_{\min}(D^2)\lambda_{\min}(Q^{-1})=\frac{\lambda_{\min}(G)\lambda_{\min}^2(D)}{\lambda_{\max}(Q)}>\frac{\lambda_{\min}(G)\lambda_{\min}^2(D)}{\mathrm{Tr}\,Q}.$$

应用引理3.3时，需检查以下条件：

- $\tilde{v}\in$张成空间$_{\mathbb{C}}\{\tilde{v}_x\}$:

$$\begin{aligned}
&\bar{\tilde{O}}P\in\mathrm{span}_{\mathbb{C}}\{D\tilde{A}_xD\}\\
\Rightarrow\quad&P(\tilde{O})^\intercal\in\mathrm{span}_{\mathbb{C}}\{D\tilde{A}_x^\dagger D\}\\
\Rightarrow\quad&D'\otimes\sqrt{P}(\tilde{O})^\intercal\in\mathrm{span}_{\mathbb{C}}\{D'\otimes\sqrt{P}^{-1}D\tilde{A}_x^\dagger D\}\\
\Rightarrow\quad&\tilde{v}\in\mathrm{span}_{\mathbb{C}}\{\tilde{v}_x\}.
\end{aligned}$$

- $\|v\|\leq\|\tilde{v}\|$:

$$\begin{aligned}
\|\tilde{v}\|=&\sqrt{\mathrm{Tr}[D'^2\otimes\sqrt{P}(\tilde{O})^\intercal((\tilde{O})^\intercal)^\dagger\sqrt{P}]}=\sqrt{\mathrm{Tr}[P]},\\
\|v\|=&\sqrt{\mathrm{Tr}[(\Phi_B O\Phi_B^\dagger)^\intercal(D'\otimes\sqrt{P})(D'\otimes\sqrt{P})((\Phi_B O\Phi_B^\dagger)^\intercal)^\dagger]}\\
=&\sqrt{\mathrm{Tr}[(\Phi_B O\Phi_B^\dagger)^\dagger(D'^2\otimes\overline{P})(\Phi_B O\Phi_B^\dagger)]}\\
=&\sqrt{\mathrm{Tr}[(D'^2\otimes\overline{P})\Phi_B O\Phi_B^\dagger\Phi_B(O)^\dagger\Phi_B^\dagger]}\\
\leq&\sqrt{\mathrm{Tr}[(D'^2\otimes\overline{P})\Phi_B\Phi_B^\dagger]}\\
\leq&\sqrt{\mathrm{Tr}[(D'^2\otimes\overline{P})]}\\
=&\sqrt{\mathrm{Tr}[P]}=\|\tilde{v}\|,
\end{aligned}$$

其中，第一个不等式由 O 是压缩算子得出，第二个不等式则由 $\Phi_B\Phi_B^\dagger \le I_{\tilde{B}B'}$ 和 $D'^2 \otimes P \ge 0$ 得出。

- 对所有 x、 v_x 和 $\tilde{v}_x$ 都很接近：

$$\begin{aligned}
\|v_x - \tilde{v}_x\| \le& \|(\Phi_A A_x^\dagger \Phi_A^\dagger)(D' \otimes D) - D' \otimes \tilde{A}_x^\dagger D\| \|\sqrt{P^{-1}} D\|_\infty \\
=& \|(D' \otimes D)(\Phi_A A_x^\dagger \Phi_A^\dagger) - D' \otimes D\tilde{A}_x^\dagger\| \|\sqrt{P^{-1}} D\|_\infty \\
=& \|(\Phi_A A_x \Phi_A^\dagger)(D' \otimes D) - D' \otimes \tilde{A}_x D\| \|\sqrt{P^{-1}} D\|_\infty \\
=& \|(\Phi_A A_x \Phi_A^\dagger \otimes I)(|\mathrm{aux}\rangle \otimes |\tilde{\psi}\rangle) - |\mathrm{aux}\rangle \otimes (\tilde{A}_x \otimes I\,|\tilde{\psi}\rangle)\| \|\sqrt{P^{-1}} D\|_\infty \\
\le& (\|(\Phi_A A_x \Phi_A^\dagger \otimes I)\Phi[|\psi\rangle] - |\mathrm{aux}\rangle \otimes (\tilde{A}_x \otimes I\,|\tilde{\psi}\rangle)\| + \varepsilon) \|\sqrt{P^{-1}} D\|_\infty \\
=& (\|\Phi[A_x \otimes I\,|\psi\rangle] - |\mathrm{aux}\rangle \otimes (\tilde{A}_x \otimes I\,|\tilde{\psi}\rangle)\| + \varepsilon) \|\sqrt{P^{-1}} D\|_\infty \\
=& \frac{2\varepsilon}{\lambda_{\min}(D^{-1}PD^{-1})^{\frac{1}{2}}} = \frac{2\varepsilon}{\lambda_{\min}(Q)^{\frac{1}{2}}}.
\end{aligned}$$

- 内积很接近：

$$\begin{aligned}
&|\langle v_x, v\rangle - \langle \tilde{v}_x, \tilde{v}\rangle| \\
=& |\langle (I \otimes \sqrt{P^{-1}} D)(\Phi_A A_x^\dagger \Phi_A^\dagger)(D' \otimes D), (D' \otimes \sqrt{P})(\Phi_B O \Phi_B^\dagger)\rangle - \langle \tilde{v}_x, \tilde{v}\rangle| \\
=& |\langle D' \otimes D, (\Phi_A A_x \Phi_A^\dagger)(I \otimes D\sqrt{P^{-1}})(D' \otimes \sqrt{P})(\Phi_B O \Phi_B^\dagger)\rangle - \langle \tilde{v}_x, \tilde{v}\rangle| \\
=& |\langle D' \otimes D, (\Phi_A A_x \Phi_A^\dagger)(D' \otimes D)(\Phi_B O \Phi_B^\dagger)\rangle - \langle \tilde{v}_x, \tilde{v}\rangle| \\
=& |\langle |\mathrm{aux}\rangle \otimes |\tilde{\psi}\rangle, (\Phi_A A_x \Phi_A^\dagger \otimes \Phi_B O \Phi_B^\dagger)(|\mathrm{aux}\rangle \otimes |\tilde{\psi}\rangle)\rangle - \langle \tilde{v}_x, \tilde{v}\rangle| \\
\le& |\langle \Phi[|\psi\rangle], (\Phi_A A_x \Phi_A^\dagger \otimes \Phi_B O \Phi_B^\dagger)\Phi[|\psi\rangle]\rangle - \langle \tilde{v}_x, \tilde{v}\rangle| + 2\varepsilon \\
=& |\langle |\psi\rangle, A_x \otimes O\,|\psi\rangle\rangle - \langle \tilde{v}_x, \tilde{v}\rangle| + 2\varepsilon \\
=& |\langle \psi| A_x \otimes O |\psi\rangle - \langle \tilde{\psi}| \tilde{A}_x \otimes \tilde{O} |\tilde{\psi}\rangle| + \varepsilon < \delta + 2\varepsilon.
\end{aligned}$$

因此，引理3.3 的所有条件3.3均成立。根据引理，我们有

$$\begin{aligned}
\|v - \tilde{v}\| &\le \left(\frac{4n}{\lambda_{\min}(G')}\right)^{\frac{1}{4}} \left(\frac{2}{\lambda_{\min}(Q)^{\frac{1}{2}}}\varepsilon (\operatorname{Tr} P)^{\frac{1}{2}} + \delta + 2\varepsilon\right)^{\frac{1}{2}} (\operatorname{Tr} P)^{\frac{1}{4}} \\
&= \left(\frac{4n \operatorname{Tr}(P) \operatorname{Tr}(Q)}{\lambda_{\min}(G)\lambda_{\min}(D)^2}\right)^{\frac{1}{4}} \left(\left(2\left(\frac{\operatorname{Tr} P}{\lambda_{\min}(Q)}\right)^{\frac{1}{2}} + 2\right)\varepsilon + \delta\right)^{\frac{1}{2}} \\
&= \left(\frac{4n(\operatorname{Tr} Q)^2 \lambda_{\max}(D)^2}{\lambda_{\min}(G)\lambda_{\min}(D)^2}\right)^{\frac{1}{4}} \left(\left(2\left(\frac{\operatorname{Tr} Q}{\lambda_{\min}(Q)}\right)^{\frac{1}{2}} \lambda_{\max}(D) + 2\right)\varepsilon + \delta\right)^{\frac{1}{2}} \\
&= \left(\frac{n}{\lambda_{\min}(G)}\right)^{\frac{1}{4}} (2(\operatorname{Tr} Q)\kappa(D))^{\frac{1}{2}} \left(\left(2\left(\frac{\operatorname{Tr} Q}{\lambda_{\min}(Q)}\right)^{\frac{1}{2}} \lambda_{\max}(D) + 2\right)\varepsilon + \delta\right)^{\frac{1}{2}},
\end{aligned}$$

这意味着

$$\begin{aligned}
&\|\Phi[I \otimes O\,|\psi\rangle] - |\mathrm{aux}\rangle \otimes (I_{\tilde{A}} \otimes \tilde{O}\,|\tilde{\psi}\rangle)\| \\
\le& \|I_{\tilde{A}A'} \otimes \Phi_B O \Phi_B^\dagger (|\mathrm{aux}\rangle \otimes |\tilde{\psi}\rangle) - |\mathrm{aux}\rangle \otimes (I_{\tilde{A}} \otimes \tilde{O}\,|\tilde{\psi}\rangle)\| + \varepsilon \\
=& \|(D' \otimes D)(\Phi_B O \Phi_B^\dagger)^\intercal - (D' \otimes D)(I_{B'} \otimes \tilde{O}^\intercal)\| + \varepsilon \\
\le& \|v - \tilde{v}\| \|\sqrt{P^{-1}} D\|_\infty + \varepsilon \\
\le& \left(\frac{n}{\lambda_{\min}(G)}\right)^{\frac{1}{4}} \left(2\frac{\operatorname{Tr} Q}{\lambda_{\min}(Q)}\kappa(D)\right)^{\frac{1}{2}} \left(\left(2\left(\frac{\operatorname{Tr} Q}{\lambda_{\min}(Q)}\right)^{\frac{1}{2}} \lambda_{\max}(D) + 2\right)\varepsilon + \delta\right)^{\frac{1}{2}} + \varepsilon.
\end{aligned}$$

■

命题3.4的一些说明：

1. 若固定 $P = I$，则命题3.4 的判据$O \in$ 张成空间$\{DA_xD\}$，这可以从以下事实预见：$\langle\tilde{\psi}|\tilde{A}_x \otimes \tilde{O}|\tilde{\psi}\rangle = \mathrm{Tr}[D\tilde{A}_xD\tilde{O}^\intercal] = \langle D\tilde{A}_x^\dagger D,\ \tilde{O}^\intercal\rangle$。然而，我们的结果允许比 O 的线性组合更一般的 $\{DA_xD\}$。

2. 当 ε, δ 较小时，我们有 $\varepsilon' = O(\sqrt{C\varepsilon + \delta})$。如果初始策略具有显式的 $\varepsilon - \delta$ 依赖关系，根据命题3.4，扩展策略也将具有显式的鲁棒性。

3. 在镜像情形下，若爱丽丝一侧有额外的酉 O，而鲍勃的酉为 B_y，则判据类似：

$$\bar{\tilde{O}}P_j \in \mathrm{span}_{\mathbb{C}}\{D\tilde{B}_yD\}.$$

4. 在公式（2）中，$\kappa(D)$ 和 $\lambda_{\max}(D)$ 意味着更多的纠缠能够带来更强的鲁棒性，这很直观：设想 $|\psi\rangle$ 的纠缠较弱（这会导致较大的 $\kappa(D)$），那么爱丽丝和鲍勃之间的关联就很弱，以至于我们无法从 O 控制 $\{A_x^{(j)}\}$。

现在我们可以给出 O 基于 $(|\psi\rangle, A_x\}$. 满足事后自检验条件的充分条件。如果命题 3.4 中的条件对广义可观测量 O 的所有次幂均成立（如定义 2.1所要求），我们便立即得到以下判据：

定理 3.5 由可观测量 $\{O\}$ 表征的另一个 L 输出投影测量，基于经过鲁棒自检的初始可观测量 $\{A_x\}$ 和初始态 $|\psi\rangle_{\tilde{A}\tilde{B}}$，若存在正定算子 $P_l > 0$ 使得，则可对其进行鲁棒的事后自检。

$$\bar{\tilde{O}}^l P_l \in \mathrm{span}_{\mathbb{C}}\{D\tilde{A}_x^j D : x, j\},$$

对每个 $l \in [0, L-1]$ 均成立。这里 $D = \mathrm{vec}^{-1}(|\tilde{\psi}\rangle) = \mathrm{diag}(\lambda_1, ..., \lambda_d)$，其中 λ_j 是 $|\tilde{\psi}\rangle$ 的施密特系数。此外，鲁棒性对 $(\varepsilon',\ (\varepsilon,\ \delta))$ 的依赖关系将为 $\varepsilon' = O(\sqrt{C\varepsilon + \delta})$。

证明。对于每个 $l \in [0, L-1]$，注意到 $\tilde{A}_x^j$，$\tilde{O}^l$ 是酉算子，$A_x^{(j)}$，$O^{(l)}$ 是压缩算子，因此可以应用命题 3.4 得到 $\varepsilon_l' = O(\sqrt{C\varepsilon + \delta})$，根据式（2）。取 $\varepsilon' = \max_l\{\varepsilon_l'\} = O(\sqrt{C\varepsilon + \delta})$ 即可得到所需的结论。■

给定具体的 $|\tilde{\psi}\rangle$，$\{\tilde{A}_x\}$ $\tilde{O}$，条件 $\tilde{O}^l P_l \in$ 张成空间$_{\mathbb{C}}\{D\tilde{A}_x^j D\}$ 可以通过可行性半定规划（半定规划）确定。此外，由于 P_l 具有缩放自由度，且 $Q_l = D^{-1}P_lD^{-1}$是正定的，我们不失一般性地取 $\lambda_{\min}(Q_l) = 1$，并通过以下半定规划最小化 $\mathrm{Tr}\, Q_l$，以获得更好的鲁棒性：

$$\begin{aligned} \min \quad & \mathrm{Tr}\, Q_l \\ \text{s. t.} \quad & \bar{\tilde{O}}^l DQ_lD = \sum_{j,x} c_{j,x,l} D\tilde{A}_x^j D, \\ & Q_l \geq I, \\ & c_{j,x,l} \in \mathbb{C} \end{aligned}$$

对每个 k 分别进行。此外还要注意，定理 3.5 并未假设测量是实数，因此对于复参考测量的可观测量也适用。

3.3 二元可观测量的闭式判据

虽然定理 3.5中的条件可以通过半定规划检验，但其存在性本质使得它在某些应用中不易使用。为了解决这一问题，我们提出定理 3.5 的闭式变体，适用于以下特殊情况：A_x 和 O 均为二元测量。这种特殊形式不仅便于证明我们的主定理，在迭代自检验的背景下也很有用。

令 中的所有测量都为 $\mathcal{S}$ 二值的，即。由于，$|\mathcal{O}_A| = |\mathcal{O}_B| = 2$。由于 A_x 和 O 现在都是正交矩阵（因为投影算子是实的），定理3.5 中的条件可简化为

$$\tilde{O}P \in \mathrm{span}_{\mathbb{C}}\{D^2, D\tilde{A}_xD\}.$$

（注意，通过取 $\tilde{O}^0 P_0 = P_0$，它总是在张成空间中 $P_0 = D^2$。）此外，我们可以将范围限制在 $\{D^2, D\tilde{A}_x D\}$的实张成空间内：如果 $\tilde{O}P \in$ 张成空间$_{\mathbb{C}}\{D^2, D\tilde{A}_x D\}$，那么 $\tilde{O}\,\mathrm{Re}(P) \in$ 张成空间 $_{\mathbb{R}}\{D^2, D\tilde{A}_x D\}$，其中$\mathrm{Re}(P)$ 是正定的[1]。因此只需考虑

$$\tilde{O}P \in \mathrm{span}_{\mathbb{R}}\{D^2, D\tilde{A}_x D\}, \tag{3}$$

其中 P为实数且正定。

由于张成空间$_{\mathbb{R}}\{D^2, D\tilde{A}_x D\}$ 中的每个算子都是实厄米矩阵（或对称矩阵），考虑以下符号映射：它将实厄米矩阵映射为特征值为 0、 ±1的实厄米矩阵，定义如下

$$\begin{aligned} &\mathrm{sgn} : H(\mathbb{R})_d \to H(\mathbb{R})_d \\ &H = \sum_j \lambda_j |v_j\rangle\langle v_j| \mapsto \mathrm{sgn}(H) = \sum_j \mathrm{sgn}(\lambda_j)|v_j\rangle\langle v_j| \end{aligned}$$

其中 $(|v_j\rangle\}_j$ 是 H的一组特征向量标准正交基。也就是说，符号函数 是通过函数演算将符号˜函数扩展而来。接下来我们证明，判据（式（3）等价于 O 属于张成空间$\{D^2, D\tilde{A}_x D\}$ 在符号函数下的像：

˜ ˜**引理 3.6** 给定 d维正交矩阵 O 和 $\{A_x\}$，以及 $D =$ 对角矩阵$(\{\lambda_j\})$，其中 $\lambda_j > 0$对 $j \in [0, d-1]$成立。则存在实正定 P，使得

$$\tilde{O}P \in \mathrm{span}_{\mathbb{R}}\{D^2, D\tilde{A}_x D),$$

当且仅当

$$\tilde{O} \in \mathrm{sgn}(\mathrm{span}_{\mathbb{R}}\{D^2, D\tilde{A}_x D\}).$$

证明。“若”部分：令 $\tilde{O} =$ 为H的符号映射，其中 $H \in$ 属于张成空间$_{\mathbb{R}}\{D^2, D\tilde{A}_x D\}$。由于 $\tilde{O}$ 非奇异，

˜ ˜ ˜H 也非奇异。因此， $OH =$ 符号映射$(H)H$ 为正定矩阵。取 $P = OH$，则 $OP = H \in$ 属于张成空间$_{\mathbb{R}}\{D^2, D\tilde{A}_x D\}$。

“仅当”部分：令 $\tilde{O}P = H \in \mathrm{span}_{\mathbb{R}}\{D^2, D\tilde{A}_x D\}$，则 $H = H^\intercal = (\tilde{O}P)^\intercal = P\tilde{O}$。因此 $\tilde{O}$、 H 和 P 可交换，故可同时对角化。令 $\{b_j\}$、 $\{p_j\}$、 $\{h_j\}$ 分别为 O， P， H 的特征值；则 $o_j p_j = h_j \neq 0$。另外注意到 $o_j = \pm 1$ 和 $p_j > 0$，因此 $p_j = |h_j|$ 和˜$o_j = h_j/|h_j| = \mathrm{sgn}(h_j)$。所以 $O = \mathrm{sgn}(H)$。■

由此立即得到二元可观测量事后自检验的等价判据：

˜命题 *3.7 </style}*一个额外的 d 维二元（二输出）可观测量 O，若基于经鲁棒自检的初始二值观测量 $\{A_x\}$ 和初始态 $|\psi\rangle_{\tilde{A}\tilde{B}}$，则可进行鲁棒事后自检验，条件是

$$\tilde{O} \in \mathrm{sgn}(\mathrm{span}_{\mathbb{R}}\{D^2, D\tilde{A}_x D : x\}),$$

其中 $D = \mathrm{vec}^{-1}(|\tilde{\psi}\rangle)$，而 符号函数 将实厄米矩阵映射为实厄米矩阵，定义为 b y

$$\begin{aligned} &\mathrm{sgn} : H(\mathbb{R})_d \to H(\mathbb{R})_d \\ &H = \sum_j \lambda_j |v_j\rangle\langle v_j| \mapsto \mathrm{sgn}(H) = \sum_j \mathrm{sgn}(\lambda_j)|v_j\rangle\langle v_j|. \end{aligned}$$

此外，鲁棒性对 $\varepsilon' - (\varepsilon, \delta)$ 的依赖关系将为 $\varepsilon' = O(\sqrt{C\varepsilon} + \delta)$。

4 迭代自检 I：任意实投影测量的自检验

现在我们介绍迭代自检技术，并借此展示如何对任意实投影测量进行自检验。从现在起，我们将研究具有二元可观测量和

[1] $\mathrm{Re}(P) = \frac{1}{2}(P + \bar{P})$，其中 P和 $\bar{P}$均为正定 te.

最大纠缠初态 $|\tilde{\psi}\rangle = |\Phi_d\rangle = \sum_j |jj\rangle/\sqrt{d}$的参考策略。在这种情况下，命题3.7 中的判据简化为 $\tilde{O} \in$ 符号函数(张成空间$\{I, \tilde{A}_x\}$)，因为 $D = 1/\sqrt{d}I$ 与单位矩阵成正比。

给定初始策略 $\tilde{\mathcal{S}} = (\Phi_d, \{\tilde{A}_x\}, \{\tilde{B}_y\})$，如果我们进行事后自检的判据 $\tilde{O} \in$ 符号函数(张成空间$\{I, B_y, O\}$)，那么我们可以使用 $\{B_y, O\}$ 对爱丽丝的另一个测量 $O' \in$ 符号函数(张成空间$\{I, B_y, O\}$)进行事后自检。通过分几轮进行这一过程，从一小组可观测量 $\{A_x\}$ 开始，我们最终甚至可以自检许多其他可观测量。我们将这一过程称为迭代自检。

我们通过直观展示关联表的扩展，帮助更好地理解迭代自检。设初始二元可观测量为 $\{A_x\}$ $\{B_y\}$，初始态 $|\psi\rangle = |\Phi_d\rangle$ 是最大纠缠的。于是，表 3 中生成的关联可以自检验初始策略 $\mathcal{S}$。回顾一下，命题 3.7 中的条件可简化为 $O \in$ 符号函数(span$\{I, A_x\}$)。现在考虑一个额外的二元可观测量 O，使得 $O \notin$ 符号函数(span$\{I, A_x\}$)，但 $O \in$ 符号函数(span{符号函数(span$\{I, A_x\}$)})。由于 $O \notin$符号函数(span$\{I, \tilde{A}_x\}$)，我们不知道基于 $\{A_x\}$ 的关联 $\{\langle\tilde{\psi}|\tilde{A}_x^{(j)} \otimes \tilde{O}^{(k)}|\tilde{\psi}\rangle\}$ 是否能对它进行事后自检。尽管如此，给定 $O \in$ 符号函数(span{符号函数(span$\{I, A_x\}$)})，我们可以这样做：取最少的二元可观测量 $B_{|\mathcal{I}_B|}$、...、$B_{Y'-1} \in$ 符号函数(span$\{I, A_x\}$)，使得 span $\{I, B_0, ..., B_{Y'-1}\} =$ span{符号函数(span$\{I, A_x\}$)}。那么，表 3 中的关联就能自检验相应的策略，因为白色部分检验 $\mathcal{S}$，绿色部分检验额外的二元可观测量 $B_{|\mathcal{I}_B|}$、...、$B_{Y'-1} \in$ 符号函数(span$\{I, A_x\}$)。现在，将 O 作为新行加入表4。因为 $O \in$符号函数(span{符号函数(span$\{I, A_x\}$)})，关联表4（迭代式）事后自检的黄色部分 O。因此，关联表4对包含 O的扩展策略进行自检。显然，通过这一构造，无论迭代次数多少，关联表的大小都有平凡上界 $d^{(d+1)} \times d(d+1)$。

	I	$\tilde{B}_0$	...	$\tilde{B}_{Y-1}$	$\tilde{B}_Y$	...	$\tilde{B}_{Y'-1}$
I	$\langle A_0, I\rangle_{\tilde{\psi}}$	$\langle A_0, B_0\rangle_{\tilde{\psi}}$	...	$\langle A_0, B_{Y-1}\rangle_{\tilde{\psi}}$	$\langle A_0, B_Y\rangle_{\tilde{\psi}}$	...	$\langle A_0, B_{Y'-1}\rangle_{\tilde{\psi}}$
$\tilde{A}_0$	$\langle A_0, I\rangle_{\tilde{\psi}}$	$\langle A_0, B_0\rangle_{\tilde{\psi}}$	...	$\langle A_0, B_{Y-1}\rangle_{\tilde{\psi}}$	$\langle A_0, B_Y\rangle_{\tilde{\psi}}$	...	$\langle A_0, B_{Y'-1}\rangle_{\tilde{\psi}}$
...	...	...	...	...	...	...	...
$\tilde{A}_{X-1}$	$\langle A_{X-1}, I\rangle_{\tilde{\psi}}$	$\langle A_{X-1}, B_0\rangle_{\tilde{\psi}}$	...	$\langle A_{X-1}, B_{Y-1}\rangle_{\tilde{\psi}}$	$\langle A_{X-1}, B_Y\rangle_{\tilde{\psi}}$	...	$\langle A_{X-1}, B_{Y'-1}\rangle_{\tilde{\psi}}$

表 3：第一次迭代中的扩展相关表。为方便起见，我们取 $X = |\mathcal{I}_A|$、$Y = |\mathcal{I}_B|$和 $Y' = |\mathcal{I}'_B|$。

	I	$\tilde{B}_1$	...	$\tilde{B}_{Y-1}$	$\tilde{B}_Y$	...	$\tilde{B}_{Y'-1}$
I	$\langle A_1, I\rangle_{\tilde{\psi}}$	$\langle A_1, B_1\rangle_{\tilde{\psi}}$	...	$\langle A_1, B_{Y-1}\rangle_{\tilde{\psi}}$	$\langle A_1, B_Y\rangle_{\tilde{\psi}}$	...	$\langle A_1, B_{Y'-1}\rangle_{\tilde{\psi}}$
$\tilde{A}_1$	$\langle A_1, I\rangle_{\tilde{\psi}}$	$\langle A_1, B_1\rangle_{\tilde{\psi}}$	...	$\langle A_1, B_{Y-1}\rangle_{\tilde{\psi}}$	$\langle A_1, B_Y\rangle_{\tilde{\psi}}$	...	$\langle A_1, B_{Y'-1}\rangle_{\tilde{\psi}}$
...	...	...	...	...	...	...	...
$\tilde{A}_{X-1}$	$\langle A_{X-1}, I\rangle_{\tilde{\psi}}$	$\langle A_{X-1}, B_1\rangle_{\tilde{\psi}}$	...	$\langle A_{X-1}, B_{Y-1}\rangle_{\tilde{\psi}}$	$\langle A_{X-1}, B_Y\rangle_{\tilde{\psi}}$	...	$\langle A_{X-1}, B_{Y'-1}\rangle_{\tilde{\psi}}$
$\tilde{O}$	$\langle O, I\rangle_{\tilde{\psi}}$	$\langle O, B_1\rangle_{\tilde{\psi}}$	...	$\langle O, B_{Y-1}\rangle_{\tilde{\psi}}$	$\langle O, B_Y\rangle_{\tilde{\psi}}$	...	$\langle O, B_{Y'-1}\rangle_{\tilde{\psi}}$

表4：第二次迭代中的扩展相关表。

4.1 任意实可观测量的自检验

在 [MPS21], 中，作者考虑了一组投影算子，其总和等于 I 的一定比例，并证明了由这些投影算子和最大纠缠态组成的策略，可以通过其产生的关联进行自检验。在此，我们采用了其中一种具有特定构造的策略。事实证明，利用我们选择的初始策略，经过两次迭代，我们将能够使用迭代方案对任意二元投影的测量进行自检验。

设 $d+1$ 单位向量 v_0、.....、$v_d \in \mathbb{R}^d$ 构成一个以原点为中心的正则（$d+1$）单纯形的顶点。注意到

$$v_x^\dagger v_{x'} = -\frac{1}{d} \tag{4}$$

对于 $x \neq x'$。定义二元可观测量 $d+1$

$$\tilde{T}_x := 2v_x v_x^\dagger - I.$$

用于生成可观测量的 Mathematica 代码见附录B。根据 [MPS21] 以下包含 T_x 且采用最大纠缠态的策略是鲁棒自检的：

推论 4.1 根据 *[MPS21]*, 中的定理 *6.10*，策略 $\tilde{\mathcal{S}}^{(0)} = (|\Phi_d\rangle, \{\tilde{T}_x\}_{x=0}^d, \{\tilde{T}_y\}_{y=0}^d)$ 可由其产生的关联进行鲁棒自检。

现在取推论 $\tilde{\mathcal{S}}^{(0)}$ 中的策略作为4.1 初始策略，并考虑形式如下的附加二元~~~~可观测量 T_{jk}：= 符号函数$(T_j + T_k)$，其中 $j \neq k$。根据命题 3.7，它们均可进行鲁棒事后自检。具体而言，我们有以下可进行鲁棒自检的扩展策略：

引理 4.2 策略 $\tilde{\mathcal{S}}^{(1)} = (|\tilde{\psi}\rangle, \{\tilde{A}_x\}_{x=0}^d, \{\tilde{B}_y\}_{y=0}^{\frac{d(d+1)}{2}-1})$ 是鲁棒自检的，其中

$$
\begin{aligned}
&|\tilde{\psi}\rangle = |\Phi_d\rangle, \\
&\{\tilde{A}_x\}_{x=0}^d = \{\tilde{T}_x\}_{x=0}^d, \\
&\{\tilde{B}_y\}_{y=0}^d = \{\tilde{T}_y\}_{y=0}^d,\ \{\tilde{B}_y\}_{y=d+1}^{\frac{d(d+1)}{2}-1} = \{\tilde{T}_{jk} : 1 \leq j < k \leq d\} \setminus \{\tilde{T}_{12}\}.
\end{aligned}
$$

证明。由于 $\tilde{\mathcal{S}}^{(0)} = (|\tilde{\psi}\rangle, \{\tilde{A}_x\}_{x=0}^d, \{\tilde{B}_y\}_{y=0}^d)$ 是鲁棒自检的，并且 $\tilde{T}_{jk} \in$ 符号函数(张成空间 $\{\tilde{T}_x\}$)，根据命题 3.7 和3.2，我们立即得到策略 $\tilde{\mathcal{S}}^{(1)}$ 可通过其生成的关联实现鲁棒自检。■

扩展策略 $\tilde{\mathcal{S}}^{(1)} = (|\Phi_d\rangle, \{\tilde{A}_x\}_{x=0}^d, \{\tilde{B}_y\}_{y=0}^{\frac{d(d+1)}{2}-1})$ 为鲍勃引入了 $d(d+1)/2 - d - 1$ 个额外的二元可观测量，这些可观测量可根据初始策略进行事后自检，并且形式为符号函数$(T_j + T_k)$（但并未包含每个 $j \neq k$）。结果表明，这些额外的二元可观测量与 $d+1$ 个初始可观测量共同张成了所有 $d \times d$ 阶对称矩阵构成的空间。为证明这一点，我们需要以下引理：

~~**引理 4.3** 对于 $d > 2$，张成空间$_{\mathbb{R}}\{T_{jk} : j, k \in [0, d], j \neq k\} = H_d(\mathbb{R})$ 为所有 d 维对称矩阵构成的空间。

~~**证明**。由于 $\dim H_d(\mathbb{R}) = d(d+1)/2 = \#\{T_{jk} : j, k \in [0, d], j \neq k\}$，只需证明~~{符号函数$(T_j + T_k) : 0 \leq j < k \leq d\}$ 线性无关。

注意到 $\tilde{T}_j + \tilde{T}_k = 2(v_j v_j^\dagger + v_k v_k^\dagger - I)$。考虑二维子空间 $\mathcal{H}_1 =$张成空间(v_j, v_k)。~~~~那么 $(\tilde{T}_j + \tilde{T}_k)|_{\mathcal{H}_1^\perp} = -2I$，并且

$$
(\tilde{T}_j + \tilde{T}_k)(v_j - v_k) = \frac{2}{d}(v_j - v_k), \quad (\tilde{T}_j + \tilde{T}_k)(v_j + v_k) = -\frac{2}{d}(v_j + v_k),
$$

~~~~因此 $(T_j + T_k)|_{\mathcal{H}_1}$ 的特征值为 $\pm 2/d$，对应于 $2/d$ 的（归一化）特征向量为 $w_{jk} := \sqrt{\frac{d}{2(d+1)}}(v_j - v_k)$。因此，符号函数$(\tilde{T}_j + \tilde{T}_k)$的特征值为 1（重数为 1），以及 -1（重数为 $d-1$）。对应于 1 的特征向量为 $w_{jk} = \sqrt{\frac{d}{2(d+1)}}(v_j - v_k)$。因此 $\tilde{T}_{jk} = 2w_{jk}w_{jk}^\dagger - I$。

~~假设对于某些实系数 c_{jk}，有 $\sum_{j<k} c_{jk} T_{jk} = 0$。那么

$$
2\frac{d}{2(d+1)} \sum_{j<k} c_{jk}(v_j - v_k)(v_j^\dagger - v_k^\dagger) = \sum_{j<k} c_{jk} I. \tag{5}
$$

根据公式（4），我们有

$$
(v_j^\dagger - v_k^\dagger)v_l = \begin{cases} 0 & j, k \neq l \\ -\frac{1}{d} - 1 & j \neq k = l \\ 1 + \frac{1}{d} & l = j \neq k \end{cases}
$$

因此，在等式（5）左侧乘以 v_ℓ 可得

$$
\frac{d}{d+1}\left(\sum_{j<l} c_{jl}(-\tfrac{1}{d} - 1)(v_j - v_l) + \sum_{l<k} c_{lk}(1 + \tfrac{1}{d})(v_l - v_k)\right) = \sum_{j<k} c_{jk} v_l
$$
~~~~

因此

$$\left(\sum_{j<l} c_{jl}(v_l - v_j) + \sum_{l<k} c_{lk}(v_l - v_k)\right) = \sum_{j<k} c_{jk} v_l$$

$$\Rightarrow \quad \left(\sum_{j<l} c_{jl} + \sum_{l<k} c_{lk} - \sum_{j<k} c_{jk}\right) v_l - \sum_{j<l} c_{jl} v_j - \sum_{l<k} c_{lk} v_k = 0.$$

由于 $\sum_j v_j = 0$，我们进一步得到

$$\left(\sum_{j<l} c_{jl} + \sum_{l<j} c_{lj} - \sum_{j<k} c_{jk}\right) \sum_{j\neq l} v_j - \sum_{j<l} c_{jl} v_j - \sum_{l<j} c_{lj} v_j = 0.$$

由于 $\{v_j : \ j \neq l\}$ 线性无关，我们看到 c_{jl} 对于 $j < l$ 相等，且 c_{lj} 对于 $l > j$ 相等；因此 $c_{jk} =:$ 对于所有 $j < k$，c。于是，

$$c\left(d - \frac{d(d+1)}{2}\right) v_l - c\sum_{j\neq l} v_j = 0$$

$$\Rightarrow \quad c\left(\frac{d - d^2}{2} v_l - \sum_{j\neq l} v_j\right) = 0,$$

这只有在 $c = 0$ 或 $d = 2$ 或 $d = -1$时才成立。因此我们得出，当 $d > 2$时，$c_{jk} = 0$ 是~$\sum_{j<k} c_{jk} T_{jk} = 0$ 的唯一解。■

~令 $T = \{T_j : \ j \in [0, d]\} \cup \{T_{jk} : \ j, \ k \in [0, d], \ j \neq k\}$。根据引理 4.3 我们知道，张成空间$_{\mathbb{R}}(T)$ $= H_d(\mathbb{R})$。注意，$|T| = d + 1 + {}^{d}{}_{(d+1)}{}_{2}$ $>$维数 $H_d(\mathbb{R})$。下面的命题给出了 T中的一个极大线性无关子集：

~ ~ ~**命题 4.4** 定义 $T = \{T_j : \ j \in [0, d]\} \cup \{T_{jk} : \ j, \ k \in [0, d], j \neq k\}$。设 $T' = T \setminus \{O_{0j} : \ j \in [1, d]\}$ 且 $T'' = T' \setminus \{O_{12}\}$。那么 T'' 是 T中的一个极大线性无关子集。

证明。注意，$|T''| = {}^{d}{}_{(d+1)2}$ $=$维数为 $H_d(\mathbb{R})$。因此，只需证明 $\tilde{T}_{0j} \in$张成$_{\mathbb{R}}(T')$，且$\tilde{T}_{12} \in$张成$_{\mathbb{R}}(T'')$。另请注意，单位矩阵 $I =$ ${}^{d}{}_{(d+1)(2-d)}$ $\sum_j \tilde{T}_j$属于$_{\mathbb{R}}(T'')$的张成空间，~$(T_j + I)/2$也属于其中。

- $O_{0j} \in$ 张成空间$_{\mathbb{R}}(T')$：注意到 $\sum_j v_j = 0$。那么对于每个 $j > 0$，

$$\begin{aligned}
\tilde{O}_{0j} =& \frac{d}{d+1}(v_0 - v_j)(v_0^\dagger - v_j) - I \\
=& \frac{d}{d+1}(-\sum_{k>0} v_k - v_j)(-\sum_{k>0} v_k^\dagger - v_j^\dagger) - I \\
=& \frac{d}{d+1}(\sum_{0<k<l} (v_k v_l^\dagger + v_l v_k^\dagger) + \sum_{k>0} (v_k v_j^\dagger + v_j v_k^\dagger) + \tilde{P}_j) - I \in \mathrm{span}_{\mathbb{R}}(T')
\end{aligned}$$

  因为对于所有 $x, \ y > 0$，$v_x v_y^\dagger + v_y v_x^\dagger = \tilde{P}_x + \tilde{P}_y - {}^{d+1}_{d}(\tilde{T}_{xy} - I) \in$张成空间$_{\mathbb{R}}(T')$。

- $\tilde{T}_{12} \in$ 张成空间$_{\mathbb{R}}(T'')$：我们证明了 $\sum_{1\leq j<k\leq d} \tilde{T}_{jk} + dv_0 v_0^* + {}^{d}{}_{(d-3)}{}_{2}$ $I = 0$，这意味着 $\tilde{T}_{12}$ 是 T''中元素的线性组合。由于张成空间$_{\mathbb{R}}\{v_l : \ l \in [1, d]\} = \mathbb{R}^d$，因此只需证明

$\sum_{1\le j<k\le d}\tilde{T}_{jk}v_l + dv_0v_0^*v_l + \frac{d(d-3)}{2}v_l = 0$ 对所有 $l\in[1,d]$:

$$\begin{aligned}
&\sum_{1\le j<k\le d}\tilde{T}_{jk}v_l + d\tilde{P}_0v_l + \frac{d(d-3)}{2}v_l\\
=&\sum_{1\le j<k\le d}\frac{d}{d-1}(v_j-v_k)(v_j^\dagger - v_k^\dagger)v_l - \frac{d(d-1)}{2}v_l - v_0 + \frac{d(d-3)}{2}v_l\\
=&\sum_{j>0,j\neq l}(v_l - v_j) - \frac{d(d-1)}{2}v_l - v_0 + \frac{d(d-3)}{2}v_l\\
=&(d-1)v_l + \sum_{j>0,j\neq l}(-v_j) - \frac{d(d-1)}{2}v_l - v_0 + \frac{d(d-3)}{2}v_l\\
=&(d-1)v_l + v_0 + v_l - \frac{d(d-1)}{2}v_l - v_0 + \frac{d(d-3)}{2}v_l = 0.
\end{aligned}$$

■

由于 $T''=\{B_y\}$ 在 $\mathcal{S}$ 中张成所有对称矩阵的空间，每个 d维二元可观测量 O_{binary} 都属于张成空间$\{B_y\}$。因此，将 O_{binary} 加入 $\{A_x\}$ 后，我们构造出一种能够自检验任意二元可观测量的策略:

命题 4.5 对于由可观测量O_{binary}给出的任意 d维实投影二元测量，策略 $\tilde{\mathcal{S}}^{(2)}=(|\tilde{\psi}\rangle, \{\tilde{A}_x\}_{x=0}^{d+1}, \{\tilde{B}_y\}_{x=0}^{\frac{d(d+1)}{2}-1})$ 是鲁棒自检的，其中

$$\begin{aligned}
&|\tilde{\psi}\rangle = |\Phi_d\rangle,\\
&\{\tilde{A}_x\}_{x=0}^{d} = \{\tilde{T}_x\}_{x=0}^{d},\ \tilde{A}_{d+1} = \tilde{O}_{\text{binary}},\\
&\{\tilde{B}_y\}_{y=0}^{d} = \{\tilde{T}_y\}_{y=0}^{d},\ \{\tilde{B}_y\}_{y=d+1}^{\frac{d(d+1)}{2}-1} = \{\tilde{T}_{jk}: 1\le j<k\le d\}\setminus\{\tilde{O}_{12}\}.
\end{aligned}$$

证明。 由于 $O_{\text{binary}}\in H_d(\mathbb{R}) =$ 张成空间$\{I, B_y\}$ 对于任意 O_{binary}，由引理 4.2 和命题 3.2 可立即得出，策略 $\tilde{\mathcal{S}}^{(2)}$ 可由其生成的关联进行鲁棒自检。 ■

最后，我们将二元测量的自检验推广到任意 L 输出测量的自检验。直观地说，我们可以将 L 输出投影测量看作一组 L 个二元测量：给定一个 L 输出投影测量 $\tilde{O}=\sum_{a=0}^{L-1}e^{i2\pi a/L}\tilde{M}_a$，考虑二元可观测量$\{2\tilde{M}_a - I\}_{a=0}^{L-1}$。如果我们能够对每个二元可观测量 $2\tilde{M}_a - I$ 进行自检验，那么我们也应当能够自检验 O。

命题 4.6 对于任意 L 输出可观测量 $\tilde{O}=\sum_{a=0}^{L-1}e^{i2\pi a/L}\tilde{M}_a$，策略

$$\tilde{\mathcal{S}}_1 = (|\tilde{\psi}\rangle, \{\tilde{A}_x, \tilde{O}: x\}, \{\tilde{B}_y: y\})$$

当且仅当策略是鲁棒自检的

$$\tilde{\mathcal{S}}_2 = (|\tilde{\psi}\rangle, \{\tilde{A}_x, 2\tilde{M}_a - I: x, a\}, \{\tilde{B}_y: y\})$$

是鲁棒自检的。

证明。 我们证明“如果”部分，“仅如果”部分的论证类似。

假设 $\tilde{\mathcal{S}}_1$ 是鲁棒自检的。那么对于任意 $\varepsilon>0$，存在 $\delta>0$，使得任意策略 $\delta/3$ 近似生成关联 $\{\langle\tilde{\psi}|\tilde{A}_x^{(j)}\otimes\tilde{B}_y^{(k)}|\tilde{\psi}\rangle, \langle\tilde{\psi}|(2\tilde{M}_a - I)\otimes\tilde{B}_y^{(k)}|\tilde{\psi}\rangle\}$，都可以由 $\tilde{\mathcal{S}}_2$ 局部 ε/L 扩张。令 $\mathcal{S}_1=(|\psi\rangle, \{A_x^{(j)}, O^{(l)}\}\ \{B_y^{(k)}\})$ 为一个以 $\delta/3$ 近似生成关联 $\{\langle\tilde{\psi}|\tilde{A}_x^{(j)}\otimes\tilde{B}_y^{(k)}|\tilde{\psi}\rangle, \langle\tilde{\psi}|\tilde{O}^l\otimes\tilde{B}_y^{(k)}|\tilde{\psi}\rangle\}$ 的策略。构造物理策略 $\mathcal{S}_2:=(|\psi\rangle,\ \{A_x, 2M_a - I\}\ \{B_y\})$，其中 $M_a:=1/L\sum_{l=0}^{L-1}e^{-i2\pi al/L}O^{(l)}$。那么

$$\begin{aligned}
&|\langle\psi|O^{(l)}\otimes B_y^{(k)}|\psi\rangle - \langle\tilde{\psi}|\tilde{O}^l\otimes\tilde{B}_y^{(k)}|\tilde{\psi}\rangle| \le \delta/3\\
\Rightarrow\quad &|\langle\psi|(2M_a - I)\otimes\tilde{B}_y^{(k)}|\tilde{\psi}\rangle - \langle\tilde{\psi}|(2\tilde{M}_a - I)\otimes\tilde{B}_y^{(k)}|\tilde{\psi}\rangle| \le \delta.
\end{aligned}$$

因此 $\mathcal{S}_2$ δ 近似生成关联 $\{\langle\tilde{\psi}|\tilde{A}_x^{(j)}\otimes\tilde{B}_y^{(k)}|\tilde{\psi}\rangle, \langle\tilde{\psi}|(2\tilde{M}_a-I)\otimes\tilde{B}_y^{(k)}|\tilde{\psi}\rangle\}$。根据 ~ 假设， $\mathcal{S}_2$ 是 $\mathcal{S}_2$ 的局部 ε/L 扩张，因此

$$(|\psi\rangle_{AB}, (2M_a-I)\otimes I_B) \xhookrightarrow[\varepsilon/L]{\Phi,|\text{aux}\rangle} (|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}}, (2\tilde{M}_a-I)\otimes I_{\tilde{B}})$$
$$\Rightarrow \quad (|\psi\rangle_{AB}, O^{(l)}\otimes I_B) \xhookrightarrow[\varepsilon]{\Phi,|\text{aux}\rangle} (|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}}, \tilde{O}^l\otimes I_{\tilde{B}}),$$

and

$$(|\psi\rangle_{AB}, I_A\otimes B_y^{(k)}) \xhookrightarrow[\varepsilon/L]{\Phi,|\text{aux}\rangle} (|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}}, I_{\tilde{A}}\otimes\tilde{B}_y^{(k)}).$$

~ ~因此， $\mathcal{S}_1$ 是 $\mathcal{S}_1$的局部 ε-扩张。因此， $\mathcal{S}_1$ 是鲁棒自检的。 ■

因此我们得出结论：任意实射影测量都可以自检验：

~**定理 4.7** 对于任意 d维、具有 L个输出的可观测量 O，该策略

$$\tilde{\mathcal{S}}^{(3)} = \left(|\tilde{\psi}\rangle, \{\tilde{A}_x\}_{x=0}^{d+1}, \{\tilde{B}_y\}_{y=0}^{\frac{d(d+1)}{2}-1}\right)$$

是鲁棒自检的，其中

$$|\tilde{\psi}\rangle = |\Phi_d\rangle,$$
$$\{\tilde{A}_x\}_{x=0}^{d} = \{\tilde{T}_x\}_{x=0}^{d},\ \tilde{A}_{d+1} = \tilde{O},$$
$$\{\tilde{B}_y\}_{y=0}^{d} = \{\tilde{T}_y\}_{x=0}^{d},\ \{\tilde{B}_y\}_{y=d+1}^{\frac{d(d+1)}{2}-1} = \{\tilde{T}_{jk}: 1\le j<k\le d\}\setminus\{\tilde{T}_{12}\}.$$

证明。对于 $L=2$，根据命题 4.5，结论成立。对于 $L>2$，令 $\tilde{O}=\sum_a e^{i2\pi a/L}\tilde{M}_a$ 为L个输出的可观测量，考虑策略 $\tilde{\mathcal{S}}_2=(|\tilde{\psi}\rangle, \{\tilde{A}_x\}_{x=0}^{d+L}, \{\tilde{B}_y\}_{x=0}^{\frac{d(d+1)}{2}-1})$ 其中

$$|\tilde{\psi}\rangle = |\Phi_d\rangle,$$
$$\{\tilde{A}_x\}_{x=0}^{d} = \{\tilde{T}_x\}_{x=0}^{d},\ \{\tilde{A}_x\}_{x=d+1}^{d+L} = \{2\tilde{M}_a - I: 0\le a\le L-1\},$$
$$\{\tilde{B}_y\}_{y=0}^{d} = \{\tilde{T}_y\}_{y=0}^{d},\ \{\tilde{B}_y\}_{y=d+1}^{\frac{d(d+1)}{2}-1} = \{\tilde{T}_{jk}: 1\le j<k\le d\}\setminus\{\tilde{T}_{12}\},$$

且 $\tilde{M}_a = 1/L\sum_{l=0}^{L-1} e^{-i2\pi al/L}\tilde{O}^l$。根据命题 4.5 $\tilde{\mathcal{S}}_2$ 的证明中类似的论证， $\tilde{\mathcal{S}}_2$ 是鲁棒自检的。接着，根据命题 4.6，策略 $\tilde{\mathcal{S}}^{(3)}$ 是鲁棒自检的。 ■

5 迭代自检 II：一般理论

~本节将一般性地发展迭代自检理论，适用于初始态 $|\psi\rangle = |\Phi_d\rangle = \sum_j |jj\rangle/\sqrt{d}$ 为最大纠缠态，且所有参考测量均为二元投影测量的情况*ie.*，即由正交矩阵描述。

~ ~ ~ ~给定初始策略 $\mathcal{S}=(|\Phi_d\rangle, \{A_x\}\ \{B_y\})$，记 $S_0=\{I, A_x\}$ 为初始二值观测量的集合，记 V_0 = 张成空间$_{\mathbb{R}}(S_0)$ 为由 S_0生成的子空间。记 S_1' = 符号函数$(V_0)\cap GL_d(\mathbb{R})$ 为根据命题 3.7 在鲍勃一侧经事后自检的二元可观测量，并令 ~ ~ ~ $S_1 = S_1'\cup\{B_y\}$。注意，由于符号函数$(A_x) = A_x$，因此 $S_0\subseteq S_1'\subseteq S_1$。令 V_1 = 张成空间$_{\mathbb{R}}(S_1)$；那么我们还有 $V_0\subseteq V_1$。现在，基于 S_1，考虑在爱丽丝一侧对其他二元可观测量进行事后自检；我们得到下一组经自检的二元可观测量 S_2 = 符号函数$(V_1)\cap GL_d(\mathbb{R})\supseteq S_1$，以及下一个子空间 V_2 = 张成空间$_{\mathbb{R}}(S_1)\supseteq V_1$。通过迭代使用这一技巧，我们在每一步都扩大经自检的二元可观测量集合 S_j。我们指出，若尝试对非最大纠缠 $|\psi\rangle$作类似论证~，则目前尚不清楚 $V_j\subseteq V_{j+1}$ 是否仍然成立。

由于 $\{V_j\}_j$ 是有限维实厄米矩阵空间 $H_d(\mathbb{R})$ 的递增子空间序列，它最终会稳定于 $V_\infty = \lim_{j\to\infty} V_j$。自然会产生这样的问题：给定初始二元观测量 $\{A_x\}\ \{B_y\}$， V_∞ 是什么？在回答这个问题之前，我们先作如下观察：

引理 5.1 给定一组正交矩阵 $\{A_x\}$，递归定义 $V_0 =$ 张成空间$_{\mathbb{R}}\{I, A_x\}$ 和 $V_j =$张成空间$_{\mathbb{R}}$(符号函数$(V_{j-1}))$[2]，其中 符号函数 的定义见命题 3.7。若 $x \in V_j$，则 $p(x) \in V_{j+1}$ 对于任意实系数多项式 $p \in \mathbb{R}[t]$均成立。因此， x， $y \in V_j$ 意味着 $xy + yx \in V_{j+1}$。

证明。 对于任意 $x \in V_j$，令 $x = U\Lambda U^\dagger$，其中 Λ 的对角元素为 λ_1，……，$\lambda_d \in \mathbb{R}$，并按降序排列。于是 $p(x)$ 的特征值为 $p(\lambda_1)$，……，$p(\lambda_d)$。注意，单位矩阵 I 属于 V_1。现在，对于每个满足 $\lambda_i \neq \lambda_{i+1}$ 的 $i \in [1, d-1]$，选取 $r_i \in (\lambda_i, \lambda_{i+1})$，并考虑

$$x_i := \operatorname{sgn}(x - r_i I) = U \operatorname{diag}(\underbrace{1, \ldots, 1}_{i\ 1s}, \underbrace{-1, \ldots, -1}_{(d-i)\ -1s}) U^\dagger.$$

因此 $x_i \in$ 符号函数$(V_j) \subseteq V_{j+1}$。由于 $\{x_i\}$ 构成 $\{p(x)\colon\ p \in \mathbb{R}[t]\}$ 的一组基，我们有，对于每个 $p \in \mathbb{R}[t]$, $p(x) \in V_{j+1}$。

取 $p(t) = t^2$，并注意

$$xy + yx = \underbrace{(x+y)^2}_{\in V_{j+1}} - \underbrace{x^2}_{\in V_{j+1}} - \underbrace{y^2}_{\in V_{j+1}} \in V_{j+1}.$$

■

引理 5.1 允许用约当代数[3] V_∞ 来刻画 [Jac68]。结合代数的向量子空间若包含单位元且对约当积 $a \star b = \frac{1}{2}(ab + ba)$封闭，则它是一个（含幺）约当代数。

命题 5.2 给定一组厄米正交矩阵 $\{A_x\}$，定义 $V_0 =$ 张成空间$_{\mathbb{R}}\{I, A_x\}$， $V_j =$张成空间$_{\mathbb{R}}(V_{j-1}$ 的符号函数$)$，其中 符号函数 的定义见命题 3.7。那么 $V_\infty = \mathcal{JA}(\{A_x\})$是由生成的实约当 $\{A_x\}$代数。

证明。 $\mathcal{JA}(\{\tilde{A}_x\}) = \mathcal{JA}(\{I, \tilde{A}_x\})$ 因为 $I = \tilde{A}_{x^0}^2$。由引理 5.1 $x\ y \in V_\infty$。我们知道，意味着 $x \star y \in V_\infty$。因此 V_∞ 是一个约当代数，所以 $\mathcal{JA}(\{I, A_x\}) \subseteq V_\infty$。

另一方面，对于任意 $x \in H_d(\mathbb{R})$，矩阵 sgn(x) 是 x 的多项式，因此属于 $\mathcal{JA}(\{x\})$。这意味着 $V_\infty \subseteq \mathcal{JA}(\{I, A_x\})$。所以我们得出结论， $V_\infty = \mathcal{JA}(\{I, A_x\}) = \mathcal{JA}(\{A_x\})$。

■

命题 5.2 表明，经过足够多步后，每个二元可观测量 $O \in \mathcal{JA}(\{I, A_x\})$ 都可以基于二元策略 $\mathcal{S} = (|\Phi_d\rangle, \{A_x\}\ \{B_y\})$ 进行迭代式事后自检。我们还给出了实约当代数的两个性质，有助于分析 $\mathcal{JA}(\{A_x\})$。第一个性质是，$\mathcal{JA}(\{A_x\})$（由 $\{A_x\}$ 生成的实结合代数）为 $M_d(\mathbb{R})$（$d \times d$ 矩阵的实代数），当且仅当 $\mathcal{JA}(\{A_x\})$（由 $\{A_x\}$ 生成的实约当代数）为 $H_d(\mathbb{R})$（对称 $d \times d$ 矩阵的实约当代数）。

引理 5.3 </style}对于对称 矩阵 ,($\{A_x\}) = M_d(\mathbb{R})$ 当且仅当 $\mathcal{JA}(\{A_x\}) = H_d(\mathbb{R})$*</style}*。

证明。 “若”部分：显然，每个实矩阵都是对称矩阵乘积的线性组合。

“仅若”部分：注意到 $M_d(\mathbb{R})$ 是一个单代数，而 $H_d(\mathbb{R})$ 的约当子代数是半单的。设 $\mathcal{A}(\{A_x\}) = M_d(\mathbb{R})$。那么我们断言 $\mathcal{JA}(\{A_x\})$ 也是单代数。事实上；若 $\mathcal{JA}(\{A_x\})$ 同构于若干单代数的非平凡直积，那么 $\mathcal{A}(\{A_x\})$ 也会同构于若干单代数的非平凡直积，这就产生了矛盾。根据约当–冯·诺依曼–维格定理 [JvNW34], , 有限维单约当代数同构于以下五种类型之一：

- $n \times n$ 厄米实矩阵 $H_n(\mathbb{R})$ 的约当代数,
- $n \times n$ 厄米复矩阵 H_n的约当代数$\mathbb{C}$,

[2]这里我们不排除 S_j 中的非奇异矩阵。事实上，span(sgn$(V_j)) =$ span(sgn$(V_j) \cap GL_d(\mathbb{R}))$：对于任意奇异的 $s =$ sgn(x)，其中 $x \in V_j$，sgn$(x \pm \delta I) \in$ sgn(V_j)。当 δ 足够小时，我们有 sgn$(x \pm \delta I) \in GL_d(\mathbb{R})$ 且 $2s =$ sgn$(x + \delta I) +$sgn$(x - \delta I)$。[3]为求简便，这里省略 $\{\tilde{B}_y\}$。这种简化只会加强我们的结论，因为现在我们不再要求 $\{\tilde{B}_y\}$ 作出贡献。

- $n \times n$ 厄米四元数矩阵 H_n的约当代数$\mathbb{H}$,
- “自旋因子” $\mathbb{R}^n \oplus \mathbb{R}$ 的乘积为 $(x,\ \alpha) \star (y,\ \beta) = (\beta x + \alpha y,\ \alpha\beta + \langle x,\ y\rangle)$,
- 3×3 厄米八元数矩阵的约当代数。

由于 $\mathcal{JA}(\{A_x\})$ 是特殊的，我们只需分别考察前四种情况：

- $\mathcal{JA}(\{A_x\}) \cong H_n(\mathbb{R})$ ，其中某个 n成立。根据证明中“若”这一部分， $\mathcal{A}(\{A_x\}) \cong M_n(\mathbb{R})$ 。但$\mathcal{A}(\{A_x\}) = M_d(\mathbb{R})$ ，因此只剩下 $n = d$这种可能性。
- $\mathcal{JA}(\{A_x\}) \cong H_n(\mathbb{C})$ ，其中某个 $n \geq 2$成立。一方面，复厄米 $n \times n$ 矩阵无法嵌入小于 $2n$阶的实矩阵中，因此 $2n \leq d$。另一方面， $\mathcal{JA}(\{A_x\}) \cong H_n(\mathbb{C})$ 意味着 $M_d(\mathbb{R}) = \mathcal{A}(\{\tilde{A}_x\})$ 是 $M_n(\mathbb{C})$ 的实子代数，因此 $d^2 \leq 2n^2$，矛盾。
- $\mathcal{JA}(\{A_x\}) \cong H_n(\mathbb{H})$ 对某个 $n \geq 2$ 成立。一方面，四元数厄米 $n \times n$ 矩阵无法嵌入到阶小于 $4n$ 的实 $H_n\ \mathbb{H}$ $M_d\ \mathbb{R} = \mathcal{A}\ \{\tilde{A}_x\}$ $M_n\ \mathbb{H}$ $d^2 \leq 4n^2$ 矩阵中，因此 . 另一方面，( ) ( ) 意味着 ( ) ( ) 是 ( ) 的实子代数，所以 ，这与矛盾相矛盾。
- $\mathcal{JA}(\{A_x\})$ 是一个自旋因子 $\mathbb{R}^n \oplus \mathbb{R}$ 对某个 $n \geq 3$。众所周知，它可以嵌入到阶为 $2^n \times 2^n$ 的厄米实矩阵中，但无法嵌入到阶更小的矩阵中 [McC04]；因此 $2^n \leq d$。另一方面，该自旋因子生成一个维数为 2^n [Jac68], ，所以 $2^n \geq d^2$，这与矛盾。

因此，我们得出结论：$\mathcal{A}(\{A_x\}) = M_d(\mathbb{R})$ 当且仅当 $\mathcal{JA}(\{A_x\}) = H_d(\mathbb{R})$。 ■

由此引理可知，如果$\{A_x\}$ 生成相应维数的实矩阵代数，那么任意二元可观测量都属于 V_∞，因此可以进行自检验。在第 4 节中，我们证明了由 [MPS21] 给出的自检策略可以用于此目的。然而，现有文献中的若干自检策略由最大纠缠态和生成完整矩阵代数的算子构成，因此根据命题 5.2，它们可用于自检任意可观测量（只要其大小合适）。注意，$\{A_x\}_x$ 生成实结合代数 $M_n(\mathbb{R})$ 当且仅当 线性系统 $[SA_x = A_x S$ 对所有 $x]$ 的实数解 $S = cI$ 都是 I 的标量倍数。因此，给定 $\{A_x\}$，可以通过以下方式检验它是否生成整个矩阵代数：假设我们有 X 个（二元、d维）可观测量；那么，对所有 $x]$ 而言，$[SA_x = A_x S$ 构成一个包含d^2 个变量（即 S的矩阵元）和 Xd^2 个方程的线性系统。因此，引理 5.3 的条件等价于检验系数矩阵的秩是否为 $d^2 - 1$。

我们提供的另一条性质有助于上界估计求得 $V_{itr} = V_\infty$ 所需的迭代次数。令U_j 表示由 S_0 中长度至多为 j的所有元素的约当积张成的空间。那么， U_j 与 V_j之间满足以下关系：

引理 5.4 对于一组厄米正交矩阵 $S_0 = \{I, A_x\}$，定义

$$U_j := \mathrm{span}_{\mathbb{R}}\{a_1 \star \cdots \star a_k, a_i \in S_0, k \leq j),$$

并按照命题 V_j 中的定义 5.2 定义 $j \geq 0$。则$U_{2^{(j)}} \subseteq V_j$。

证明。 根据定义， $U_1 = V_0$。现在假设 $U_{2^{(j)}} \subseteq V_j$ 对某个 j成立。根据命题 5.1 $x \star y \in V_{j+1}$对每个 x， $y \in V_j$，因此特别有 $x \star y \in V_{j+1}$对每个 x成立， $y \in U_{2^{(j)}}$。由于 $U_{2^{j+1}} = U_{2 \cdot 2^{(j)}}$由 $U_{2^{(j)}} \star U_{2^{(j)}}$张成，我们得出 $U_{2^{j+1}} \subseteq V_{j+1}$。 ■

请注意，虽然 V_j 不容易确定（因为符号函数是非线性映射），但 U_j 很容易计算。若对于某个 j，有 $U_j = U_{j+1}$ ，则 U_j 是一个约当代数，因此 $U_j = V_\infty$；由此可得迭代次数的上界为 $itr \leq \lceil \log_2 j \rceil$。对于 U_j 停止增长，一个平凡的上界是$d(d+1)\,2$ $= \dim H_d(\mathbb{R})$，因此

$$itr \leq \left\lceil \log_2 \frac{d(d+1)}{2} \right\rceil \leq \lceil 2 \log_2 d \rceil.$$

我们指出，对于具有显式 $\varepsilon - \delta$ 依赖关系的鲁棒自检初始策略，可以反复使用命题3.7 来获得最终策略的鲁棒性。例如，一些鲁棒的

自检验结果汇总于 [ŠB20]，其鲁棒性为 $\varepsilon = O(\sqrt{\delta})$，因此 $O(C\varepsilon + \delta) = O(\sqrt{\delta})$ 在命题 3.7中。如果我们采用这些初始策略，就会得到

$$\varepsilon_\infty = O(\delta^{\frac{1}{2^{ttr}+1}}) = O(\delta^{\frac{1}{4d}}).$$

总结命题5.2 和引理5.4，并应用命题4.6 来讨论多输出（而不仅仅是二元输出）测量，我们得到了一个易于使用的判据，用于判断实测量 O 能否通过迭代自检实现：

定理 5.5 设 $\mathcal{S} = (|\Phi_d\rangle, \{A_x\}, \{B_y\})$ 是一个使用最大纠缠态和二元实投影测量的自检策略。若满足以下条件，则实投影测量 $\{M_\ell, \ell \in [0, L-1]\}$ 可以通过迭代自检实现

$$\tilde{M}_\ell \in \mathcal{JA}(\{\tilde{A}_x\}) \quad \forall \ell \in [0, L-1],$$

其中 $\mathcal{JA}(\{A_x\})$ 是由 $\{A_x\}$生成的实约当代数。此外，迭代次数的上界为 $\lceil 2\log_2 d \rceil$。

特别地，若 $\mathcal{JA}(\{A_x\}) = H_d(\mathbb{R})$，即 $\{A_x\}$ 生成了由对称$d \times d$ 矩阵构成的整个实约当代数，那么每个 d维测量都可以自检验。正如我们在引理5.3中所示，这等价于 $\{A_x\}$ 具有平凡中心化子，而这可以高效地检验。

6 结论

我们通过使用二元测量和最大纠缠态构造自检协议，解决了对任意实射影测量进行自检验的问题。只要维数 d 固定，我们的协议对于任何实射影测量都保持不变。该协议具有一个规模为 $O(d^3)$ 的问题集，以及一个常数规模的答案集。我们证明了该协议具有噪声鲁棒性，这一点从实际应用的角度来看至关重要。我们还引入了一种新颖的迭代自检理论技术，为基于已有自检构建新的自检提供了一种便捷方法。我们的结果表明，可自检观测量的集合包括由我们用于迭代自检的观测量生成的实约当代数。

我们将一些开放问题和改进方向留待未来工作。既然我们知道所有实射影测量都可以进行自检验，一个尚待解决的挑战是提高协议的效率——具体而言，即协议的规模和鲁棒性。已知一些高维态和测量可以进行常数规模自测试（例如 [MPS21、Fu22], 和 [SSKA21、ŠCB21], 它们具有常数规模的问题集）。是否所有量子态和测量都可以通过常数规模协议进行自检验？另一个开放问题是，如何明确给出我们的任意实射影测量自检协议的鲁棒性对 (δ, ϵ) 的依赖关系。这可能会应用于可验证分布式量子计算 [RUV13]。

最后，从理论角度来看，迭代自检也适用于采用部分纠缠态的策略，但其背后的代数结构仍有待理解。

致谢。

本研究由 VILLUM FONDEN 通过 QMATH 卓越中心（资助编号：10059）、Villum 青年研究者资助（编号：37532）、美国国家科学基金会资助（DMS-1954709）以及欧盟“地平线 2020”计划（资助编号：101017733，VERIqTAS；资助编号：101078107，Qinteract）提供支持。

参考文献

[ABDC18] Ole Andersson, Piotr Badzi.ag, Irina Dumitru, and Adán Cabello. 从一个纠缠比特和 Gisin 优雅贝尔不等式中设备无关地认证两比特随机性。《物理评论 *A*》，97:012314，2018年1月。doi:10.1103/PhysRevA.97.012314。[ABG+07] Antonio Acín、Nicolas Brunner、Nicolas Gisin、Serge Massar、Stefano Pironio 和 Valerio Scarani。针对集体攻击的量子密码学设备无关安全。《*Physical Review Letters*》，98:230501，2007年6月。doi:10.1103/PhysRevLett.98.230501。

[BCP+14] Nicolas Brunner、Daniel Cavalcanti、Stefano Pironio、Valerio Scarani 和 Stephanie Wehner。贝尔非定域性。《现代物理评论》，86(2):419–478，2014年4月。doi:10.1103/revmodphys.86.419.[Bel64] John Stewart Bell。论爱因斯坦-波多尔斯基-罗森悖论。《Physics Physique Fizika》，1:195–200，1964年11月。doi:10.1103/PhysicsPhysiqueFizika.1.195.[Bor26] Max Born。论碰撞过程的量子力学。《物理学杂志》，37(12):863–867，1926年。doi:10.1007/BF01397477.[CGS17] Andrea Coladangelo、Koon Tong Goh 和 Valerio Scarani。所有纯双体纠缠态都可以自检验。《自然·通讯》，8(1)，2017年5月。doi:10.1038/ncomms15485.[Col17] Andrea Coladangelo。通过倾斜 CHSH 的多个副本和魔方游戏并行自检验（倾斜）EPR对。《Quantum Info. Comput.》，17(9–10):831–865，2017年8月。doi:10.5555/3179561.3179567.[Fu22] Honghao Fu。有限大小的关联足以自检验维数无界的最大纠缠态。《Quantum》，6:614，2022年1月。doi:10.22331/q-2022-01-03-614.[GP92] N. Gisin 和 A. Peres。任意大自旋下贝尔不等式的最大违背。《物理快报A》，162(1):15–17，1992年。doi:https://doi.org/10.1016/0375-9601(92)90949-M.[Jac68] Nathan Jacobson。《约当代数的结构与表示》，美国数学学会丛书第39卷。美国数学学会，罗得岛州普罗维登斯，1968年。doi:10.1090/coll/039.[JvNW34] Pascual Jordan、John von Neumann 和 Eugene Wigner。论量子力学形式体系的一种代数推广。《数学年刊》，35(1):29–64，1934年。doi:10.2307/1968117.[KŠT+19] J.edrzej Kaniewski、Ivan Šupi´c、Jordi Tura、Flavio Baccari、Alexia Salavrakos 和 Remigiusz Augusiak。最大纠缠与互 unbiased 基产生的最大非定域性，以及双三能级量子系统的自检验。《Quantum》，3:198，2019年10月。doi:10.22331/q-2019-10-24-198.[McC04] Kevin McCrimmon。《约当代数浅谈》。Universitext。施普林格出版社，纽约，2004年。[McK16] Matthew McKague。通过自检验图态实现有界错误量子多项式时间的交互式证明。《计算理论》，12(3):1–42，2016年。doi:10.4086/toc.2016.v012a003.[McK17] Matthew McKague。利用 CHSH 并行进行自检验。《Quantum》，1:1，2017年4月。doi:10.22331/q-2017-04-25-1.[MMG09] Matthew McKague、Michele Mosca 和 Nicolas Gisin。利用实希尔伯特空间模拟量子系统。《物理评论快报》，102(2)，2009年1月。doi:10.1103/physrevlett.102.020505.[MPS21] Laura Manˇcinska、Jitendra Prakash 和 Christopher Schafhauser。用于无界维数量子态和测量的有限规模鲁棒自检验，2021年。doi:10.48550/ARXIV.2103.01729.[MY04] Dominic Mayers 和 Andrew Yao。量子装置的自检验。《 Quantum Info. Comput. 》，4(4):273–286，2004 年 7月。doi:10.5555/2011827.2011830.[PV08] Ká roly F. Pál 和 Tamás Vértesi。高维希尔伯特空间在违背贝尔不等式方面的效率。《Physical Review A》，77(4)，2008年4月。doi:10.1103/physreva.77.042105.

[RTW+21] Marc-Olivier Renou、David Trillo、Mirjam Weilenmann、Thinh P. Le、Armin Tavakoli、Nico- las Gisin、Antonio Acin 和 Miguel Navascues。《基于实数的量子理论可通过实验证伪》。《自然》，600(7890):625–629，2021年。doi:10.1038/s41586-021- 04160-4.[RUV13] Ben W. Reichardt、Falk Unger 和 Umesh Vazirani。《量子系统的经典控制》。《自然》，496(7446):456–460，2013年4月。doi:10.1038/nature12035.[ŠB20] Ivan Šupi´c 和 Joseph Bowles。《量子系统的自检验：综述》。《Quantum》，4:337，2020年9月。doi:10.22331/q-2020-09-30-337.[SBJ+23] Shubhayan Sarkar、Jakub J. Borkała、Chellasamy Jebarathinam、Owidiusz Makuta、De- bashis Saha 和 Remigiusz Augusiak。《在单侧设备无关场景中，使用最少测量实现任意纯纠缠态的自检验与最优随机性认证》。《Physical Review Applied》，19(3)，2023年3月。doi:10.1103/physrevapplied.19.034038.[ŠBR+23] Ivan Šupi´c、Joseph Bowles、Marc-Olivier Renou、Antonio Acín 和 Matty J Hoban。《量子网络可对所有纠缠态进行自检验》。《自然·物理》，19:670–675，2023年2月。doi:10.1038/s41567-023-01945-4.[ŠCB21] Ivan Šupi´c、Daniel Cavalcanti 和 Joseph Bowles。《使用单副本自检协议对量子态张量积进行设备无关认证》。《Quantum》，5:418，2021年3月。doi:10.22331/q-2021-03-23-418.[SSKA21] Shubhayan Sarkar、Debashis Saha、Jédrzej Kaniewski 和 Remigiusz Augusiak。《使用最少测量对任意局部维数的量子系统进行自检验》。《npj Quantum Information》，7(1):1–5，2021年。doi:10.1038/s41534-021-00490-3.[TPKLR22] Armin Tavakoli、Alejandro Pozas-Kerstjens、Ming-Xing Luo 和 Marc-Olivier Renou。《网络中的贝尔非定域性》。《Reports on Progress in Physics》，85(5):056001，2022年3月。doi:10.1088/1361-6633/ac41bb.[WKB+20] Erik Woodhead、Jedrzej Kaniewski、Boris Bourdoncle、Alexia Salavrakos、Joseph Bowles、Antonio Acín 和 Remigiusz Augusiak。《从部分纠缠态中获得最大随机性》。《Physical Review Research》，2:042028，2020年11月。doi:10.1103/PhysRevResearch.2.042028.[WPGF09] Michael M. Wolf、David Perez-Garcia 和 Carlos Fernandez。《在量子理论中不相容的测量无法在任何其他无信号理论中联合测量》。《Physical Review Letters》，103:230402，2009年12月。doi:10.1103/PhysRevLett.103.230402.[YN13] Tzyh Haur Yang 和 Miguel Navascué s。《将未知量子系统鲁棒自检验为任意纠缠双量子比特态》。《Physical Revie w A》，87(5)，2013年5月。doi:10.1103/physreva.87.050102。

A 事后自检验的示例与反例

A.1 二维情形下符号函数的解析像

尽管在一般情况下难以描述符号函数 sgn 的像，但我们给出一个例子，其中 sgn(span$\{D^2, DA_x^{(j)}D\}$)具有解析形式。在这种情况下，初始态是部分纠缠的，$|\psi\rangle = \cos\gamma|00\rangle + \sin\gamma|11\rangle$ 适用于$\gamma \in (0, \frac{\pi}{4})$，而二元可观测量 $A_0 = X$ 是 Pauli X。

我们证明，存在一个参数为 1 的族，其中符号函数（$\{D^2, DA_x^{(j)}D\}$）对应的二元可观测量是事后自检验的。注意，对于 $\tilde{A}_0 = X$，$D\tilde{A}_x D = \sin\gamma\cos\gamma X$。不失一般性，设对于某个实参数 a，sgn($X + aD^2$)= $\tilde{O} =$。若 $|a|$ 较大，则 $X + aD^2$ 是对角占优的，因此 $X + aD^2$ 将是正定或负定，从而导致平凡情形 $O = \pm I$。因此，要得到非平凡的 O，$|a|$ 必须有界，并且当 $X + aD^2$ 变为奇异时达到上界：

$$\det(X + aD^2) = (a\cos\gamma\sin\gamma)^2 - 1 = 0 \Rightarrow a = \pm\frac{1}{\cos\gamma\sin\gamma}.$$

当 $a \in [-\frac{1}{\text{余弦}\ \gamma\ \text{正弦}\ \gamma}, \frac{1}{\text{余弦}\ \gamma\ \text{正弦}\ \gamma}]$时，我们可以将 $\tilde{O}$ 显式地表示为参数 a 的函数：

$$\tilde{O} = \begin{bmatrix} \frac{a(-1+2g^2)}{\sqrt{4+a^2(1-2g^2)^2}} & \frac{2}{\sqrt{4+a^2(1-2g^2)^2}} \\ \frac{2}{\sqrt{4+a^2(1-2g^2)^2}} & \frac{a-2ag^2}{\sqrt{4+a^2(1-2g^2)^2}} \end{bmatrix},$$

其中 $g = \cos\gamma$。设 $\tilde{O} = r_x X + r_z Z$，则 $r_x = \frac{2}{\sqrt{4+a^2(1-2g^2)^2}}$，取值范围为 1 到 $\sin 2\gamma$。因此在这种情况下，符号函数的像为 $\{r_x X \pm \sqrt{1 - r_x^2} Z : \sin(2\gamma) < r_x \leq 1\}$，这是一个不可数集。

我们还给出一个无法通过事后自检验证的显式 $\tilde{O}$：令 $\gamma =$反正切$(1/\sqrt{2})$，$\tilde{O} = H = (X + Z)/\sqrt{2} \notin$ 符号函数(span$\{D^2, X\}$)。那么，一个“作弊”的 POVM $\{\hat{M}_0, \hat{M}_1\}$ 可表示为

$$\hat{M}_0 = \begin{bmatrix} \frac{6-\sqrt{2}}{8} & \frac{\sqrt{2}}{4} \\ \frac{\sqrt{2}}{4} & \frac{\sqrt{2}}{2} \end{bmatrix}, \hat{M}_1 = \begin{bmatrix} \frac{2+\sqrt{2}}{8} & -\frac{\sqrt{2}}{4} \\ -\frac{\sqrt{2}}{4} & 1 - \frac{\sqrt{2}}{2} \end{bmatrix}.$$

可以验证，该 POVM 生成的关联与 O相同，但不存在将它们联系起来的局部等距映射。事实上，假设 $\Phi[I_A \otimes \hat{M}_j |\tilde{\psi}_\gamma\rangle] = I_A \otimes \tilde{M}_j |\tilde{\psi}_\gamma\rangle$ 适用于 $j = 0, 1$，其中 $\tilde{M}_j = \frac{\tilde{O} + (-1)^j I}{2}$，那么我们有

$$0 = \langle\tilde{\psi}_\gamma|I_A \otimes \tilde{M}_0\tilde{M}_1|\tilde{\psi}_\gamma\rangle = \langle\tilde{\psi}_\gamma|I_A \otimes \hat{M}_0\Phi_A^\dagger\Phi_A\hat{M}_1|\tilde{\psi}_\gamma\rangle = \langle\tilde{\psi}_\gamma|I_A \otimes \hat{M}_0\hat{M}_1|\tilde{\psi}_\gamma\rangle \neq 0,$$

矛盾。因此，O 不能基于 $|\psi\rangle$ 和 X进行事后自检。

A.2 事后自检的一个障碍

我们将在此证明，只要输入数量相对于局部维数较少，对自测试策略进行事后扩展就是一种极其非平凡的现象。具体而言，主定理并非平凡结果，因为当局部维数远大于输入数量时，自检验无法扩展到“大多数”二元可观测量。

命题 A.1 设$(|\tilde{\psi}\rangle、\ \{\tilde{A}_x\}_{x=0}^{n-1}、\ \{\tilde{B}_y\}_{y=0}^{n-1})$是一个 n输入／二输出策略，其局部维数为 d。

假设 $|\psi\rangle$ 具有满施密特秩，且可观测量 B_y 在 $M_d(\mathbb{R})$中具有平凡中心化子。

(a) 若 $B_{-n}、\ B_n \in M_d(\mathbb{R})$ 是不同的二元可观测量，则这些策略中没有任何一个$(|\psi\rangle、\ \{A_x\}\ \{B_y, B_{\pm n}\}$)

是另一个策略的局部扩张。***(b)*** 如果 $\lfloor\frac{d^2}{4}\rfloor > n + 1$或 $|\psi\rangle$是最大纠缠态，且 $\lfloor\frac{d^2}{4}\rfloor > n$，那么存在不同的二元观测量 $B_{-n}、\ B_n \in M_d(\mathbb{R})$，使得策略 $(|\psi\rangle, \{A_x\}\ \{B_y, B_{\pm n}\})$ 产生相同的关联，但它们中没有任何一个是另一个的局部扩张（由 ***(a)*** 可知）。

证明。 (a) 假设 $(|\psi\rangle, \{A_x\}$ $\{B_y, B_{-n}\})$ 是 $(|\psi\rangle, \{A_x\}$ $\{B_y, B_n\})$ 的局部扩张。因此，存在等距映射 Φ_A、Φ_B 和一个辅助态 $|\text{aux}\rangle = \sum_i \sigma_i |ii\rangle \in \mathbb{R}^{d'}$，满足 $\sigma_1 > 0$，且 $\Phi_A \otimes \Phi_B |\tilde{\psi}\rangle = |\text{aux}\rangle \otimes |\psi\rangle$，并且

$$(\Phi_A \otimes \Phi_B)(\tilde{A}_x \otimes \tilde{B}_y) |\tilde{\psi}\rangle = |\text{aux}\rangle \otimes ((\tilde{A}_x \otimes \tilde{B}_{|y|}) |\tilde{\psi}\rangle).$$

Then

$$(I \otimes \Phi_B \tilde{B}_y \Phi_B^\dagger)(|\text{aux}\rangle \otimes |\tilde{\psi}\rangle) = (I \otimes I \otimes \tilde{B}_{|y|})(|\text{aux}\rangle \otimes |\tilde{\psi}\rangle)$$

对所有 $y \in \{0, \ldots, n-1, -n\}$。令 $\pi\colon\ \mathbb{R}^d \otimes \mathbb{R}^{d'} \to \mathbb{R}^d$ 为投影 $\mathbb{R}^{d'} \to \mathbb{R}$ 在第一分量上诱导的投影。于是

$$(I \otimes \pi \Phi_B \tilde{B}_y \Phi_B^\dagger \pi^\dagger) |\tilde{\psi}\rangle = (I \otimes \tilde{B}_{|y|}) |\tilde{\psi}\rangle$$

由于 $|\psi\rangle$ 具有满施密特秩，

$$\pi \Phi_B \tilde{B}_y \Phi_B^\dagger \pi^\dagger = \tilde{B}_{|y|}$$

对所有 $y \in \{0, \ldots, n-1, -n\}$。令 $C = \pi \Phi_B \in \mathbb{R}^{d \times d}$。注意，$C$是一个压缩算子。由于对所有 $y \geq 0$，$C\tilde{B}_y C^\dagger = \tilde{B}_y$，且 B_y 作为一个 $\mathbb{R}$-代数生成整个 $M_d(\mathbb{R})$，因此 C 可逆（否则$\tilde{B}_y$ 会有一个公共核）。此外，若 λ 是 $C^\dagger$的一个特征值，则 $C^\dagger v = \lambda v$ 推出$C(\tilde{B}_y v) = \frac{1}{\lambda} \tilde{B}_y v$ 对所有 $y \geq 0$均成立。由于当 $v \neq 0$ 时，$\tilde{B}_y v$ 中至少有一个非零，因此 $\frac{1}{\lambda}$ 是 C的一个特征值。由于 C，$C^\dagger$ 都是压缩算子，我们 conclude that C 是酉。因此

$$C\tilde{B}_y = \tilde{B}_{|y|} C$$

对所有 $y \in \{0, \ldots, n-1, -n\}$都成立。由于 B_y的中心化子是平凡的（在 $M_d(\mathbb{C})$ 中也如此），因此 C是单位算子的一个标量倍。所以 $B_{-n} = B_n$，矛盾。

(b) $M_n(\mathbb{R})$ 中二元可观测量构成的实代数集有一个维数为 $\lfloor \frac{n^2}{4} \rfloor$ 的不可约分支 Z（具体而言，Z是具有 $\lfloor \frac{n}{2} \rfloor$ 个正特征值的二元可观测量集合）。考虑映射

$$Z \to \mathbb{R}^{d+1}, \qquad U \mapsto (\langle\psi| \tilde{A}_x \otimes U |\psi\rangle, \langle\psi| I \otimes U |\psi\rangle); \tag{6}$$

若 $|\tilde{\psi}\rangle$ 是最大纠缠态，则可以舍去最后一个分量 $\langle\psi| I \otimes U |\psi\rangle) = \frac{1}{\sqrt{n}} \operatorname{Tr}(U)$，因为它在 Z上为常数。于是（6）是半代数集之间的线性映射，因此其一般纤维的维数至少为 $\lfloor \frac{d^2}{4} \rfloor - n - 1 > 0$（在最大纠缠的情形下为 $\lfloor \frac{d^2}{4} \rfloor = n > 0$）。因此存在互不相同的 B_{-n}，$B_n \in Z$ 使得

$$\langle\tilde{\psi}| I \otimes \tilde{B}_{-n} |\tilde{\psi}\rangle = \langle\tilde{\psi}| I \otimes \tilde{B}_n |\tilde{\psi}\rangle, \quad \langle\tilde{\psi}| \tilde{A}_x \otimes \tilde{B}_{-n} |\tilde{\psi}\rangle = \langle\tilde{\psi}| \tilde{A}_x \otimes \tilde{B}_n |\tilde{\psi}\rangle$$

对所有 x均成立。 ■

如果 $|\psi\rangle$ 是最大纠缠态，且 $A_y = B_y$，那么我们知道，经过足够多的事后步骤后，所有二元可观测量都可以自检验（在满足关于 B_y的给定条件下）。命题A.1(b) 保证，当输入数量 n 远小于局部维数 d时，第一步之后并不总能立即实现这一点；对于第 $d+1$4节中含有 $d+1$ 个输入的首选策略，命题保证存在“坏的”二元可观测量 $d \geq 5$。然而，对于 $d = 3$，它们已经存在：

例 A. 2 $\tilde{A}_0 \ldots \tilde{A}_3 \in M_3\ \mathbb{R}$ 5, $|\Phi_3\rangle \in \mathbb{R}^3 \otimes$ 令 , , () 为第 节中的二元可观测量，$\mathbb{R}^3$ $\tilde{S} = |\Phi_3\rangle\ \{\tilde{A}_x\}_x\ \{\tilde{A}_x\}_x\}$ 并令 为最大纠缠态（在其施密特基下）。那么(, , 可由其关联自检验，且 $\{A_x\}_x$ 在 $M_3(\mathbb{R})$中具有平凡中心化子。直接计算可得

$$\tilde{A}_{\pm 4} = \begin{pmatrix} 0 & -\frac{1}{\sqrt{2}} & \pm\frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & -\frac{1}{2} & \mp\frac{1}{2} \\ \pm\frac{1}{\sqrt{2}} & \mp\frac{1}{2} & -\frac{1}{2} \end{pmatrix}$$

是只有一个正特征值的二元可观测量，并且

$$\langle\Phi_3| \tilde{A}_x \otimes A_{-4} |\Phi_3\rangle = \langle\Phi_3| \tilde{A}_x \otimes A_4 |\Phi_3\rangle \qquad \textit{for } x = 0, \ldots, 3.$$

因此，根据命题($|\Phi_3\rangle$，$\{A_x\}$ $\{A_x, A_{\pm 4}\}$) 这些策略给出了相同的关联，但根据命题 *A.1(a)*，它们彼此并非局部扩张，因此它们不是自检验的。

B 鲁棒自检验策略的构造方法

我们首先展示如何构造 $d+1$ 个单位向量 v_0，……，$v_d \in \mathbb{R}^d$ 使其构成以原点为中心的正$d+1$维单纯形的顶点。对于所有 $j \neq k$，这可由 $\langle v_j, v_k \rangle = -1/d$ 保证。为找到满足这一性质的向量，考虑 $\mathbb{R}^{d+1}$ 中的任意酉矩阵 U，其第一行为全一单位向量 $a = (1, 1, \ldots\ldots, 1)/\sqrt{d+1}$。然后，将 U 作用于向量 $d+1$ $\{f_j\}$，其中 f_j 是 $f'_j = e_j - \langle a, e_j \rangle a$的归一化向量，而 $\{e_j\}_{j=0}^d$是基向量。我们有，所有 Uf_j都与 e_0正交。因此，$\{Uf_j\}_{j=0}^d$张成一个 d维子空间。我们还可以证明 $\langle Uf_j, Uf_k \rangle = \langle f_j, f_k \rangle = -1/d$。因此我们取 $v_x = Uf_x$、$\tilde{P}_x = v_x v_x^\dagger$和 $\tilde{T}_x = 2\tilde{P}_x - I$。

(*局部维数*) d = 4; (*寻找酉矩阵*) allone =Normalize[ConstantArray[1, d + 1]]; unitary =ConstantArray[0, {d + 1, d + 1}]; unitary[[1, All]] = allone; unitary[[2 ;; d + 1, All]] =Table[UnitVector[d + 1, i], {i, 2, d + 1}]; unitary = Orthogonalize[unitary]; (*d+1 个向量*) vect[x_]:= (unitary . Normalize[(UnitVector[d + 1, x] - Projection[UnitVector[d + 1, x], allone])])[[2;; d + 1]]// 完全化简; (*d+1 个投影算子*) proj[x_]:= 转置[{vect[x]}] . {vect[x]} // 完全化简; (*d+1 个二元可观测量*) obs[x_]:= 2proj[x] - IdentityMatrix[d]; jordanproduct[x_, y_]:=(x . y + y . x)/2; 符号函数[x_] :=JordanDecomposition[x][[1]] . 实符号函数[JordanDecomposition[x][[2]]] . Inverse[JordanDecomposition[x][[1]]] // 完全化简; (* 替代符号映射*) (* 符号函数[x_]:= Inverse[x].MatrixPower[x.x,1/2] *)

基于此，可以计算 $\tilde{T}_{jk} =$ 符号函数$(\tilde{T}_j + \tilde{T}_k)$，或者计算 $\tilde{T}_{jk} = 2w_{jk}w_{jk}^\dagger - I$，其中$w_{jk} := \sqrt{2}^{\,d}\,(\overline{d+1}(v_j - v_k)$。

观测量2[x_、y_] :=符号函数[观测量[x] + 观测量[y]]; (*替代 O_{jk} 算子*) (* 观测量2[x_、y_]:=d/(d+1) \ 转置[{vect[x]-vect[y]}].{vect[x]-vect[y]}//完全化简;*)