物理学报 Acta Physica Sinica
Chinese Physical Society
Institute of Physics, CAS

制备-测量量子比特系统的自测试标准

王玉坤　李泽阳　许康　王子正

Self-testing criteria for preparing-measuring qubit system

Wang Yu-Kun　Li Ze-Yang　Xu Kang　Wang Zi-Zheng

引用信息 Citation: Acta Physica Sinica, 72, 100303 (2023)　DOI: 10.7498/aps.72.20222431
在线阅读 View online: https://doi.org/10.7498/aps.72.20222431
当期内容 View table of contents: http://wulixb.iphy.ac.cn

制备-测量量子比特系统的自测试标准*

王玉坤[1)2)†] 李泽阳[1)] 许康[1)] 王子正[1)]

1) (中国石油大学 (北京), 北京石油数据挖掘重点实验室, 北京 102249)

2) (密码科学技术全国重点实验室, 北京 100036)

(2022 年 12 月 24 日收到; 2023 年 2 月 28 日收到修改稿)

自测试是对所声称量子设备的一种高安全级别验证, 仅根据设备观测到的统计数据来确认设备中所制备的量子态和所执行的测量. 制备-测量场景下量子系统的自测试可依赖于测量统计关联来实现. 目前针对制备-测量场景量子系统自测试的研究比较单一, 只有当统计关联满足一定的不等式要求时才能实现其系统的自测试. 本文进一步提出了制备-测量场景下量子比特态制备集和测量集实现自测试的新标准, 实现了比 BB84 粒子更多的量子比特态集及测量集的自测试, 这有利于满足实际实验对不同量子态集制备的需求. 此外, 对所提出的标准进行了鲁棒性分析, 使新标准在实验噪声下具有实际意义. 本文的研究增加了量子比特态制备和测量系统自测试标准的多样性, 有利于实际不同非纠缠单量子系统的自测试.

关键词: 自测试, 制备与测量系统, 目击违背, 鲁棒性

PACS: 03.65.Ud, 03.67.–a **DOI:** 10.7498/aps.72.20222431

1 引 言

近年来, 量子计算、量子通信和量子测量等技术不断取得突破, 推进了量子信息技术的实用化进程. 然而与真正实用化还存在距离, 其中一个制约因素是量子系统的可信性. 在实际中, 用户购买的量子设备可能不可信, 存在缺陷甚至来自恶意供应方, 可以说量子设备的可信性决定了量子信息处理任务的安全性.

量子系统自测试是保证实际设备不可信量子信息处理任务顺利完成的关键技术, 是量子态和量子测量设备的在设备无关 (device independent, DI)[1−3] 下的表征, 通常也被简化为“盲层析”. 假设量子系统是一个“黑盒”, 自测试的目的是根据观测到的设备输入输出之间的统计值, 推断出量子设备中量子态的状态和具体所执行的量子测量操作. 自测试理论可行性依据在于, 一些由量子理论预测的观测统计具有唯一性, 这种唯一性可以唯一地确定出系统中的量子态和测量. 设备无关表征确保了自测试可以使设备的可信性测试从复杂的内部细节中 (如具体的维度假设, 具体的测量参数等) 解放出来, 转而检查实验观测到的概率分布[2].

在量子物理中, 量子态的状态可能是纠缠的, 量子测量可能是不相容的. 这些不同于经典物理的特征能表现出惊人的观测现象: 在纠缠量子态的局域子系统上进行不相容的测量可以显示出比经典理论所产生的任何结果都更强的相关性, 即所称的 Bell 非局域性[4,5]. 作为反映量子与经典物理学本质差别的一个引人注目的现象, Bell 非局域性目前是一个非常活跃领域, 有着非常广泛的应用[6−11]. 随着对 Bell 非局域性研究的深入, 学者们发现, 存在 Bell 非局域关联[4], 其不仅需要纠缠源和不相容的量子测量, 而且只能通过对特定的纠缠态进行特

* 国家自然科学基金 (批准号: 62101600)、中国石油大学 (北京) 科研基金 (批准号: 2462021YJRC008) 和密码科学技术全国重点实验室基金 (批准号: MMKFKT202109) 资助的课题.

† 通信作者. E-mail: wykun06@gmail.com

定的不相容测量来实现. 例如, 研究发现 Clauser-Horn-Shimony-Holt (CHSH) 不等式 [4] 的最大违背可以唯一地刻画出设备中的态为两粒子最大纠缠态. 然而直到 2004 年, Mayers 和 Yao[2] 才第一次明确地给出了自测试 (self-testing) 这一概念, 并引起了设备无关量子信息处理领域的研究, 目前已经成为国内外学者研究的热点.

自测试的核心问题是对于未知的量子设备, 通过观测设备输入输出之间的条件概率统计 $p(x|r)$, 来推断设备中的量子态和测量操作. 很容易想到, 经典统计到量子系统的映射是一对多. 不同的态和测量操作可能给出相同的统计值, 即存在 $\mathrm{tr}(\rho_1 M_1)=\mathrm{tr}(\rho_2 M_2)$, 其中 $\{\rho_1, M_1\}$ 与 $\{\rho_2, M_2\}$ 不同. 此外, $\{\rho_1, M_1\}$ 与 $\{\rho_2, M_2\}$ 可以是酉等价的系统, 也可以非酉等价, 甚至于维度也可以不同. 因此概率统计必须满足一定的条件, 才有可能“唯一”地确定设备中的态和测量操作. 此外由于在局域同构映射下等价的量子系统能完成同样的量子信息处理任务, 因而在信息处理能力的角度上不必区分这种等价的系统. Mayers 和 Yao[2] 给出自测试的定义: 在局域同构映射等价的意义下, 观测到的相关性唯一地确定了设备中的未知系统.

自 Mayers 和 Yao[2] 的相关研究之后, 自测试受到了极大的关注. 以往的研究大多都集中在对于设备之间共享纠缠态系统的自测试, 例如包括单态 [12]、W 态 [13]、图态 [14]、Dicke 态 [15]、三方对称纠缠态 [16]、高维纠缠态 [17] 等. 在对设备中量子态进行自测试的同时, 测量操作也可以同时实现自测试, 也就是量子态和量子测量设备是通过同一个观测标准同时实现自测试的. 这些自测试方案指的是设备无关的表征, 在设备无关的框架中, 非局域性在量子系统的自测试中起着至关重要的作用. 并在此基础上, 提出了超越非局域性甚至是纠缠的更为一般性的量子自测试情形. Šupić和 Hoban[18] 提出了通过量子导引而不是非局域性的量子系统自测试. 量子导引位于纠缠态和贝尔非局域性之间: 证明贝尔非局域性的量子态构成了证明 EPR 导引的量子态子集, EPR 导引也构成了纠缠态子集. Tavakoli 等 [19] 基于维度目击违背不等式研究了制备和测量系统自测试的方法, 其中不涉及纠缠系统. 将来可能会有其他更为通用的自测试情形出现.

本文考虑制备和测量情形下的自测试, 即非纠缠量子系统的自测试. 其涉及 $2\to 1$ 量子随机访问码 (quantum random access code, QRAC)[20,21], 其中 4 个制备态记为 $\{\rho_x\}_{x\in(0,1)^2}$, 相关的两个半正定算子测量 (positive opeartor-valued measurement, POVM) 记为 $\{M_y\}_{y\in(0,1)}$, $\{\rho_x, M_y\}$ 是需要自测试的集合. 该非纠缠量子系统在各种量子信息处理任务中有非常重要的应用, 如量子随机性认证 [22]、量子密钥分发 [23] 等. 文献 [19] 基于一种维度目击不等式的违背对量子比特态和测量 $\{\rho_x, M_y\}$ 集合进行了自测试. 指出见证维度不等式的最大违背能同时对设备中的量子比特态和测量 $\{\rho_x, M_y\}$ 集合进行自测试. 不等式为 $W=\sum_{x,y} c_{x,y} p(0|x,y)\leqslant 2$, 其中 $c_{x,y}=(-1)^{x_y}$, $p(0|x,y)=\mathrm{tr}(\rho_x M_y^0)$. 量子系统的最大违背值是 $2\sqrt{2}$, 而经典系统的最大违背值是 2. 然而, 除了不等式的最大违背外, 任意离最大违背存在偏离的统计, 都无法实现所制备的量子态和测量的自测试. 那么除了对不等式 W 的最大违背之外, 是否还有其他方法可以同时对量子态和测量进行自测试的统计标准. 如果有, 有多少标准是值得研究的问题. 本文的主要目的是给出在上述制备-测量量子比特系统所有可实现其自测试的新标准. 已知描述上述制备-测量情形的测量结果蕴含着比单个不等式更为丰富的信息. 因此, 本文将直接关注全观测统计, 并给出观测统计量的自测试标准, 该标准可实现一系列制备态集合和测量集合的自测试. 此外, 考虑到在实际实验中由于实验噪声、探测效率及统计误差的存在, 设备的输入输出之间的统计关联值常常达不到理想值. 为了使自测试方案真正成为一项有实际意义的检测方案, 我们进一步给出了所提方案的鲁棒性分析.

本文第 2 节给出本文所涉及的研究场景、自测试的定义及局域同构映射的构造; 主要结论将在第 3 节以定理的形式给出, 并在 3.1 节中给出了严格的证明; 3.2 节介绍了在实验有噪声、误差时自测试方案的鲁棒性分析, 并具体给出了几种自测试方案的鲁棒性比较; 最后, 第 4 节是文章的总结部分.

2 预备知识

2.1 自测试定义

自测试最初被称为 DI 态验证, 一些从量子设备观测到的统计值 $p(a,b|x,y)$ 可以“唯一”地确定底

层量子态和测量. 考虑单体量子态的制备及测量情形, 除维度假定为 2 维以外, 不对 Alice 和 Bob 设备内部参数进行假设. 具体地, Alice 随机制备量子态 $\{\rho_x\}_x$, 由指标 $x=00,01,10,11$ 来控制, 发送给 Bob. 同时 Bob 随机选择两种测量 $\{M_y\}_y$, 由 $y=0,1$ 来控制测量的选择, 其中每个测量基对应两个输出结果 $b=0,1$, 用测量算子 M_y^b (其中 $M_y^b=\left[I+(-1)^b M_y\right]/2$) 表示. 具体场景见图 1. 每一轮实验中 Alice 和 Bob 都随机地选择一个制备态和测量, 即选择 (x, y). 经过大量次实验后, Alice 和 Bob 可以构造出联合概率分布, 即 $p(b|x,y)=\mathrm{tr}(\rho_x M_y^b)$.

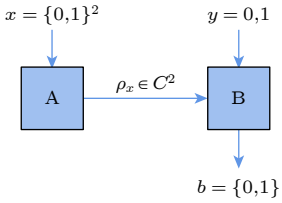

图 1 制备测量量子系统示意图, 其中 Alice 一侧随机制备 4 个量子态由 x 来控制态的选择; Bob 一侧随机从两个测量基中进行选择, 以测量发送来的量子态, 由 y 控制

Fig. 1. Schematic diagram of the preparation measurement quantum system, in which four quantum states are randomly prepared on Alice's site and x controls the selection of states. The measurements in Bob's site are randomly selected from two measurement bases with y.

由于维度是固定的, 不失一般性设备中的测量可以假设为一般半正定形式 POVM. 然而, 已知在两个测量并且每个测量都有两个结果时, 所有测量得到的统计概率所构成的概率空间的极值点都可以通过用正交投影 POVMs 测量纯态来实现[24,25]. 理论上, 由于统计概率空间的凸性, 也只有纯态和投影测量得到的统计才能实现自测试的任务. 显然, 只有极值点是可实现自测试的概率统计值. 因此, 在这里只考虑纯态和投影测量情形, 非纯态和投影测量系统的测量统计可以由极值点的线性组合给出. 注意到, 在二维希尔伯特空间中量子系统可以用 Bloch 球表示. 所以将制备态表示为 $\{\rho_x=(I+\boldsymbol{r}_x\cdot\boldsymbol{\sigma})/2\}_x$, 测量表示为 $\{M_y=\boldsymbol{b}_y\cdot\boldsymbol{\sigma}\}_y$, 其中 $|\boldsymbol{r}_x|=|\boldsymbol{b}_y|=1$. 利用量子态及测量的 Bloch 球表示, 统计值 $\mathrm{tr}(\rho_{00}M_y)$ 有表 1 的表达形式, 该值可通过 QRAC 实验得到. 具体为 $\mathrm{tr}(\rho_{00}M_y)=p(0|x,y)-p(1|x,y)$, 其中联合概率 $p(b|x,y)$ 可由实际实验直接观测到.

表 1 QRAC 实验中统计值 $\mathrm{tr}(\rho_{00}M_y)$ 在 Bloch 球上的表示

Table 1. The Bloch sphere expression of the value of $\mathrm{tr}(\rho_{00}M_y)$ in QRAC experiment.

制备态	测量基	
	M_0	M_1
ρ_{00}	$\mathrm{tr}(\rho_{00}M_0)=\boldsymbol{r}_{00}\cdot\boldsymbol{b}_0$	$\mathrm{tr}(\rho_{00}M_1)=\boldsymbol{r}_{00}\cdot\boldsymbol{b}_1$
ρ_{01}	$\mathrm{tr}(\rho_{01}M_0)=\boldsymbol{r}_{01}\cdot\boldsymbol{b}_0$	$\mathrm{tr}(\rho_{01}M_1)=\boldsymbol{r}_{01}\cdot\boldsymbol{b}_1$
ρ_{10}	$\mathrm{tr}(\rho_{10}M_0)=\boldsymbol{r}_{10}\cdot\boldsymbol{b}_0$	$\mathrm{tr}(\rho_{10}M_1)=\boldsymbol{r}_{10}\cdot\boldsymbol{b}_1$
ρ_{11}	$\mathrm{tr}(\rho_{11}M_0)=\boldsymbol{r}_{11}\cdot\boldsymbol{b}_0$	$\mathrm{tr}(\rho_{11}M_1)=\boldsymbol{r}_{11}\cdot\boldsymbol{b}_1$

经典统计到量子系统的映射通常是一对多的. 自测试指由量子理论预测的 $p(b|x,y)$ 唯一地决定量子态和量子测量. 下面给出具体的定义形式. 与文献 [11, 26—29] 中介绍的纠缠自测试方法类似, 将自测试系统"交换"到辅助系统, 构造图 2 中的局域同构 Φ 用来将自测试系统交换到辅助系统. 因此, 自测试可以正式的由定义 1 给出.

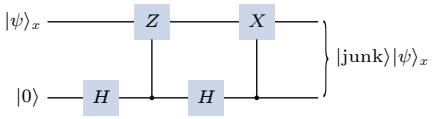

图 2 允许对制备状态和相应测量操作进行自测试的局域同构映射, H 为哈达玛门, Z 和 X 为与泡利 σ_x, σ_z 门局域等价的门, $|0\rangle_{\mathrm{ancilla}}$ 是辅助系统, 具有所需自测试系统的正确维度, 并将输入态系统记为主 (Main) 系统

Fig. 2. The local isometry for the prepared states and corresponding measurements. H is the Hadamar gate, Z and X is the locally equivalent gate to the Pauli gate σ_x,σ_z. $|0\rangle_{\mathrm{ancilla}}$ is ancilla system, which has the correct dimensions for the system to be self-tested, and the input-state system is labeled as the Main system.

定义 1 对于观测统计量 $p(b|x,y)$, 如果存在 Φ 使得下式成立, 则称观测统计量 $p(b|x,y)$ 可以确定系统中的量子态与 BB84 粒子 $|\mathrm{BB84}_x\rangle\in\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$ 酉等价, 其相关测量与泡利测量 $M_y^{\mathrm{target}}=\dfrac{\sigma_x+(-1)^y\sigma_z}{\sqrt{2}}$ 酉等价. 具体为

$$\begin{aligned}&\Phi|\psi_x\rangle|0\rangle_{\mathrm{ancilla}}=|\mathrm{junk}\rangle(|\mathrm{BB84}_x\rangle)_{\mathrm{ancilla}},\\&\Phi M_y|\psi_x\rangle|0\rangle_{\mathrm{ancilla}}=|\mathrm{junk}\rangle(M_y^{\mathrm{target}}|\mathrm{BB84}_x\rangle)_{\mathrm{ancilla}}.\end{aligned}\quad(1)$$

其中, $|0\rangle_{\mathrm{ancilla}}$ 是辅助系统, 具有所需自测试系统的维度, 并将输入态及测量 $\{|\psi_x\rangle,\ M_y\}$ 系统记为主 (Main) 系统, 即要测试的系统. Φ 为局域同构映射, 是根据测量操作构造的"虚拟"运算, 在实际实验中并不存在. 即 Φ 只是作为一种分析工具, 其功能是将主系统交换到附加系统. 如果可以找到这么一个

Φ, 使得交换到附加系统中的部分恰好为目标系统, 剩余的系统与所提取出的系统成直积关系, 即无任何关联, 此时可以称为"残余"$|\text{junk}\rangle$, 那么就可以实现目标系统的自测试.

定义 1 说明了由特殊的量子统计关联可以唯一地确认设备中的量子系统. 这里的唯一是在局域同构映射等价的意义下定义的. 此外由于在局域同构映射下等价的量子系统能完成同样的量子信息处理任务, 因而在信息处理能力的角度上不必区分这种等价的系统. 因此, 通常讲自测试技术在局域同构映射等价的意义下, 能唯一地确定设备中的未知系统.

2.2 局域同构运算构造

如上所述, 在自测试定义中引入的局域同构映射实际上是一个虚拟协议. 在实验中, 需要做的就是查询黑盒统计到联合概率分布 $p(b|x,y)$. 从联合概率中推测出 Bob 一侧测量间的相互关系, 依此来构造局域同构映射. 局域同构映射的构造原则上不唯一, 而且不同的构造形式可能影响着协议鲁棒性分析. 这里借助在设备无关情形下常用的构造形式, 如图 2 所示. 这种构造可以被理解为一个"交换操作", 它将顶部线中的系统交换到辅助系统. 它的构造灵感来自于在设备可信的情形下, 该操作可以将目标系统交换到附加系统上.

具体地, 在设备可信情形下线路中的 Z, X 就定义为 σ_z, σ_x 操作. 通过这种交换, 可以通过辅助系统来研究原始系统的具体形式. 在利用这种酉变换后, 辅助系统变为

$$\begin{aligned}
&\mathrm{tr}_{\text{Main}}\left(\Phi|\psi_x\rangle\langle\psi_x|(|0\rangle\langle 0|)_{\text{ancilla}}\right)\\
=&\left[\langle\psi_x|\frac{I+Z}{2}|\psi_x\rangle|0\rangle\langle 0|_{\text{ancilla}}\right.\\
&+\langle\psi_x|\frac{2X+2\mathrm{i}Y}{4}|\psi_x\rangle|0\rangle\langle 1|_{\text{ancilla}}\\
&+\langle\psi_x|\frac{2X-2\mathrm{i}Y}{4}|\psi_x\rangle|1\rangle\langle 0|_{\text{ancilla}}\\
&\left.+\langle\psi_x|\frac{I-Z}{2}|\psi_x\rangle|1\rangle\langle 1|_{\text{ancilla}}=|\psi_x\rangle\langle\psi_x|\right., \quad (2)
\end{aligned}$$

其中 Z, X 和 Y 对应为 σ_x, σ_y 和 σ_z 门, 分别为局域酉门. 显然这种构造, 将 $|\text{BB84}_x\rangle\in\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$ 粒子变换为 $|\text{BB84}_x\rangle\in\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$ 粒子. 同时, 将测量 $\{M_y=\boldsymbol{b}_y\cdot\boldsymbol{\sigma}\}_y$ 变换为 $M_y^{\text{target}}=\dfrac{\sigma_x+(-1)^y\sigma_z}{\sqrt{2}}$ 测量.

$$\begin{aligned}
&\mathrm{tr}_{\text{Main}}\left(\Phi M_y|\psi_x\rangle\langle\psi_x|M_y(|0\rangle\langle 0|)_{\text{ancilla}}\right)\\
=&\left[\langle\psi_x|M_y\frac{I+Z}{2}M_y|\psi_x\rangle|0\rangle\langle 0|_{\text{ancilla}}\right.\\
&+\langle\psi_x|M_y\frac{2X+2\mathrm{i}Y}{4}M_y|\psi_x\rangle|0\rangle\langle 1|_{\text{ancilla}}\\
&+\langle\psi_x|M_y\frac{2X+2\mathrm{i}Y}{4}M_y|\psi_x\rangle|1\rangle\langle 0|_{\text{ancilla}}\\
&\left.+\langle\psi_x|M_y\frac{I-Z}{2}M_y|\psi_x\rangle|1\rangle\langle 1|_{\text{ancilla}}\right]\\
=&M_y^{\text{target}}|\psi_x\rangle\langle\psi_x|M_y^{\text{target}}. \quad (3)
\end{aligned}$$

在实际中, 图 2 中的 Z, X 并不确定为 σ_z, σ_x, 但保持 σ_z, σ_x 之间的相对关系. 它们是与实际设备中的测量操作相关的, 由实际测量操作来构造. 例如, 如果观测到的统计量满足:

$$\begin{aligned}
&\boldsymbol{r}_{00}\cdot\boldsymbol{b}_0=\boldsymbol{r}_{01}\cdot\boldsymbol{b}_0=\boldsymbol{r}_{00}\cdot\boldsymbol{b}_1=\boldsymbol{r}_{10}\cdot\boldsymbol{b}_1=\frac{1}{\sqrt{2}},\\
&\boldsymbol{r}_{10}\cdot\boldsymbol{b}_0=\boldsymbol{r}_{11}\cdot\boldsymbol{b}_0=\boldsymbol{r}_{01}\cdot\boldsymbol{b}_1=\boldsymbol{r}_{11}\cdot\boldsymbol{b}_1=-\frac{1}{\sqrt{2}}. \quad (4)
\end{aligned}$$

那么就可知道 $\boldsymbol{b}_0\cdot\boldsymbol{b}_1=0$. 显然 M_0, M_1 具有 Z, X 之间的相对关系. 因此, 可定义 $Z=M_0$, $X=M_1$. 显然, 如果 $|\psi_x\rangle$ 与 Z 和 X 在同一平面上, 那么得到的辅助量子比特是一个纯态并且正好是 $|\psi_x\rangle$, 同时测量 $M_0|\psi_x\rangle$ 为 $\sigma_z|\psi_x\rangle$, $M_1|\psi_x\rangle$ 为 $\sigma_x|\psi_x\rangle$. 也就是说, 图 2 中的控制操作将相关的自测试系统交换到 Z 和 X 平面中的可信辅助量子比特, 而且在酉等价的意义下它们即为目标系统.

3 主要结果

文献 [19] 利用维度目击违背不等式作为量子比特态制备-测量系统自测试的标准. 作者指出维度目击不等式的最大违背能够同时对设备中的量子比特态和测量 $\{\rho_x,M_y\}$ 集合进行自测试, 其不等式为

$$W=\sum_{x,y}c_{x,y}p(0|x,y)\leqslant 2\sqrt{2}, \quad (5)$$

其中 $c_{x,y}=(-1)^{x_y}$, $p(0|x,y)=\mathrm{tr}(\rho_xM_y^0)$. 使得违背值达到 $2\sqrt{2}$ 的系统酉等价于 $|\text{BB84}_x\rangle\in\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$ 粒子和 $M_y^{\text{target}}=\left[\sigma_x+(-1)^y\sigma_z\right]/\sqrt{2}$ 测量. 因此说明, W 的最大量子违背值可以唯一地实现 BB84 系统的自测试.

然而可以看到, 利用目击违背不等式 W 的方法并不能区分并实现以下系统的自测试.

第 1 个系统:

$$\begin{aligned}
&\boldsymbol{r}_{00}=\Big[\cos^2(\theta),\cos(\theta)\sin(\theta),\\
&\qquad\sqrt{\sin^2(\theta)-\cos^2(\theta)}\,\Big]/\sin(\theta);\\
&\boldsymbol{r}_{01}=[-\sin(\theta),\cos(\theta),0];\\
&\boldsymbol{r}_{10}=[\sin(\theta),-\cos(\theta),0];\\
&\boldsymbol{r}_{11}=\Big[-\cos^2(\theta),-\cos(\theta)\sin(\theta),\\
&\qquad\sqrt{\sin^2(\theta)-\cos^2(\theta)}\,\Big]/\sin(\theta);\\
&\boldsymbol{b}_0=[0,1,0];\ \boldsymbol{b}_1=[\sin(2\theta),-\cos(2\theta),0].
\end{aligned}\tag{6}$$

第 2 个系统:

$$\begin{aligned}
&\boldsymbol{r}_{00}=[\cos(\alpha),\sin(\alpha),0];\\
&\boldsymbol{r}_{01}=[\sin(\alpha),-\cos(\alpha),0];\\
&\boldsymbol{r}_{10}=[-\sin(\alpha),\cos(\alpha),0];\\
&\boldsymbol{r}_{11}=[-\cos(\alpha),-\sin(\alpha),0];\\
&\boldsymbol{b}_0=[0,1,0],\ \boldsymbol{b}_1=[\cos(2\alpha),-\sin(2\alpha),0].
\end{aligned}\tag{7}$$

其中, $\cos(\theta)=\sin(\pi/4+\alpha)/\sqrt{2}$. 通过计算, 两个系统的测量统计值相同, 均为 $W=4\cos(\theta)$. 所以用目击违背不等式 W 的方法并不能来区分这两个量子系统. 事实上, 除了 $\theta=\pi/4$ 外, 两个系统并不是酉等价的. 此时不等式 W 也并不能达到最大违背值, 因而并不能实现上述两种系统的自测试. 主要结论是给出下面的定理, 该定理描述了基于所有测量统计量而非不等式的方法对量子态集合和相应测量进行自测试的标准. 基于该定理可以得到上述第 2 个系统可以实现自测试.

3.1 理想情形

在无噪声情况下, 即假设统计到的概率是实际条件概率时有如下定理.

定理 1 考虑 4 个未知的制备纯态 $\{\rho_{00},\rho_{01},\rho_{10},\rho_{11}\}$ 和两个投影测量 $\{M_0,M_1\}$, 其中二进制结果标记为 ±1. 观测到相关性 $E_{xy}\equiv\mathrm{tr}(\rho_xM_y)$ 唯一地自测试设备中的制备态和测量 (在局部酉等价意义下), 如果:

1) 对于表 1 中任一行, 记为 t, 都存在另一行 t', 使 t 和 t' 这两行中观察得到的统计量满足以下 8 个条件中的一个

$$\begin{aligned}
&\sum\nolimits_{(x,y)\neq(i,j)}\arcsin(E_{xy})-\arcsin(E_{ij})\\
&=\xi\pi x,i\in\{t,t'\},\xi\in\{+1,-1\},
\end{aligned}\tag{8}$$

其中 $\arcsin(E_{xy})_{x,y\in\{0,1\}}\in\left[-\frac{\pi}{2},\frac{\pi}{2}\right]$, 并且假设 $\arccos(E_{xy})=0$ 或 π 至多对一对 (x,y) 成立.

2) 至少存在一行 t 使 1) 发生两次, 并且在 (8) 式中有不同的条件.

证明

1) 如果观测到的统计数据允许量子描述, 那么可以表示 $\mathrm{tr}(\rho_xM_y)\equiv\boldsymbol{r}_x\cdot b_y=\cos\alpha_{xy}$ 有 $\alpha_{xy}\geqslant0$. 给定它们与 b_0 的标量积, $\boldsymbol{r}_x$ 与 $\boldsymbol{r}_{t'}$ 之间的角度 θ 必须满足

$$|\alpha_{t0}-\alpha_{t'0}|\leqslant\theta\leqslant\alpha_{t0}+\alpha_{t'0},\tag{9}$$

当 $\boldsymbol{b}_0$ 位于同一平面 (在任意一侧或在两个平面之间) 时达到上界和下界. 类似地, 因为有 $\boldsymbol{b}_1$ 的标量积, 所以可得

$$|\alpha_{t1}-\alpha_{t'1}|\leqslant\theta\leqslant\alpha_{t1}+\alpha_{t'1},\tag{10}$$

(8) 式中的 8 个等式在某种意义上是等价的, 即每个等式都可以通过重新标记测量或者测量的结果转换为另一个等式[24,25]. 因此, 在不失一般性的情况下, 考虑 $i=0$, $j=1$ 和 $\xi=+1$. (8) 式可以重写为

$$\arccos(E_{t0})+\arccos(E_{t'0})=\arccos(E_{t1})-\arccos(E_{t'1}),$$

即

$$\alpha_{t0}+\alpha_{t'0}=\alpha_{t1}-\alpha_{t'1},\tag{11}$$

结合 (9) 式与 (10) 式, 特别是当所有 4 个向量都位于图 3 中所示位置的同一平面内时, 表明 $\theta=\alpha_{t0}+\alpha_{t'0}=\alpha_{t1}-\alpha_{t'1}$. 因此得到结论, 如果观测到的统计数据允许量子描述, 那么制备的量子态和相应的测量与图 3 所示的系统局部酉等价.

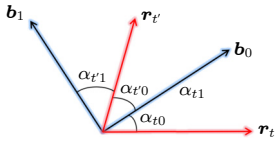

图 3 t 和 t' 行的态及测量操作所对应方向的空间位置关系

Fig. 3. The spatial position relation of the states and the measurements directions in t and t' rows.

2) 仅仅是 (8) 式中的条件则不足以保证观测到的统计数据来自量子系统. 事实上, 制备的量子态的数量应该大于 2, 否则输入 x 可以用经典比特 a 完美地编码并传输给 Bob, 此时 Bob 可以输出与任何概率分布 $p(b|x,y)$ 兼容的 b, 即在只有两个制备态时, 得到的概率统计可以由经典系统来描述. 此时, 两个设备的行为可以通过依赖于设备之间共

享的附加隐藏随机参数 λ 来关联[30], 在这种情况下

$$p(b|x,y)=\sum_{\lambda}\rho(\lambda)\,D_{\lambda}(b|a,y)\,, \tag{12}$$

其中, $p(\lambda)$是 λ 的密度函数 $D_{\lambda}(b|a,y)\in\{0,1\}$是确定性事件.

这里使用条件 2) 是确保至少制备了 3 个不同的量子态. 也就是说, 如果至少存在一行 t 使 1) 发生两次, 并且在 (8) 式中有不同的条件, 那么就可以保证观测到的统计数据来自量子系统.

到目前为止, 已经证明了定理 1 中的所有标准都可以将制备态与测量方向的相对空间位置关系确定下来. 接下来, 将利用这种确定的空间位置关系构造定义 1 所示的交换算子. 特别地, 将 M_0, M_1 平面设为 σ_x 平面和 σ_z 平面, 并将控制算子构造为

$$Z=M_0,\ \ X=\frac{M_1-\cos(\alpha_{t'0}+\alpha_{t'1})M_0}{\sin(\alpha_{t'0}+\alpha_{t'1})}, \tag{13}$$

它们是酉算子, 因为 $Z^2=X^2=I$. 此外由于 X 是酉的, 还可得到 $M_0M_1+M_1M_0=2\cos(\alpha_{t'0}+\alpha_{t'1})I$, $\mathrm{tr}\,(ZX\rho)=0$.

结合状态 $|\psi_x\rangle$ (其中 $x=t,t'$) 与相关测量位于同一平面的事实, 可以得到

$$\begin{aligned}
&\mathrm{tr}_{\mathrm{Main}}\left(\Phi\,|\psi_x\rangle\,\langle\psi_x|\left(\,|0\rangle\,\langle 0|\,\right)_{\mathrm{ancilla}}\right)\\
=&\left[\frac{1+\boldsymbol{r}_x\cdot\boldsymbol{b}_0}{2}\,|0\rangle\langle 0|_{\mathrm{ancilla}}\right.\\
&+\frac{\boldsymbol{r}_x\cdot\boldsymbol{b}_1-\cos(\alpha_{t'0}+\alpha_{t'1})\boldsymbol{r}_x\cdot\boldsymbol{b}_0}{2\sin(\alpha_{t'0}+\alpha_{t'1})}\,|0\rangle\langle 1|_{\mathrm{ancilla}}\\
&+\frac{\boldsymbol{r}_x\cdot\boldsymbol{b}_1-\cos(\alpha_{t'0}+\alpha_{t'1})\boldsymbol{r}_x\cdot\boldsymbol{b}_0}{2\sin(\alpha_{t'0}+\alpha_{t'1})}\,|1\rangle\langle 0|_{\mathrm{ancilla}}\\
&\left.+\frac{1-\boldsymbol{r}_x\cdot\boldsymbol{b}_0}{2}\,|1\rangle\langle 1|_{\mathrm{ancilla}}\right]\\
=&\left(\frac{I}{2}+\frac{\boldsymbol{r}_x\cdot\boldsymbol{b}_0}{2}\sigma_z\right.\\
&\left.+\frac{\boldsymbol{r}_x\cdot\boldsymbol{b}_1-\cos(\alpha_{t'0}+\alpha_{t'1})\boldsymbol{r}_x\cdot\boldsymbol{b}_0}{2\sin(\alpha_{t'0}+\alpha_{t'1})}\sigma_x\right).
\end{aligned}\tag{14}$$

代入 $\boldsymbol{r}_x\boldsymbol{b}_0$, $\boldsymbol{r}_x\boldsymbol{b}_1$ 的观测值, 可得到 $|\psi_x\rangle$ 被自测试出的酉等价形式. 同理将测量引入, 即 Φ 作用在 $M_y\,|\psi_x\rangle$ 上, 经计算推导可得 $M_y\,|\psi_x\rangle$ 的酉等价形式.

3.2 鲁棒性分析

以上完成了在理想情形下自测试标准的给出及证明. 考虑到在实际实验中由于实验噪声、探测效率及统计误差的存在, 设备的输入输出之间的统计关联值常常达不到理想的值. 因此, 讨论自测试标准在出现误差时的表现非常重要. 假设观测值与理想值存在 ε 的误差:

$$\left|\langle\psi_x|\,M_y\,|\psi_t\rangle-E_{xy}^{\mathrm{ideal}}\right|\leqslant\varepsilon. \tag{15}$$

这将使我们能够量化制备态 $\{|\psi_x\rangle\}_x$ 和测量 $\{M_y=\alpha_y\cdot\sigma\}_y$ 相对于理想态 $\left|\psi_x^{\mathrm{target}}\right\rangle$ 和 M_y^{target} 的距离, 如 (15) 式所示. 在经过图 2 的局域同构运算之后, 量子态及测量系统将被交换到可信的辅助系统中, $\mathrm{tr}_{\mathrm{Main}}\left(\Phi\,|\psi_x\rangle\,\langle\psi_x|\left(\,|0\rangle\,\langle 0|\,\right)_{\mathrm{ancilla}}\right)$. 此时刻画交换到辅助系统中的部分及理想值之间的误差就好. 为方便起见, 将交换到辅助系统的部分表示为 ρ_{swap}, 然后可以用保真度来描述它与 $\left|\psi_x^{\mathrm{target}}\right\rangle$ 的接近程度:

$$F=\left\langle\psi_x^{\mathrm{target}}\right|\rho_{\mathrm{swap}}\left|\psi_x^{\mathrm{target}}\right\rangle. \tag{16}$$

对于给定的任意一组制备的量子态集合, 定义其与所期望的理想量子态集合间的平均保真度为

$$\overline{F}=\frac{1}{|x\cdot y|}\left(\sum_x F_x+\sum_y\overline{F}_y\right), \tag{17}$$

其中 $\overline{F}_y$ 是关于测量操作的平均保真度. 现在需要做的就是找到 F 的下限. 也就是需要求解优化问题:

$$\begin{aligned}
&\overline{F}=\frac{1}{|x\cdot y|}\left(\sum_x F_x+\sum_y\overline{F}_y\right),\\
&\text{s.t.}\ \ p(b|x,y)=\mathrm{tr}\left(\rho M_y^b\right),\ \Gamma(\rho,M_y)\geqslant 0,
\end{aligned}\tag{18}$$

其中, $\Gamma(\rho,M_y)$ 是关于 ρ,M_y 的约束条件. 由于经典统计到量子统计是一对多的, 通常需要遍历 2 维空间上的所有能给出观测值 $p\,(b|\,x,y)$ 的量子态和测量 ρ,M_y 来实现. 在知道了如何将图 2 中酉操作的控制算子与实际算子 B_y 联系起来后, F 中的一些项则可以由观测到的相关关系 (13) 式给出. F 中不确定的项与潜在的所有可能取得 (15) 式观测值的量子系统 $\{\rho,M_y\}$ 兼容. 这个优化问题可以借助于一个半定层析方法 $\Gamma_{s,s'}$ 来实现[31−34]. 该方法最早由 Navascués 等[31,32] 提出, 所以被称为 NPA (Navascués-Pironio-Acín, NPA) 方法. 由于这里涉及维度, 所以利用改进的与维度相关的 NPA 方法[33,34] 来求优化问题 (18) 式. 此外需要注意的是, NPA 方法通常应用于纠缠测量场景. 对于准备测量的场景, 可以通过借助纠缠态[35,36], 将 Alice 一方的制备态看成是 Alice-Bob 事先共享纠缠, 分别进行局域测量得到. 所以可以重新将制备测量情形表述为纠缠测量-测量场景.

在存在误差时, 已知 (13) 式中的 X 定义并不能保证是酉的. 此时在利用半正定层析方法时并不能直接用 (13) 式所定义的 X 算子作为图 2 酉算子的构造. 因为只要 $\varepsilon>0$, (13) 式定义的 X 算子就不能保证是酉的. 而 $Z=M_0$ 始终保留着酉性, 可以通过用适当的旋转重新定义目标状态, $\psi_x\to\psi_x=R_y\left(-\mathrm{i}\alpha_{00}Y/2\right)\psi_x$, 其中 $R_y\left(-\mathrm{i}\alpha_{00}Y/2\right)\psi_x$ 是关于 Y 基的旋转算子. 此时就可以将 M_0 看作是 Z 算子. 对于 X 不是酉的情形, 引进“附加矩阵”的方法, 该方法由 Bancal 等[11] 给出. “附加矩阵”的思想是引入一个新的算子 M_2, 满足 $M_2^2=I$, 并简单地设置 $X=M_2$. 新算子的引入是为了给出一个与理想情况 (13) 式的定义没有太大差别的酉算子. 所以需要将新引入的算子与实际的算子联系起来. 可以用下面的方式进行约束, 使得 M_2 与 X_B 比较接近:

$$M_2[M_1-\cos(\alpha_{10}+\alpha_{11})]M_0\equiv M_2\widetilde{X_B}\geqslant 0. \tag{19}$$

在半正定层析过程中, 将会引入一个额外的一个矩阵约束块 $\Gamma\left(M_2\widetilde{X_B}\right)_{j,j'}$, 其为厄米的和半正定来的, 来制约关系 (19) 式得以满足.

3.2.1 自测试标准的鲁棒性下界

上文已经给出了鲁棒性分析所有需要的工具, 下面以具体的统计观测值作为例子利用上述工具给出自测试的鲁棒性. 为简单起见, 将重点放在一个单参数族的情形, 即

$$\begin{aligned}
&\boldsymbol{r}_{00}\cdot\boldsymbol{b}_0=\boldsymbol{r}_{00}\cdot\boldsymbol{b}_1=\cos(\theta);\\
&\boldsymbol{r}_{01}\cdot\boldsymbol{b}_0=\boldsymbol{r}_{10}\cdot\boldsymbol{b}_1=\sin(\theta);\\
&\boldsymbol{r}_{10}\cdot\boldsymbol{b}_0=\boldsymbol{r}_{01}\cdot\boldsymbol{b}_1=-\sin(\theta);\\
&\boldsymbol{r}_{11}\cdot\boldsymbol{b}_0=\boldsymbol{r}_{11}\cdot\boldsymbol{b}_1=-\cos(\theta).
\end{aligned}\tag{20}$$

根据定理 1, 这种概率统计值可以实现其背后量子系统的自测试, 而且可以自测试出其背后的量子系统为

$$\begin{aligned}
\rho=\{&\cos(\theta)\sigma_z+\sin(\theta)\sigma_x,\sin(\theta)\sigma_z-\cos(\theta)\sigma_x,\\
&-\sin(\theta)\sigma_z+\cos(\theta)\sigma_x,-\cos(\theta)\sigma_z-\sin(\theta)\sigma_x\},
\end{aligned}\tag{21}$$

相关测量为

$$M=\{\sigma_z,\cos(2\theta)\sigma_z+\sin(2\theta)\sigma_x\}. \tag{22}$$

运行 NPA 半正定优化, 利用到算法的第 2 层, 即算法中包含所有 $\{M_y,M_yM_{y'}\}$ 引入的条件. 为了使得代码简化, 在半正定矩阵的构造中只考虑到保真度表达中出现的三层操作形式 $M_0M_{1/2}M_0$. 此外, 使用最简单的非平凡形式的附加矩阵, 即 4×4 矩阵 $\boldsymbol{\Gamma}\left(M_2\widetilde{X_{\mathrm{B}}}\right)_{j,j'}=\langle\mathcal{B}_j\left(M_2\widetilde{X_{\mathrm{B}}}\right)\mathcal{B}_{j'}\rangle$, 其中 $\mathcal{B}=(\mathrm{I},M_0,M_1,M_2)$. 采用 MATLAB 包来实现本文提出的优化问题, 利用到 YALIMP[37] 软件包和求解器 SEDUMI [38]. 运行结果如图 4 所示. 需要注意, 这些曲线虽然是有效的下限, 但不能保证是紧的. 曲线不紧的原因源于两个方面: 一是在半正定层次方面, 应用了有限层, 这可能会导致结果不紧; 二是附加矩阵的方法可能会增大紧致度的不足. 从比较结果看, $\alpha_{01}=\pi/4$ 所对应的自测试标准鲁棒性更强. 这时的自测试标准恰好为文献 [19] 中给出的标准. 虽然结果显示这个标准的鲁棒性更强, 但是其只能自测试出 BB84 粒子, 不能实现其他类型制备态集合的自测试. 而不同的制备态集合可能对应不同的实际应用, 在实际中更多制备态集合的自测试对应更多量子信息处理任务的实现, 因此对不同制备态的自测试有实际意义. 而本文中定理 1 给出了更多制备态的自测试, 如 $\alpha_{01}=2\pi/3,7\pi/12,\pi/2$ 所对应的态集合, 并且从运行结果看其鲁棒性并没有比文献 [19] 中给出的低很多. 注意文献 [19] 中的鲁棒性分析利用的是构造提取信道的解析方法, 该种方法依赖于不等式的构造具有局限性, 这里用 NPA 数值方法虽然给出的界不是最优的, 但应用范围更广泛.

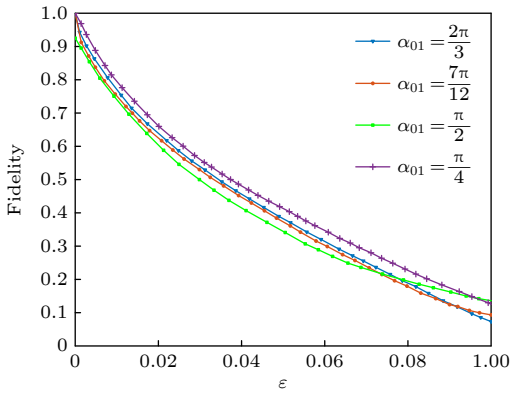

图 4 单态保真度 F 的下限. 在相关性误差为 ε 时, 4 种自测试标准的鲁棒性 ($\theta=\pi/2,\alpha_{00}=\pi/4,\alpha_{01}=\pi/4,2\pi/3,7\pi/12,\pi/2$)

Fig. 4. Lower bound for the certifiable singlet fidelity F as a function of the imperfection of the observed correlations ε. We plot the bounds for four-setting criteria ($\theta=\pi/2,\alpha_{00}=\pi/4,\alpha_{01}=\pi/4,2\pi/3,7\pi/12,\pi/2$).

4 总 结

制备测量情形是一种应用广泛的量子非纠缠系统, 在各种量子信息处理任务中有非常重要的应用, 如量子随机性认证, 量子密钥分发等. 本文研究了制备测量情形下的量子比特系统的自测试问题, 即非纠缠单量子比特态和测量操作的自测试. 在此之前, 文献 [19] 基于目击违背不等式, 给出了同时对设备中的量子比特态和测量 $\{\rho_x, M_y\}$ 集合进行自测试的标准. 然而其研究指出只有不等式达到量子系统最大违背值时其系统才能实现自测试, 任意偏离不等式的统计关联, 都无法实现所制备的量子态和测量的自测试. 这导致了他们的研究只能实现 BB84 粒子的自测试. 本文的研究主要是给出制备测量量子系统实现其自测试的新标准. 本工作直接关注全观测统计而非单一的不等式, 给出了观测统计量在满足什么条件时, 可实现制备态和测量设备的自测试. 文献 [19] 中给出的测试标准只对应于本方案中的一个点. 因此, 研究增加了量子比特态及测量集系统自测试标准的多样性, 有利于实际不同非纠缠系统的自测试. 此外, 考虑到在实际实验中由于实验噪声、探测效率及统计误差的存在, 设备的输入输出之间的统计关联值常常达不到理想的值, 进一步给出了所提出自测试方案的鲁棒性分析, 使得新给出的方案有实际应用意义.

参考文献

[1] Acín A, Brunner N, Gisin N, Massar S, Pironio S, Scarani V 2007 *Phys. Rev. Lett.* **98** 230501
[2] Mayers D, Yao A 2004 *Quant. Inf. Comput.* **4** 273
[3] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[4] Bell J S 1964 *Physics Physique Fizika* **1** 195
[5] Brunner N, Cavalcanti D, Pironio S, Scarani V, Wehner S 2014 *Rev. Mod. Phys.* **86** 419
[6] Pironio S, Acín A, Massar S, de La Giroday A B, Matsukevich D N, Maunz P, Olmschenk S, Hayes D, Luo L, Manning T A, Monroe C 2010 *Nature* **464** 1021
[7] Liu Y, Zhao Q, Li M H, Guan J Y, Zhang Y, Bai B, Zhang W, Liu W Z, Wu C, Yuan X, Li H, Munro W J, Wang Z, You L, Zhang J, Ma X, Fan J, Zhang Q, Pan J W 2018 *Nature* **562** 548
[8] Aharon N, Massar S, Pironio S, Silman J 2016 *New J. Phys.* **18** 025014
[9] Maitra A, Paul G, Roy S 2017 *Phys. Rev. A* **95** 042344
[10] Gheorghiu A, Kashefi E, Wallden P 2015 *New J. Phys.* **17** 083040
[11] Bancal J D, Navascués M, Scarani V, Vértesi T, Yang T H, 2015 *Phys. Rev. A* **91** 022115
[12] Wang Y K, Wu X Y, Scarani V 2016 *New J. Phys.* **18** 025021
[13] Pál K F, Vértesi T, Navascués M 2014 *Phys. Rev. A* **90** 042340
[14] Baccari F, Augusiak R, Šupić I, Tura J, Acín A 2020 *Phys. Rev. Lett.* **124** 020402
[15] Šupić I, Bowles J 2020 *Quantum* **4** 337
[16] Li X H, Wang Y K, Han Y G, Qin S J, Gao F and Wen Q Y 2020 *IEEE J. Sel. Areas Commun.* **38** 589
[17] Coladangelo A, Goh K T, Scarani V 2017 *Nat. Commun.* **8** 15485
[18] Šupić I, Hoban M J 2016 *New J. Phys.* **18** 075006
[19] Tavakoli A, Kaniewski J, Vértesi T, Rosset D, Brunner N 2018 *Phys. Rev. A* **98** 062307
[20] Ambainis A, Leung D, Mancinska L, Ozols M 2008 arXiv: 0810.2937
[21] Hayashi M, Iwama K, Nishimura H, Raymond R, Yamashita S 2006 *New J. Phys.* **8** 129
[22] Pawłowski M, Brunner N 2011 *Phys. Rev. A* **84** 010302(R)
[23] Li H W, Pawłowski M, Yin Z Q, Guo G C, Han Z F 2012 *Phys. Rev. A* **85** 052308
[24] Masanes L 2003 arXiv: quant-ph/0309137 [quant-ph]
[25] Masanes L 2005 arXiv: quant-ph/0512100 [quant-ph]
[26] McKague M, Yang T H, Scarani V 2012 *J. Phys. A Math. Theor.* **45** 455304
[27] Yang T H, Vértesi T, Bancal J D, Scarani V, Navascués M 2014 *Phys. Rev. Lett.* **113** 040401
[28] Scarani V 2012 *Acta Phys. Slovaca.* **62** 347
[29] Wu X Y, Cai Y, Yang T H, Le H N, Bancal J D, and Scarani V 2014 *Phys. Rev. A* **90** 042339
[30] Clauser J F, Horne M A, Shimony A, Holt R A 1969 *Phys. Rev. Lett.* **23** 880
[31] Navascués M, Pironio S, Acín A 2007 *Phys. Rev. Lett.* **98** 010401
[32] Navascués M, Pironio S, Acín A 2008 *New J. Phys.* **10** 073013
[33] Navascués M, de la Torre G, Vértesi T 2014 *Phys. Rev. X* **4** 011011
[34] Navascués M, Vértesi T 2015 *Phys. Rev. Lett.* **115** 020501
[35] Li H W, Mironowicz P, Pawłowski M, Yin Z Q, Wu Y C, Wang S, Chen W, Hu H G, Guo G C, Han Z F 2013 *Phys. Rev. A* **87** 020302(R)
[36] Mironowicz P, Li H W, Pawłowski M 2014 *Phys. Rev. A* **90** 022322
[37] Lofberg J *YALMIP: A Toolbox for Modeling and Optimization in MATLAB, Proceedings of the CACSD Conference* Taipei, China, September 24, 2004
[38] Sturm J F 1999 *Optim. Methods Softw.* **11** 625

Self-testing criteria for preparing-measuring qubit system*

Wang Yu-Kun [1)2)†] Li Ze-Yang [1)] Xu Kang [1)] Wang Zi-Zheng [1)]

1) (*Beijing Key Laboratory of Petroleum Data Mining, China University of Petroleum, Beijing* 102249, *China*)

2) (*State Key Laboratory of Cryptology, Beijing* 100036, *China*)

(Received 24 December 2022; revised manuscript received 28 February 2023)

Abstract

Self-testing is the high-level security verification of a claimed quantum device, confirming the quantum states prepared in the device and the measurements performed based solely on the observed statistics. The statistical correlations can realize the self-testing of the quantum system in the preparing-and-measuring scenario. However, most of previous studies focused on the self-testing of shared entangled states between devices, at present only a few researches are presented and the existing work can only simultaneously self-test the states and measurements when some witness inequalities reach a maximum violation. We focus on four-state preparation and the selected scenarios of two measurements. In this scenario, Armin Tavakoli et al. [Tavakoli A, Kaniewski J, Vértesi T, Rosset D, Brunner N 2018 *Phys. Rev. A* **98** 062307] have put forward a criterion based on the dimensional witness violation inequality which can achieve BB84 particles and corresponding Pauli measurements. However, in addition to the maximum violation of the inequality, any statistics with deviation from the maximum deviation cannot be self-tested. Besides, only the BB84 particle preparation and measurements system can be self-tested with that criterion, resulting in a large number of four-state preparation and two measurement systems that cannot be self-tested. Therefore, in this work, in addition to the maximum violation of that dimension inequality, we directly focus on the full observed statistics and further propose some new criteria for self-testing qubit quantum systems in the preparing-and-measiuring scenarios. And the self-testing criteria are proven in an ideal case. We construct a local isometry by using the constructions commonly used in device-independent cases, exchange the target system with the additional system, and realize the self-testing of more qubit state sets and measurement sets than BB84 particles. This meets the requirements for practical experiments to realize various tasks by different quantum state sets. In addition, we perform a robust analysis of the proposed criteria and use fidelity to describe the closeness of the state to the ideal state of the auxiliary system. Finally, an improved dimensional-dependent NPA method is used to optimize the lower bound of the robustness, making the new criteria practical under experimental noise. We use the YALIMP software package in MATLAB and the solver SEDUMI to solve this optimization problem. The present research increases the diversity of qubit state preparations and self-testing of measurement system, which is beneficial to the actual self-testing of different non-entangled single quantum systems.

Keywords: self testing, prepare-and-measurement, witness inequality, robustness

PACS: 03.65.Ud, 03.67.–a **DOI:** 10.7498/aps.72.20222431

* Project supported by the National Nature Science Foundation of China (Grant No. 62101600), the Science Foundation of China University of Petroleum, Beijing, China (Grant No. 2462021YJRC008), and the State Key Laboratory of Cryptology, China (Grant No. MMKFKT202109).

† Corresponding author. E-mail: wykun06@gmail.com