



中华人民共和国国家标准化指导性技术文件

GB/Z XXXXX—XXXX

器件无关量子随机数发生器检测规程

Code of practice for testing of device-independent quantum random number
generators

（征求意见稿）

本草案完成时间：2026.7.8

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX - XX - XX 发布

国家市场监督管理总局 发布
国家标准化管理委员会

目 次

前言 II

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 符号和缩略语 2

5 总体要求 2

6 性能表征参数 3

7 测试方法 4

8 检测报告 8

附录 A（资料性） 基于极大似然估计的量子态层析方法 9

附录 B（资料性） 非信令条件检验数据分析方法 11

附录 C（资料性） 检测记录模板 15

前 言

本文件为规范类指导性技术文件。

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国量子技术标准化技术委员会（SAC/TC 578）归口。

本文件起草单位：合肥国家实验室、济南量子技术研究院、中国科学技术大学、国科量子通信网络有限公司、中移量子科技有限公司、科大国盾量子技术股份有限公司、中国计量科学研究院、中国科学院软件研究所、香港大学、宁波大学、武汉量子技术研究院、中电长城科技有限公司、中国信息通信研究院、中电信量子信息科技集团有限公司、中国信息安全测评中心、中国标准化研究院、中国人民解放军网络空间部队信息工程大学、中科酷原科技（武汉）有限公司、山东省体育彩票管理中心。

本文件主要起草人：江扬帆、陈肖含、张强、程苏艺、聂友奇、张军、吴佳颖、李明翰、魏瑛、李东东、邓玉强、陈华、张行健、王超凡、陈超、韩玄、李阳、郑明睿、姜艳、赖俊森、于春霖、安雪碧、刘宏伟、康健、侯一凡、石志全、许修竹。

器件无关量子随机数发生器检测规程

1 范围

本文件确立了基于光学偏振系统的器件无关量子随机数发生器检测的总体要求，明确了性能表征参数，描述了相关测试方法。

本文件适用于基于光学偏振系统的器件无关量子随机数发生器的检测。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 32915-2026 信息安全技术 二元序列随机性检测方法

GB/T 43692-2024 量子通信术语和定义

GB/T 45240-2025 器件无关量子随机数发生器通用要求

3 术语和定义

GB/T 45240-2025界定的以及下列术语和定义适用于本文件。

3.1

纠缠光源 entanglement photon source

所产生的光子间存在量子纠缠的光子源。

[来源：GB/T45240—2025，3.4，有修改]

3.2

纠缠光子对 entanglement photon pair

由纠缠光源(3.1)产生的一对存在量子纠缠的光子。

3.3

随机性估计 randomness estimation

对熵源的随机性（或称熵）进行量化评估的过程。

3.4

探测效率 detection efficiency

探测器成功探测到入射光子的概率。

3.5

符合计数 coincidence count

在多通道信号处理系统中，多个通道中的信号在指定的时间窗口内同时发生的计数结果。

3.6

平均光子数 mean photon number

每个光脉冲信号含有的光子数量的平均值。

[来源：GB/T43692—2024，3.35]

4 符号和缩略语

下列符号和缩略语适用于本文件。

|H>: 水平偏振态

|V>: 垂直偏振态

|D>: 偏振态 $\frac{1}{\sqrt{2}}(|H\rangle+|V\rangle)$

|A>: 偏振态 $\frac{1}{\sqrt{2}}(|H\rangle-|V\rangle)$

|R>: 偏振态 $\frac{1}{\sqrt{2}}(|H\rangle+i|V\rangle)$

|L>: 偏振态 $\frac{1}{\sqrt{2}}(|H\rangle-i|V\rangle)$

ω : 贝尔检验中获胜的概率

S: 贝尔检验中贝尔不等式的破坏值

HWP: 半波片 (Half-Wave Plate)

PBS: 偏振分束器 (Polarizing Beam Splitter)

QWP: 四分之一波片 (Quarter-Wave Plate)

TDC: 时间数字转换器 (Time to Digital Converter)

5 总体要求

5.1 基本职责

5.1.1 送检机构

提供完整的设备档案与相关资料,包括设备的安装、初始化及使用说明,并确保所提供的资料真实可靠。

5.1.2 检测机构

对送检机构提交的档案、资料实行严格保密管理,切实保障送检机构权益。

5.2 检测环境

5.2.1 环境要求

检测环境应根据被测设备标称的使用条件要求进行搭建。除被测设备另有规定外,检测环境应满足下列条件:

- a) 环境温度: 20 °C ~30 °C;
- b) 相对湿度: 20 %~70 %。

5.2.2 可测试性要求

器件无关量子随机数发生器应具备可测试性,具体包括:

- a) 在送检阶段,应提供物理测试接口,支持按照 GB/T 45240—2025 中图 1 对纠缠光源、测量基模块、探测器的独立测试;在非送检阶段,应关闭探测器的测试接口。
- b) 在送检阶段,应提供软件测试接口,支持贝尔检验模块和数据后处理模块的独立测试;在非送检阶段,应关闭软件测试接口。

5.3 测量设备

5.3.1 激光器

激光器参数要求如下：

- a) 输出功率：大于-20 dBm 且小于 20 dBm；
- b) 输出功率不稳定性：10 min 内小于 5%；
- c) 波长范围：覆盖纠缠光子对波长。

5.3.2 光功率计

光功率计参数要求如下：

- a) 可测功率范围：-50 dBm~20 dBm；
- b) 测量不确定度：小于 5%；
- c) 波长范围：覆盖纠缠光子对波长。

5.3.3 光谱仪

光谱仪参数要求如下：

- a) 波长分辨率：不低于 0.1 nm；
- b) 波长范围：覆盖纠缠光子对波长。

5.3.4 时间数字转换器

TDC参数要求如下：

- a) 单通道计数率：覆盖被检设备纠缠态制备速率和选基随机序列模块输出速率；
- b) 时间分辨率：不高于 1 ns。

6 性能表征参数

根据器件无关量子随机数发生器的工作原理，性能表征参数宜包括表1所列检测项目。

注：器件无关量子随机数发生器的工作原理参见GB/T 45240-2025。

表1 检测项目表

序号	检测项目	测试方法对 应章节号	定义	性能要求
1	纠缠光源纠缠态制备速率	7.2	单位时间内纠缠光源生成纠缠光子对的数量	不低于 50 kbits/s 且满足被 测设备标称值
2	纠缠光源量子态保真度	7.3	见 GB/T 45240—2025 6.1.1	不低于 90%且满足被测设 备标称值
3	测量基模块测量效率	7.4	光子入射到测量基模块，至输 出测量基模块的概率	不低于 90%且满足被测设 备标称值
4	纠缠光源总体探测效率	7.5	见 GB/T 45240—2025 6.2.2	大于 76%且满足被测设备 标称值
5	非信令条件检验	7.6	见 GB/T 45240—2025 6.2.3	通过非信令条件检验
6	贝尔检验	7.7	见 GB/T 45240—2025 6.2.4	ω 大于 0.7501 或 S 大于 0.0002，且满足被测设备 标称值

7	器件无关量子随机数产率	7.8	单位时间内系统生成的最终随机数的数量	不低于被测设备标称值
8	器件无关量子随机数随机性统计检测	7.9	对系统生成的最终随机数的随机性检测	样本通过率不低于 98%

7 测试方法

7.1 测试前准备

在器件无关量子随机数发生器系统测试前，应对其基本信息进行确认，包括但不限于：

- a) 纠缠光源的基本信息；
- b) 各组件的功能和指标参数；
- c) 随机性估计方法；
- d) 随机数提取方法；
- e) 选基随机序列模块输出电信号的电气特性及功能正常性；
- f) 探测模块输出电信号的电气特性及功能正常性；
- g) 纠缠光源偏振态可调范围；
- h) 测量基模块偏振态可调范围；
- i) 测量结果的可读性；
- j) 贝尔检测模块源代码可查；
- k) 数据后处理模块源代码可查；
- l) 确认检测环境满足 5.2.1。

7.2 纠缠光源纠缠态制备速率

7.2.1 操作步骤

纠缠光源纠缠态制备速率应按如下步骤进行：

- a) 按图 1 所示，开启泵浦光源，将泵浦光功率设置至标称工作点并稳定不少于 5 min；
- b) 使用 TDC 记录探测器 A 和探测器 B 的输出计数 N_A 、 N_B 及符合计数 N_{AB} ，调节纠缠光源端的波片及测量基模块的波片，使符合计数 N_{AB} 最大，设置 TDC 统计时长 t 不少于 60 s；
- c) 根据公式（1）计算纠缠态制备速率 N ：

$$N=(N_A N_B)/(N_{AB} t) \cdots \cdots \cdots (1)$$

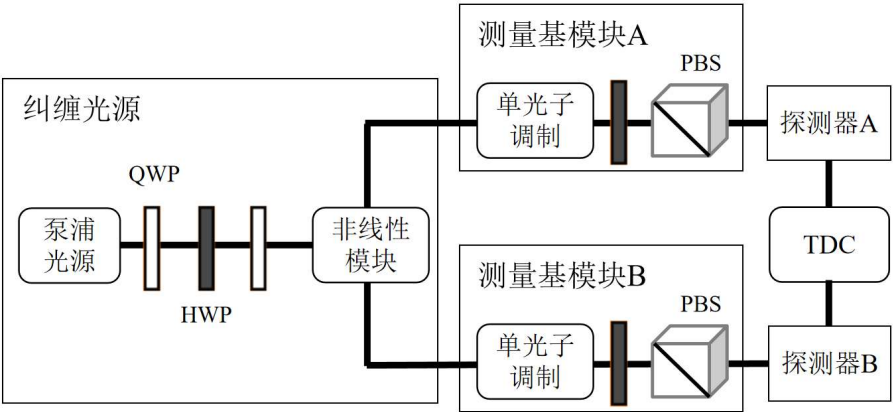


图1 器件无关量子随机数发生器示意图

注：非线性模块包含非线性晶体和生成纠缠光子对的光路结构。所有波片可调。

7.2.2 判定依据

纠缠态制备速率宜不低于50 kbits/s且满足被测设备标称值。

7.3 纠缠光源量子态保真度

7.3.1 操作步骤

纠缠光源量子态保真度应按如下步骤进行：

- 如图 2 所示，开启泵浦光源，通过调节纠缠光源中的波片组合制备被测设备标称目标非最大纠缠态 $|\psi\rangle$ ；
- 分别设置测量基模块 A 和测量基模块 B 的波片，进行量子态测量，使其分别进行 $|H\rangle$ 、 $|V\rangle$ 、 $|D\rangle$ 、 $|A\rangle$ 、 $|R\rangle$ 、 $|L\rangle$ 投影测量，TDC 记录每一组测量设置下的探测器 A 和探测器 B 的符合计数，共 36 组计数结果；
- 对符合计数进行归一化处理，将其转化为概率分布；
- 进行量子态层析，重构系统纠缠态的密度矩阵 ρ_1 ，量子态层析方法可参见附录 A。
- 按公式（2）计算纠缠光源量子态保真度：

$$F(\rho_1, \rho_2) = \left(\text{Tr} \left\{ \sqrt{\sqrt{\rho_2} \rho_1 \sqrt{\rho_2}} \right\} \right)^2 \dots\dots\dots (2)$$

式中：

ρ_1 ——量子态层析重构的实际纠缠态的密度矩阵；

ρ_2 ——被测设备标称目标非最大纠缠态 $|\psi\rangle$ 的密度矩阵。

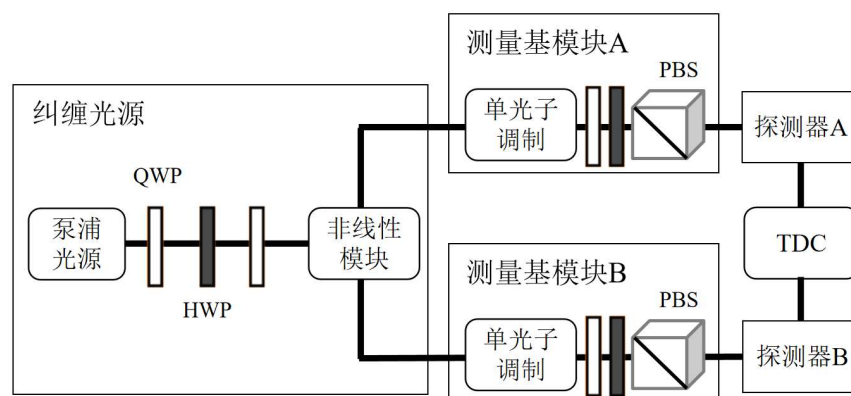


图2 纠缠光源量子态保真度检测示意图

注：非线性模块包含非线性晶体和生成纠缠光子对的结构。

7.3.2 判定依据

量子态保真度应不低于90%且满足被测设备标称值。

7.4 测量基模块测量效率

7.4.1 操作步骤

测量基模块测量效率应按如下步骤进行：

- 开启激光器并稳定不少于 10 min，使用光谱仪测量激光器中心波长，并调节至与纠缠光子波长的差异不超过 1 nm；
- 阻隔测量基模块至探测器模块光路，将激光器出射的激光起偏为 $|H\rangle$ ，注入测量基模块，将功率计置于测量基模块输入端口处，待读数稳定后连续测量入射光功率不少于 5 次，每次采样时间不少于 1 s，取算术平均值，记为 P_1 ；
- 在 PBS 之前的偏振态制备单元处，调节波片，使注入激光的偏振态对准至 PBS 透射轴；
- 保持激光器输出功率与偏振态不变，将功率计移至 PBS 透射端口之后，待读数稳定后连续测量透射光功率不少于 5 次，每次采样时间不少于 1 s，取算术平均值，记为 P_2 ；
- 测量基模块测量效率按公式（3）计算：

$$\eta_M = P_2/P_1 \dots\dots\dots (3)$$

7.4.2 判定依据

测量基模块测量效率应不低于90%且满足被测设备标称值。

7.5 纠缠光源总体探测效率

7.5.1 操作步骤

纠缠光源总体探测效率应按如下步骤进行：

- 如图 1 所示，开启泵浦光源，设置泵浦光功率，使生成的纠缠态的平均光子数不高于 0.02；
- 通过调节纠缠光源中的波片组合，将泵浦光的偏振态设置为 $|H\rangle$ ，使用 TDC 记录探测器 A 和探测器 B 的输出计数 $N_{A|H}$ 、 $N_{B|H}$ 及符合计数 $N_{AB|H}$ ，调节测量基模块的波片，使符合计数 $N_{AB|H}$ 最大，设置 TDC 统计时长 t 不少于 60 s；
- 通过调节纠缠光源中的波片组合，将泵浦光的偏振态设置为 $|V\rangle$ ，使用 TDC 记录探测器 A 和探测器 B 的输出计数 $N_{A|V}$ 、 $N_{B|V}$ 及符合计数 $N_{AB|V}$ ，调节测量基模块的波片，使符合计数 $N_{AB|V}$ 最大，设置 TDC 统计时长 t 不少于 60 s；
- 记 A 这一侧光路的纠缠光源总体探测效率为 η_A ，记 B 这一侧光路的纠缠光源总体探测效率为 η_B ，按公式（4）和公式（5）计算：

$$\eta_A = \frac{1}{2} (N_{AB|H}/N_{B|H} + N_{AB|V}/N_{B|V}) \dots\dots\dots (4)$$

$$\eta_B = \frac{1}{2} (N_{AB|H}/N_{A|H} + N_{AB|V}/N_{A|V}) \dots\dots\dots (5)$$

- 将 η_A 和 η_B 取平均，得到最终的纠缠光源总体探测效率。

注：可多次测量 η_A 和 η_B 计算平均值和均方差。

7.5.2 判定依据

纠缠光源总体探测效率应大于76%且满足被测设备标称值。

7.6 非信令条件检验

7.6.1 操作步骤

按GB/T 45240-2025的6.2.3执行。非信令条件检验数据分析方法可参见附录B实现。

7.6.2 判定依据

$D_{KL}(f||p_{NS}) \leq 10^{-6}$ 或 $p_n = 1$ ，则通过非信令条件检验。

7.7 贝尔检验

7.7.1 操作步骤

贝尔检验应按如下步骤进行：

- 如图 1 所示，开启泵浦光源，通过调节纠缠光源中的波片组合制备被测设备标称目标非最大纠缠态 $|\psi\rangle$ ；
- 设置贝尔检验轮数大于 1×10^8 ，如 GB/T 45240-2025 图 1 所示，开启选基随机序列 X 和 Y，使用 TDC 记录 X、Y、A、B。
- 使用 TDC 记录结果计算贝尔不等式：
- 根据表 2 进行数据统计和处理，按公式（6）计算贝尔检验结果；或根据表 3 进行数据统计和处理，按公式（7）计算贝尔检验结果：

$$\omega = (n1+n2+n3+n4)/4 \dots\dots\dots (6)$$

$$S = p1-p2-p3-p4 \dots\dots\dots (7)$$

注： ω 与 S 的转换关系为 $\omega = S/2 + 3/4$

表2 贝尔检验数据统计

符合计数		ab				
		00	01	10	11	
xy	00	a1	b1	c1	d1	$n1=(a1+d1)/(a1+b1+c1+d1)$
	01	a2	b2	c2	d2	$n2=(a2+d2)/(a2+b2+c2+d2)$
	10	a3	b3	c3	d3	$n3=(a3+d3)/(a3+b3+c3+d3)$
	11	a4	b4	c4	d4	$n4=(b4+c4)/(a4+b4+c4+d4)$

表3 贝尔检验数据统计

符合计数		ab				
		00	01	10	11	
xy	00	a1	b1	c1	d1	$p1=a1/(a1+b1+c1+d1)$
	01	a2	b2	c2	d2	$p2=b2/(a1+b1+c1+d1)$
	10	a3	b3	c3	d3	$p3=c3/(a1+b1+c1+d1)$
	11	a4	b4	c4	d4	$p4=a4/(a1+b1+c1+d1)$

7.7.2 判定依据

ω 大于0.7501或 S 大于0.0002，且满足被测设备标称值。

7.8 器件无关量子随机数产率

7.8.1 操作步骤

器件无关量子随机数产率应按如下步骤进行：

- a) 被测设备完成贝尔检验后，将被测设备设置为工作模式；
- b) 按 GB/T 45240-2025 6.3.2 对数据后处理模块进行检测；
- c) 按 GB/T 45240-2025 附录 C 进行器件无关量子随机数产率计算。

7.8.2 判定依据

器件无关量子随机数产率应不低于被测设备标称值。

7.9 器件无关量子随机数随机性统计检测

7.9.1 操作步骤

器件无关量子随机数随机性统计检测应按如下步骤进行：

- a) 采集器件无关量子随机数二元序列样本数量不少于 1000 个,每个样本长度不低于 20000 比特；
- b) 按照 GB/T 32915-2026 第 5 章描述的检测方法对每一个样本进行随机性检验。

7.9.2 判定依据

按GB/T 32915-2026 规定的检测项目逐项进行检测，每项检测的样本通过率应不低于98%。

8 检测报告

检测报告应至少包含以下内容：

- a) 被测设备信息；
- b) 检测机构；
- c) 送检机构；
- d) 报告编号；
- e) 外部环境条件；
- f) 重要设备性能参数；
- g) 各项检测结果；
- h) 负责人；
- i) 检测日期；

检测报告参见附录C。

附录 A

(资料性)

基于极大似然估计的量子态层析方法

A.1 适用范围与概述

本附录给出了利用偏振自由度对纠缠光源进行量子态层析的常规流程。当实验受系统漂移、统计涨落等误差影响，导致直接线性重构的密度矩阵不满足物理实在性（如出现负本征值）时，采用本附录规定的极大似然估计算法进行物理重构。

A.2 两比特偏振基矢与投影测量

单比特偏振状态空间的测量定义在布洛赫球的三个正交轴上。设Z轴基矢为水平偏振 $|H\rangle$ 和竖直偏振 $|V\rangle$ 。定义X, Y, Z三个测量方向的主本征态为 $|\psi_i\rangle$ ，其对应的正交态（对偶本征态）记为 $|\psi_i^\perp\rangle$ 。具体物理定义如表A.1所示。

表A.1 测量定义

测量方向	主本征态 $ \psi_i\rangle$	正交态 $ \psi_i^\perp\rangle$
X 轴 ($\hat{\sigma}_x$)	$ D\rangle = \frac{ H\rangle + V\rangle}{\sqrt{2}}$	$ A\rangle = \frac{ H\rangle - V\rangle}{\sqrt{2}}$
Y 轴 ($\hat{\sigma}_y$)	$ R\rangle = \frac{ H\rangle + i V\rangle}{\sqrt{2}}$	$ L\rangle = \frac{ H\rangle - i V\rangle}{\sqrt{2}}$
Z 轴 ($\hat{\sigma}_z$)	$ H\rangle$	$ V\rangle$

单比特系统量子态层析所需的投影状态集合为 $\Omega = \{|H\rangle, |V\rangle, |D\rangle, |R\rangle\}$ 。两比特系统的完整层析需要对两个粒子进行联合投影测量，实验共需执行 $4^2 = 16$ 种空间组合测量。定义实验测量的16种联合投影状态为 $|\Psi_\nu\rangle$ （其中 $\nu = 1, 2, \dots, 16$ ），其由两粒子的单比特状态张量积组成： $|\Psi_\nu\rangle = |\phi\rangle_1 \otimes |\chi\rangle_2$ ，其中 $|\phi\rangle, |\chi\rangle \in \{|H\rangle, |V\rangle, |D\rangle, |R\rangle\}$ 。具体16种实验配置对应的联合状态参见表A.2。

表A.2 两比特系统的联合投影

序号 ν	联合投影态 $ \psi_\nu\rangle$	序号 ν	联合投影态 $ \psi_\nu\rangle$
1	$ H\rangle_1 \otimes H\rangle_2$	9	$ D\rangle_1 \otimes H\rangle_2$
2	$ H\rangle_1 \otimes V\rangle_2$	10	$ D\rangle_1 \otimes V\rangle_2$
3	$ H\rangle_1 \otimes D\rangle_2$	11	$ D\rangle_1 \otimes V\rangle_2$
4	$ H\rangle_1 \otimes R\rangle_2$	12	$ D\rangle_1 \otimes R\rangle_2$
5	$ V\rangle_1 \otimes H\rangle_2$	13	$ R\rangle_1 \otimes H\rangle_2$
6	$ V\rangle_1 \otimes V\rangle_2$	14	$ R\rangle_1 \otimes V\rangle_2$
7	$ V\rangle_1 \otimes D\rangle_2$	15	$ R\rangle_1 \otimes D\rangle_2$
8	$ V\rangle_1 \otimes R\rangle_2$	16	$ R\rangle_1 \otimes R\rangle_2$

注：每个通道的基矢选择通过调整各自光路中的四分之一波片（QWP）和二分之一波片（HWP）的角度实现，最终通过偏振分束器（PBS）投影至探测器。

A.3 线性斯托克斯重构

两比特密度矩阵 $\hat{\rho}$ 可由两比特泡利算符张量积 $\hat{\sigma}_{i_1} \otimes \hat{\sigma}_{i_2}$ 线性展开，见公式（A.1）：

$$\hat{\rho} = \frac{1}{4} \sum_{i_1, i_2=0}^3 S_{i_1, i_2} \hat{\sigma}_{i_1} \otimes \hat{\sigma}_{i_2} \dots \dots \dots (A.1)$$

式中： $\hat{\sigma}_0 = \hat{I}$ ， $\hat{\sigma}_{1,2,3}$ 分别对应 $\hat{\sigma}_{x,y,z}$ 。

除 $S_{0,0} = 1$ 外，其余15个两比特斯托克斯参量 S_{i_1, i_2} 分别通过各个通道的归一化符合计数概率之差计算得出，见公式（A.2）：

$$S_{i_1, i_2} = (P_{|\psi_{i_1}\rangle} - P_{|\psi_{i_1}^\perp\rangle}) \cdot (P_{|\psi_{i_2}\rangle} - P_{|\psi_{i_2}^\perp\rangle}) \dots \dots \dots (A.2)$$

定义 $P_\nu \equiv P(|\Psi_\nu\rangle)$ 为第 ν 种投影测量的测量概率。直接利用上式重构得到的密度矩阵记为 $\hat{\rho}_{linear}$ 。若实验中存在系统漂移、统计涨落或波片轴向校准误差， $\hat{\rho}_{linear}$ 可能无法满足半正定性（即出现负的本征值），从而失去合法的物理意义。此时，必须以 $\hat{\rho}_{linear}$ 作为初值，转入A.4的极大似然估计寻优。

A.4 极大似然估计（MLE）非线性重构

为了确保在数值寻优过程中重构的密度矩阵严格满足厄米性、迹为1以及半正定性，引入Cholesky分解。按公式（A.3）定义一个 4×4 的下三角矩阵 $\hat{T}(t)$ ：

$$\hat{T}(t) = \begin{pmatrix} t_1 & 0 & 0 & 0 \\ t_5 + it_6 & t_2 & 0 & 0 \\ t_7 + it_8 & t_9 + it_{10} & t_3 & 0 \\ t_{11} + it_{12} & t_{13} + it_{14} & t_{15} + it_{16} & t_4 \end{pmatrix} \dots \dots \dots (A.3)$$

式中 $t = [t_1, t_2, \dots, t_{16}]^T$ 为包含16个独立实变量的参数向量（其中主对角线 $t_1 \sim t_4$ 为实数，其余为复数的实部与虚部）。则具有严格物理意义的候选密度矩阵参数化表示（A.4）：

$$\hat{\rho}_p(t) = \frac{\hat{T}^\dagger(t)\hat{T}(t)}{\text{Tr}\{\hat{T}^\dagger(t)\hat{T}(t)\}} \dots \dots \dots (A.4)$$

设在16个联合测量基矢下，实验实际测得的符合计数集合为 n_ν （ $\nu = 1, 2, \dots, 16$ ）。假定计数服从高斯分布，且各通道归一化系数 $\mathcal{N}$ （由 $n_\nu = \mathcal{N}P_\nu$ 定义）在各测量基下基本恒定。将归一化系数吸收至矩阵元中，令 $t' = \sqrt{\mathcal{N}}t$ ，则由参数矩阵导出的第 ν 个基矢的理论预测计数为（A.5）：

$$\bar{n}_\nu(t') = \langle \psi_\nu | \hat{\rho}_p(t') | \psi_\nu \rangle \dots \dots \dots (A.5)$$

根据误差分布，构建负对数似然函数作为数值优化的目标函数 $\mathcal{L}(t')$ ，见公式（A.6）：

$$\mathcal{L}(t') = \sum_{\nu=1}^{16} \frac{[\langle \psi_\nu | \hat{\rho}_p(t') | \psi_\nu \rangle - n_\nu]^2}{2\langle \psi_\nu | \hat{\rho}_p(t') | \psi_\nu \rangle} \dots \dots \dots (A.6)$$

利用A.3线性斯托克斯法求得的 $\hat{\rho}_{linear}$ ，通过数学逆运算解出对应的 t'_0 向量，作为非线性优化的初始搜索点，以避免寻优陷入局部极小值。采用非线性常规优化算法对 $\mathcal{L}(t')$ 进行全局极小化搜索。将寻优终止时获得的最优参数 t'_{opt} 代入参数矩阵，得到最终的2比特物理密度矩阵 $\hat{\rho}_{est}$ ，见公式（A.7）：

$$\hat{\rho}_{est} = \frac{\hat{T}^\dagger(t'_{opt})\hat{T}(t'_{opt})}{\text{Tr}\{\hat{T}^\dagger(t'_{opt})\hat{T}(t'_{opt})\}} \dots \dots \dots (A.7)$$

附录 B (资料性) 非信令条件检验数据分析方法

B.1 适用范围

本非信令条件检验数据分析方法基于python语言程序，通过约束优化求解最优非信令概率分布 $p_{NS}(ab|xy)$ ，并计算KL散度进行判定。

B.2 参考实现

```
import numpy as np
from scipy.optimize import minimize
from typing import Dict, Tuple

def nonsignaling_judgment(counts: np.ndarray) -> Dict:
    """
    非信令条件检验（GB/T 45240—2025 附录 A.2）

    输入:
        counts: 4×4 numpy数组，N(ab|xy)原始计数矩阵（非负整数）
            行: xy = [00, 01, 10, 11]
            列: ab = [00, 01, 10, 11]

    输出:
        字典，包含:
        - 'satisfies': bool, 最终判定结果
        - 'D_KL': float, KL散度值
        - 'p_xy': array, 选基概率
        - 'f': array, 观测条件概率
        - 'p_NS': array, 最优非信令条件概率
        - 'R': array, 比值矩阵
        - 'total_N': int, 总试验轮次
    """
    counts = np.array(counts, dtype=float)
    if counts.shape != (4, 4) or np.any(counts < 0):
        raise ValueError("输入必须为 4×4 非负计数矩阵")

    total_N = int(np.sum(counts))
    if total_N == 0:
        return {'satisfies': False, 'D_KL': np.inf, 'total_N': 0}

    # 1. 选基随机数概率分布 p_xy
    row_sums = np.sum(counts, axis=1)
```

```

p_xy = row_sums / total_N

# 2. 经验条件概率 f(ab|xy)
f = np.zeros((4, 4))
for i in range(4):
    if row_sums[i] > 0:
        f[i] = counts[i] / row_sums[i]

# 3. KL散度最小化目标函数
def objective(x):
    p = x.reshape((4, 4))
    p = np.maximum(p, 1e-12)
    p /= np.sum(p, axis=1, keepdims=True)
    kl = 0.0
    for i in range(4):
        if p_xy[i] > 1e-12:
            kl += p_xy[i] * np.sum(f[i] * np.log(np.maximum(f[i] / p[i], 1e-12)))
    return kl

# 4. 约束条件
constraints = []
# 每行归一化
for i in range(4):
    def norm(x, idx=i):
        p = x.reshape((4, 4))
        return np.sum(p[idx]) - 1.0
    constraints.append({'type': 'eq', 'fun': norm})

# Alice边际独立于y
def a_marginal_x0(x):
    p = x.reshape((4, 4))
    return (p[0,0] + p[0,1]) - (p[1,0] + p[1,1])
constraints.append({'type': 'eq', 'fun': a_marginal_x0})

def a_marginal_x1(x):
    p = x.reshape((4, 4))
    return (p[2,0] + p[2,1]) - (p[3,0] + p[3,1])
constraints.append({'type': 'eq', 'fun': a_marginal_x1})

# Bob边际独立于x
def b_marginal_y0(x):
    p = x.reshape((4, 4))
    return (p[0,0] + p[0,2]) - (p[2,0] + p[2,2])

```

```

constraints.append({'type': 'eq', 'fun': b_marginal_y0})

def b_marginal_y1(x):
    p = x.reshape((4, 4))
    return (p[1,0] + p[1,2]) - (p[3,0] + p[3,2])
constraints.append({'type': 'eq', 'fun': b_marginal_y1})

# 优化
x0 = np.full(16, 0.25)
bounds = [(0, None)] * 16
res = minimize(objective, x0, method='SLSQP', bounds=bounds,
               constraints=constraints, tol=1e-14, options={'maxiter': 2000})

if not res.success:
    return {'satisfies': False, 'D_KL': np.inf, 'total_N': total_N}

p_ns = res.x.reshape((4, 4))
p_ns = np.maximum(p_ns, 1e-12)
p_ns /= np.sum(p_ns, axis=1, keepdims=True)

# 5. KL散度
D_KL = res.fun

# 6. R矩阵
R = np.ones((4, 4))
mask = (f > 1e-12) & (p_ns > 1e-12)
R[mask] = f[mask] / p_ns[mask]

# 7. 判定
satisfies = D_KL < 1e-6

return {
    'satisfies': satisfies,
    'D_KL': float(D_KL),
    'total_N': total_N,
    'p_xy': p_xy.tolist(),
    'f': f.tolist(),
    'p_NS': p_ns.tolist(),
    'R': R.tolist()
}

```

B.3 使用说明

将4×4原始计数矩阵传入函数，返回字典中 ‘satisfies’ 为True时，满足非信令条件。

GB/Z XXXXX—XXXX

本实现为资料性参考，实际检测可采用等效的商用优化工具或MATLAB实现。

附 录 C
(资料性)
检测记录模板

检测记录模板见表C.1。

表C.1 检测记录模板

序号	项目	内容	
1	被测设备		
2	检测机构		
3	送检机构		
4	报告编号		
5	外部环境	温度	
		相对湿度	
6	重要设备性能	激光器	
		光功率计	
		光谱仪	
		时间数字转换器	
7	检测结果	纠缠光源纠缠态制备速率	
		纠缠光源量子态保真度	
		测量基模块测量效率	
		纠缠光源总体探测效率	
		非信令条件检验	
		贝尔检验	
		器件无关量子随机数产率	
	器件无关量子随机数随机性统计检测		
测试人姓名：测试单位联系电话：			
测试单位地址：审核人姓名：			
测试单位（公章）：测试日期：			
报告书共 页			