



论文

基于概率克隆的量子态区分定理

张文海^{①②③*}, 戴结林^②, 曹卓良^{②③}, 杨名^③

① 淮南师范学院物理系, 淮南 232001;

② 合肥师范学院物理系, 合肥 230601;

③ 安徽大学物理与材料科学学院, 合肥 230039

*E-Mail: zhangwenhaihui@yahoo.com.cn

收稿日期: 2010-10-06; 接受日期: 2010-12-20

国家自然科学基金(批准号: 10704001)、安徽省级高等学校自然科学研究(编号: KJ2010ZD08, KJ2010B172 和 KJ2010B204)和淮南师范学院博士研究启动资金资助项目

摘要 基于概率量子克隆, 给出两个量子态区分理论中著名的 Helstrom 界限, 并将著名的 IDP 极限推广到一般情况. 基于最优概率克隆的么正变换, 给出验证 Helstrom 界限和推广 IDP 极限的一般么正变换. 对于特殊的输入态, 给出有利于在实验上实现两种测量的具体么正变换.

关键词 量子态区分, POVM 测量, Helstrom 界限, IDP 极限, 概率量子克隆

PACS: 03.65.-w, 03.67.-a, 03.67.Dd, 03.67.Hk

量子叠加原理确定非正交量子态的存在. 限于量子不可克隆定理^[1], 非正交量子态不可能精确地测量. 在量子信息科学中, 非正交量子态作为量子编码是量子密码术^[2]的核心. 非正交量子态区分理论^[3,4]为量子密码术的安全性提供理论支撑, 也揭示认识量子世界的一种限度. 由于非正交量子态不可精确测量, 测量方式可能会有两种. 第一, 可能会出错, 但希望出错的概率最小(Minimum Error Discrimination, MED). 第二, 不允许出错, 即测量的结果是明确最优的(Optimal Unambiguous Discrimination, OUD), 但有时可能测不到需要的结果.

考虑具有输入概率 p_1 和 $p_2 = 1 - p_1$ 的两个非正交量子态 $|\psi_1\rangle$ 和 $|\psi_2\rangle$, 系统可以表示为 $\hat{P} = \sum_{i=1}^2 (p_i \hat{\rho}_i)$ (其中 $\hat{\rho}_i = |\psi_i\rangle\langle\psi_i|$ 表示输入态的密度矩

阵算符), 根据量子力学的保迹性有 $\text{Tr}(\hat{P}) = 1$ (其中 Tr 为求迹算符). 利用广义测量(Generalized Measurements)或称正定算符值测量(Positive-Operator-Valued Measures, POVM)^[5~7], 可以在理论上给出 MED 和 OUD 的最优值.

对 MED 测量, 定义 POVM 元 $\hat{M}_i$ 并满足完全性关系 $\sum_{i=1}^2 \hat{M}_i = \hat{I}$ (其中 $\hat{I}$ 为单位算符). 当测量到 $\hat{M}_i$ 时可以认为输入态是 $|\psi_i\rangle$. 因此, 利用定义的 POVM 元 $\hat{M}_i$, 量子态 MED 测量可以表示为

$$\begin{aligned}\text{Tr}(\hat{P}) &= \text{Tr}\left[\sum_{i=1}^2 (p_i \hat{\rho}_i \hat{I})\right] \\ &= \text{Tr}\left[\sum_{i=1}^2 (p_i \hat{\rho}_i \hat{M}_i)\right] + \text{Tr}\left[\sum_{i \neq j}^2 (p_i \hat{\rho}_i \hat{M}_j)\right] = 1.\end{aligned}$$

在这个表示式中, 能够正确判断量子态 MED 测

引用格式: 张文海, 戴结林, 曹卓良, 等. 基于概率克隆的量子态区分定理. 中国科学: 物理学 力学 天文学, 2011, 41: 850–854

Zhang W H, Dai J L, Cao Z L, et al. Quantum state discrimination theorem based on probabilistic cloning (in Chinese). Sci Sin Phys Mech Astron, 2011, 41: 850–854, doi: 10.1360/132010-955

量结果的概率为 $P_{\text{corr}}^{(\text{MED})} = \text{Tr} \left[\sum_{i=1}^2 (p_i \hat{\rho}_i \hat{M}_i) \right]$, 习惯上

最优 MED 测量是求出最小错误测量概率 $P_{\text{err}}^{(\text{MED})} = 1 - P_{\text{corr}}^{(\text{MED})}$. 著名的 Helstrom 界限^[8]给出 MED 测量错误概率的最小值为

$$P_{\text{err}}^{(\text{MED})} = \frac{1}{2} \left(1 - \sqrt{1 - 4p_1 p_2 \left| \langle \psi_1 | \psi_2 \rangle \right|^2} \right). \quad (1)$$

对 OUD 测量, 定义 POVM 元 $\hat{O}_1$, $\hat{O}_2$ 和 $\hat{O}_0$ 且满足完全性关系 $\sum_{i=0}^2 \hat{O}_i = \hat{I}$ (其中 $\hat{I}$ 为单位算符). 因此, OUD 测量可以表示为

$$\begin{aligned} & \text{Tr} \left[\sum_{i=1}^2 (p_i \hat{\rho}_i \hat{O}_i) \right] + \text{Tr} \left[\sum_{i,j=1}^2 (p_i \hat{\rho}_i \hat{O}_j) \right] \\ & + \text{Tr} \left[\sum_{i=1}^2 (p_i \hat{\rho}_i \hat{O}_0) \right] = 1. \end{aligned}$$

由于不允许出错(明确性结果), 即当测量到 $\hat{O}_i$ 时输入态一定是 $|\psi_i\rangle$, 而不允许是 $|\psi_j\rangle$ ($i \neq j$), 这必须要求

$$\text{Tr} \left[\sum_{i,j=1}^2 (p_i \hat{\rho}_i \hat{O}_j) \right] = 0.$$

当测量到 $\hat{O}_0$ 时, 就不能判断输入态. 因此, OUD 测量中会出现不确定结果($\hat{O}_0$), 但是, 一旦测量到结果($\hat{O}_1$ 或 $\hat{O}_2$), 输入态是能够被明确地判定. 能够正确判断测量结果的概率为

$$P_{\text{corr}}^{(\text{OUD})} = \text{Tr} \left[\sum_{i=1}^2 (p_i \hat{\rho}_i \hat{O}_i) \right],$$

习惯上最优 OUD 测量是求出 $P_{\text{corr}}^{(\text{OUD})}$ 的最大值. 当等概率 $p_1 = p_2 = 1/2$ 输入时, 著名的 IDP 极限^[9-11]给出 OUD 测量最大值为

$$P_{\text{corr}}^{(\text{OUD})} = 1 - \left| \langle \psi_1 | \psi_2 \rangle \right|. \quad (2)$$

利用 POVM 测量, 可以得到(1)和(2)式, 同时也给出 POVM 元 $\hat{M}_i$ 和 $\hat{O}_i$ 的具体形式. 由于 $\hat{M}_i$ 和 $\hat{O}_i$ 都是非正交算符, 可以将 POVM 元转化为合适的 Von Neumann 正交测量^[12]并能够在实验上的实现^[13,14]. 最近, 基于无信号条件^[15]给出这两个定理的证明^[16-19], 但没有给出具体的么正变换. 本文基于概率量子克隆^[20], 给出 Helstrom 界限并推广 IDP 极限, 并给出一般性么正变换. 基于一般性么正变换, 对于具体的输入态, 给出可以在物理实验上直接验证的具体么正变换.

1 基于概率克隆的量子态区分定理

量子力学测量假设认为: 对无限多同样拷贝的未知量子态的测量, 就可以精确地判断未知量子态. 利用概率量子克隆, 可以将输入态进行复制到无限多个, 然后对其测量便可以确定未知量子态. 如果概率克隆是最优的, 则量子态区分就是最优的. 对输入概率为 p_1 和 $p_2 = 1 - p_1$ 的两个非正交量子态 $|\psi_1\rangle$ 和 $|\psi_2\rangle$, 不失一般性, 设 $\langle \psi_1 | \psi_2 \rangle = s e^{i\varphi}$ 和 $|\langle \psi_1 | \psi_2 \rangle| = s$ (其中 $s \in (0, 1)$ 和 $\varphi \in [0, 2\pi)$). 定义概率 $1 \rightarrow M$ 量子克隆的么正变换为

$$\begin{aligned} |\psi_1\rangle & \rightarrow \sqrt{\gamma_1} |\psi_1\rangle^{\otimes M} |1\rangle_a + \sqrt{1-\gamma_1} |\psi_2\rangle^{\otimes M} |2\rangle_a, \\ |\psi_2\rangle & \rightarrow e^{i\varphi} \left(\sqrt{\gamma_2} |\psi_2\rangle^{\otimes M} |2\rangle_a + \sqrt{1-\gamma_2} |\psi_1\rangle^{\otimes M} |1\rangle_a \right), \end{aligned} \quad (3)$$

其中 $\gamma_1, \gamma_2 \in (0, 1)$ 分别是复制 $|\psi_1\rangle$ 和 $|\psi_2\rangle$ 的成功系数, $|1\rangle_a$ 和 $|2\rangle_a$ 是可以进行 Von Neumann 正交测量^[12]的辅助系统. 为省略篇幅, 这里不证明概率克隆(3)式的最优性, 因为下面的结论就可以说明. 经过概率克隆后, 利用正交测量, 一定会得到塌缩态 $|\psi_1\rangle^{\otimes M}$ 或 $|\psi_2\rangle^{\otimes M}$. 对它们再次测量, 当 M 为无穷大时, 就可以精确判断塌缩态. 当以概率 $(1-\gamma_1)$ 获得塌缩态并对 $|\psi_2\rangle^{\otimes M}$ 测量会让测量者认为输入态是 $|\psi_1\rangle$, 则测量 $|\psi_1\rangle$ 的出错概率为 $p_1(1-\gamma_1)$. 同理, 当以概率 $(1-\gamma_2)$ 获得塌缩态 $|\psi_1\rangle^{\otimes M}$ 时, 测量 $|\psi_2\rangle$ 的出错概率为 $p_2(1-\gamma_2)$. 所以, MED 测量的出错概率为

$$P_{\text{err}}^{(\text{MED})} = \sum_{i=1}^2 p_i (1-\gamma_i), \quad (4)$$

并求出(4)式的最小值. 当 M 为无穷大时, 由(3)式的内积得

$$s = \sqrt{\gamma_1(1-\gamma_2)} + \sqrt{\gamma_2(1-\gamma_1)}. \quad (5)$$

在约束条件(5)式下求(4)式的最小值, 可以容易得到概率系数为

$$\begin{aligned} \gamma_1 &= \frac{1}{2} + \frac{1-2p_2s^2}{2\sqrt{1-4p_1p_2s^2}}, \\ \gamma_2 &= \frac{1}{2} + \frac{1-2p_1s^2}{2\sqrt{1-4p_1p_2s^2}}. \end{aligned} \quad (6)$$

代入(4)式即可得到 Helstrom 界限(1)式.

对 OUD 测量, 定义概率 $1 \rightarrow M$ 量子克隆幺正变换为

$$\begin{aligned} |\psi_1\rangle &\rightarrow \sqrt{\chi_1} |\psi_1\rangle^{\otimes M} |1\rangle_a + \sqrt{1-\chi_1} |1\rangle^{\otimes M} |3\rangle_a, \\ |\psi_2\rangle &\rightarrow e^{i\varphi} \left(\sqrt{\chi_2} |\psi_2\rangle^{\otimes M} |2\rangle_a + \sqrt{1-\chi_2} |1\rangle^{\otimes M} |3\rangle_a \right). \end{aligned} \quad (7)$$

如果辅助系统测量基 $|1\rangle_a$ 和 $|2\rangle_p$ 被测量到, 可以通过测量塌缩态 $|\psi_1\rangle^{\otimes M}$ 和 $|\psi_2\rangle^{\otimes M}$ 而获得输入态的信息. 当 M 为无穷大时, 就可以精确判断塌缩态. 但是, 当 $|3\rangle_a$ 被测量到, 完全不知道输入态(不确定结果).

OUD 测量的成功概率为

$$P_{\text{corr}}^{(\text{OUD})} = p_1 \chi_1 + p_2 \chi_2. \quad (8)$$

当 M 为无穷大时, (7)的内积为

$$s = \sqrt{(1-\chi_1)(1-\chi_2)}. \quad (9)$$

在约束条件(9)式下求(8)式的最大值, 可以容易得到概率系数为

$$\chi_1 = 1 - \sqrt{\frac{p_2}{p_1}} s, \quad \chi_2 = 1 - \sqrt{\frac{p_1}{p_2}} s. \quad (10)$$

由于成功概率 $\chi_1, \chi_2 \in (0, 1)$, 因此要求

$$p_1 \in (s^2/(1+s^2), 1/(1+s^2)),$$

最优成功概率为

$$P_{\text{corr}}^{(\text{OUD})} = 1 - 2\sqrt{p_1 p_2} s. \quad (11)$$

当等概率 $p_1 = p_2 = 1/2$ 输入时, (11)包含 IDP 极限(2).

由于高维量子系统在物理实验上较难实现, 这里给出 2 维空间的幺正变换. 从约束条件(5)式, 可以给出 MED 测量的一般性幺正变换为

$$\begin{aligned} |\psi_1\rangle_{\text{in}} &\rightarrow \sqrt{\gamma_1} |1\rangle_{\text{in}} + \sqrt{1-\gamma_1} |2\rangle_{\text{in}}, \\ |\psi_2\rangle_{\text{in}} &\rightarrow e^{i\varphi} \left(\sqrt{\gamma_2} |2\rangle_{\text{in}} + \sqrt{1-\gamma_2} |1\rangle_{\text{in}} \right). \end{aligned} \quad (12)$$

从约束条件(9)式, 可以给出 OUD 测量的一般性幺正变换为

$$\begin{aligned} |\psi_1\rangle_{\text{in}} |1\rangle_a &\rightarrow \sqrt{\chi_1} |1\rangle_{\text{in}} |1\rangle_a + \sqrt{1-\chi_1} |1\rangle_{\text{in}} |2\rangle_a, \\ |\psi_2\rangle_{\text{in}} |1\rangle_a &\rightarrow e^{i\varphi} \left(\sqrt{\chi_2} |2\rangle_{\text{in}} |1\rangle_a + \sqrt{1-\chi_2} |1\rangle_{\text{in}} |2\rangle_a \right). \end{aligned} \quad (13)$$

(13)中是对直积态(例如 $|1\rangle_{\text{in}} |1\rangle_a$)进行两次测量, 如果测量到 $|2\rangle_a$ 就不能确定输入态而不需要做第二次测量. 对于具体的输入态, 可以通过(12)和(13)式给出具体的幺正变换.

2 特殊输入态的幺正变换

为了验证 Helstrom 界限和推广 IDP 极限的实验实现的一般性, 应考虑输入态实验制备的可控性和具体幺正变换实验实现的简单与可行性. 设输入态为

$$\begin{aligned} |\psi_1\rangle_{\text{in}} &= |1\rangle_{\text{in}}, \\ |\psi_2\rangle_{\text{in}} &= s e^{i\varphi} |1\rangle_{\text{in}} + \sqrt{1-s^2} |2\rangle_{\text{in}}, \end{aligned} \quad (14)$$

其中 $s \in (0, 1)$ 和 $\varphi \in [0, 2\pi)$. 这种形式的输入态可以在实验上易于制备和控制, 同时, 选择不同的 s 和 φ 就可以验证 Helstrom 界限和推广 IDP 极限的一般性. 对于(14)式具体的输入态, MED 测量的幺正变换为

$$\begin{aligned} |1\rangle_{\text{in}} &\rightarrow \sqrt{\gamma_1} |1\rangle_{\text{in}} + \sqrt{1-\gamma_1} |2\rangle_{\text{in}}, \\ |2\rangle_{\text{in}} &\rightarrow \frac{e^{i\varphi}}{\sqrt{1-s^2}} \left[\left(\sqrt{1-\gamma_2} - s\sqrt{\gamma_1} \right) |1\rangle_{\text{in}} \right. \\ &\quad \left. + \left(\sqrt{\gamma_2} - s\sqrt{1-\gamma_1} \right) |2\rangle_{\text{in}} \right], \end{aligned} \quad (15)$$

其中 γ_1 和 γ_2 由(6)式所给出. (15)式作用在输入态(14)式后, 就可以得到 MED 测量(12)式. 利用(5), (15)式的幺正性可以从其右边的内积

$$\begin{aligned} &\frac{e^{i\varphi}}{\sqrt{1-s^2}} \left\{ \left[\sqrt{\gamma_1(1-\gamma_2)} - s\gamma_1 \right] \right. \\ &\quad \left. + \left[\sqrt{\gamma_2(1-\gamma_1)} - s(1-\gamma_1) \right] \right\} \\ &= \frac{e^{i\varphi}}{\sqrt{1-s^2}} \left[\sqrt{\gamma_1(1-\gamma_2)} + \sqrt{\gamma_2(1-\gamma_1)} - s \right] \\ &= 0 \end{aligned} \quad (16)$$

和其第二式的归一性

$$\begin{aligned} &\frac{1}{1-s^2} \left\{ \left[(1-\gamma_2) - 2s\sqrt{\gamma_1(1-\gamma_2)} + s^2\gamma_1 \right] \right. \\ &\quad \left. + \left[\gamma_2 - 2s\sqrt{\gamma_2(1-\gamma_1)} + s^2(1-\gamma_1) \right] \right\} \\ &= \frac{1}{1-s^2} \left\{ 1 - 2s \left[\sqrt{\gamma_1(1-\gamma_2)} + \sqrt{\gamma_2(1-\gamma_1)} \right] + s^2 \right\} \\ &= 1, \end{aligned} \quad (17)$$

所保证. OUD 测量的幺正变换为

$$\begin{aligned} |1\rangle_{\text{in}} |1\rangle_a &\rightarrow \sqrt{\chi_1} |1\rangle_{\text{in}} |1\rangle_a + \sqrt{1-\chi_1} |1\rangle_{\text{in}} |2\rangle_a, \\ |2\rangle_{\text{in}} |1\rangle_a &\rightarrow \frac{e^{i\varphi}}{\sqrt{1-s^2}} \left[\left(\sqrt{\chi_2} |2\rangle_{\text{in}} - s\sqrt{\chi_1} |1\rangle_{\text{in}} \right) |1\rangle_a \right. \\ &\quad \left. + \left(\sqrt{1-\chi_2} - s\sqrt{1-\chi_1} \right) |1\rangle_{\text{in}} |2\rangle_a \right], \end{aligned} \quad (18)$$

其中 χ_1 和 χ_2 由(10)所给出. (18)作用在输入态(14), 就可以得到 OUD 测量(13)式. 利用(9), (18)式的么正性可以从其右边的内积

$$\begin{aligned} & \frac{e^{\pm i\varphi}}{\sqrt{1-s^2}} \left\{ -s\chi_1 + \left[\sqrt{(1-\chi_1)(1-\chi_2)} - s(1-\chi_1) \right] \right\} \\ &= \frac{e^{\pm i\varphi}}{\sqrt{1-s^2}} \left[\sqrt{(1-\chi_1)(1-\chi_2)} - s \right] = 0, \end{aligned} \quad (19)$$

和其第二式的归一性

$$\begin{aligned} & \frac{1}{1-s^2} \left\{ \chi_2 + s^2 \chi_1 \right. \\ & \left. + \left[(1-\chi_2) - 2s\sqrt{(1-\chi_1)(1-\chi_2)} + s^2(1-\chi_1) \right] \right\} \end{aligned}$$

$$= \frac{1}{1-s^2} \left[1 - 2s\sqrt{(1-\chi_1)(1-\chi_2)} + s^2 \right] = 1 \quad (20)$$

所保证. 对于(15)和(18)式, 就目前物理实验技术, 2 维空间 2 粒子相互作用是比较成熟的技术, 给出的么正变换可以期望在实验上实现.

3 结论

利用最优概率量子克隆得出 Helstrom 界限并推广 IDP 极限. 根据约束条件, 给出实现两种测量的一般性么正变换. 对于具体的输入态, 给出便于在实验上实现的具体的 MED 测量和 OUD 测量的么正变换.

参考文献

- 1 Wootters W K, Zurek W H. A single quantum cannot be cloned. *Nature (London)*, 1982, 299: 802–803; Scarani V, Iblisdir S, Gisin N, et al. Quantum cloning. *Rev Mod Phys*, 2005, 77: 1225–1256
- 2 Gisin N, Ribordy G, Tittel W, et al. Quantum cryptography. *Rev Mod Phys*, 2002, 4: 145–195; Scarani V, Pasquinucci H B, Cerf N J, et al. The security of practical quantum key distribution. *Rev Mod Phys*, 2009, 81: 1301–1350
- 3 Chefles A. Quantum state discrimination. *Contemp Phys*, 2000, 41: 401–424
- 4 Barnett S M, Croke S. Quantum state discrimination. *Adv Opt Photon*, 2009, 1: 238–278
- 5 Kraus K. States, effects and operations. *Lecture Notes in Physics*. Berlin: Springer, 1983
- 6 Peres P. Quantum Theory: Concepts and Methods. Amsterdam: Kluwer, 1993
- 7 Busch P, Grabowski M, Lahti P. Operational Quantum Physics. Berlin: Springer, 1995
- 8 Helstrom C W. Quantum Detection and Estimation Theory. New York: Academic, 1976
- 9 Ivanovic I D. How to differentiate between non-orthogonal states. *Phys Lett A*, 1987, 123: 257–259
- 10 Dieks D. Overlap and distinguishability of quantum states. *Phys Lett A*, 1988, 126: 303–306
- 11 Peres P. How to differentiate between non-orthogonal states. *Phys Lett A*, 1988, 128: 19
- 12 Von Neumann J. Mathematical Foundations of Quantum Mechanics. Princeton: Princeton University Press, 1983
- 13 Sun Y, Hillery M, Bergou A J. Optimum unambiguous discrimination between linearly independent nonorthogonal quantum states and its optical realization. *Phys Rev A*, 2001, 64: 022311
- 14 Wu X, Yu S, Zhou T. One-photon interferometer for realizing optimal unambiguous discrimination among quantum subsets. *Phys Rev A*, 2009, 79: 052302
- 15 Simon C, Buzek V, Gisin N. The no-signaling condition and quantum dynamics. *Phys Rev Lett*, 2001, 87: 170405
- 16 Barnett S M, Andersson E. Bound on measurement based on the no-signaling condition. *Phys Rev A*, 2002, 65: 044307
- 17 Croke S, Andersson E, Barnett S M. No-signaling bound on quantum state discrimination. *Phys Rev A*, 2008, 77: 012113
- 18 Hwang W Y. Helstrom theorem from the no-signaling condition. *Phys Rev A*, 2005, 71: 062315
- 19 Bae J, Lee J W, Kim J, et al. Optimality of minimum-error discrimination by the no-signaling condition. *Phys Rev A*, 2008, 78: 022335
- 20 Duan L M, Guo G C. Probabilistic cloning and identification of linearly independent quantum states. *Phys Rev Lett*, 1998, 80: 4999–5002

Quantum state discrimination theorem based on probabilistic cloning

ZHANG WenHai^{1,2,3*}, DAI JieLin², CAO ZhuoLiang^{2,3} & YANG Ming³

¹ *Department of Physics, Huainan Normal University, Huainan 232001, China;*

² *Department of Physics and Electronic Engineering, Hefei Teachers College, Hefei 230601, China;*

³ *School of Physics and Material Science, Anhui University, Hefei 230039, China*

Based on the probabilistic quantum cloning, the well-known Helstrom bound is derived and the IDP limit is generalized in quantum state discrimination theory. By exploring the unitary transformation of the optimal probabilistic quantum cloning, the general unitary transformations of the Helstrom bound and the general IDP limit are presented. For the explicit input states, the explicit unitary transformations enabling to realize two measures in experiment are provided.

quantum state discrimination, POVM measurement, Helstrom bound, IDP limit, probabilistic quantum cloning

PACS: 03.65.-w, 03.67.-a, 03.67.Dd, 03.67.Hk

doi: 10.1360/132010-955