

# 量子操作区分中叠加资源优势的比较

刘 锋<sup>1</sup>, 高冬梅<sup>1</sup>, 蔡晓秋<sup>2</sup>

(1. 山东工商学院数学与信息科学学院, 山东烟台 264005; 2. 洛阳师范学院 数学科学学院, 河南洛阳 471934)

**摘 要:** 量子资源理论研究的一个中心问题是为具体的资源提供操作性解释, 即在完成某种量子信息处理任务时资源态比任何非资源态更有优势. 最近, Theurer 等人 [T Theurer, et al. Phys Rev Lett 119, 230401 (2017)] 通过扩展相干资源理论建立了严格的叠加资源理论框架. 在叠加资源理论框架下, 本文利用 Holevo-Helstrom 定理定量地刻画单量子比特叠加态在不同类型的量子操作区分任务中的优势, 即计算得到叠加态辅助量子操作区分的最大成功概率大于非叠加态辅助时的值. 这些定量结果还表明, 在相同的叠加态辅助下, 不同类型的操作(自由操作与非自由操作)之间最易于区分, 而相同类型的量子操作之间, 非自由操作之间的区分易于自由操作的区分. 这一结果为新型量子安全通信协议的设计提供了新的依据.

**关键词:** 叠加资源理论; 量子操作区分; 区分优势

**中图分类号:** TN914.4

**文献标识码:** A

**文章编号:** 0372-2112 (2020)02-0303-05

**电子学报 URL:** <http://www.ejournal.org.cn>

**DOI:** 10.3969/j.issn.0372-2112.2020.02.012

## Comparison of Operational Advantages of Superposition in Operational Discrimination

LIU Feng<sup>1</sup>, GAO Dong-mei<sup>1</sup>, CAI Xiao-qi<sup>2</sup>

(1. School of Mathematic and Information Science, Shandong Technology and Business University, Yantai, Shandong 264005, China;

2. School of Mathematic Science, Luoyang Normal University, Luoyang, Henan 471934, China)

**Abstract:** In the study of quantum resource theories, one of the central problems is to provide an operational meaning for a given resource. In the provided quantum information processing task, every resource state provides an advantage compared to the case where all resourceless states are used. Recently, Theurer et al. [T Theurer, et al. Phys Rev Lett 119, 230401 (2017)] introduced a rigorous resource theory framework for the quantification of superposition through generalizing of resource theories of coherence. Under the framework, we show that every one-qubit superposition state provides an advantage in different channel discrimination, quantified in terms of the Holevo-Helstrom theorem. Then, the maximum probability of success in superposition-assisted channel discrimination has been calculated, which is larger than the value of maximum probability of success in no superposition-assisted channel discrimination. Our results contribute to understanding the discrimination relevance of channels: assisting by the unique coherent state, different kinds of channels are most distinguishable, and different coherent channels are more distinguishable than different incoherent channels.

**Key words:** resource theory of superposition; unambiguous channel discrimination; operational advantage

## 1 引言

量子信息科学的一个重要的研究目标是深入理解量子资源. 最近, 量子资源理论<sup>[1]</sup>作为量化和操作量子系统内在资源的强有力工具引起了广泛关注. 纠缠资源理论<sup>[2,3]</sup>、相干资源理论<sup>[4,5]</sup>和叠加资源理论<sup>[6]</sup>等不同物理场景下的理论都已经被提出和分析. 而研究量

子资源理论的一个核心问题是选定的资源寻找量子操作意义, 即在执行某种物理任务时资源态比任意非资源态都有操作优势. 量子操作(子信道)区分任务是当前最常用的用来说明资源态有操作优势的物理任务之一<sup>[3,7]</sup>. 比如, Takagi 等人<sup>[7]</sup>指出下凸资源理论中任意资源态辅助的量子操作区分成功概率恒大于非资源态辅助的成功概率. 通过推广相干资源理论, Theurer 等

人<sup>[6]</sup>得到了可量化的叠加资源理论. 由于叠加是下凸的, 所以任意的叠加态都可以提高量子操作区分的成功概率.

在量子操作区分任务中, 目前的研究结果只是关注资源态与非资源态在区分中发挥作用的大小差异, 总是忽略不同类型的量子操作在被区分过程中的差异. 在实际的量子信息处理过程中, 不仅仅信源(输入的量子态), 信道(量子操作)类型的不同往往对应不同的信息编码方法, 会在更大程度上影响信息的传输效率<sup>[8]</sup>. 因此, 在量子通信领域, 一个自然的问题是: 不同类型的量子操作进行区分时有什么差异?

本文仅比较信道的输入态来自二维空间时两个量子操作区分的最优概率. 通过比较发现: 两个操作的类型不同(一个是自由操作, 另一个是非自由操作)时最易于区分; 令人惊奇的是, 有了资源态的辅助, 两个非自由操作反倒比两个自由操作更易于区分.

## 2 基础知识

本节介绍量子操作区分任务<sup>[9,10]</sup>.

记  $\mathcal{L}(\mathcal{X})$  是作用在 Hilbert 空间  $\mathcal{X}$  上线性操作的集合,  $\mathcal{L}(\mathcal{X}, \mathcal{Y}) = \{\Phi | \Phi: \mathcal{L}(\mathcal{X}) \rightarrow \mathcal{L}(\mathcal{Y})\}$  是将 Hilbert 空间  $\mathcal{X}$  上的操作映射为 Hilbert 空间  $\mathcal{Y}$  上操作的线性映射集,  $\mathcal{D}(\mathcal{X})$  是  $\mathcal{X}$  上量子态的集合, 并且  $\mathcal{T}(\mathcal{X})$  是  $\mathcal{X}$  上非资源态(自由态)的集合(从而,  $\mathcal{T}^c(\mathcal{X})$  是  $\mathcal{X}$  上资源态(非自由态)的集合). 另外, 若  $\sum_i \Psi_i$  是  $\mathcal{X}$  到  $\mathcal{Y}$  上的完全正的保迹(CPTP)映射, 称完全正的迹不减映射  $\Psi_i \in \mathcal{L}(\mathcal{X}, \mathcal{Y})$  是  $\mathcal{X}$  到  $\mathcal{Y}$  的一条子信道.

不失一般性, 我们假设信道的输入态  $\rho \in \mathcal{D}(\mathcal{X})$  只经过一条子信道. 操作区分任务是指, 对信道的输出态选取最优的正算子取值测量(POVM)  $\{M_i\}$ , 实现以最大的成功概率.

$$p_{succ}(\{\Psi_i\}, \{M_i\}, \rho) = \sum_i \text{tr}[M_i \Psi_i(\rho)] \quad (1)$$

判断输入态  $\rho$  被施加了哪一种量子操作.

Piani 与 Watrous<sup>[11]</sup>证明了, 存在量子操作区分任务, 任意的纠缠态  $\rho$  都可以使  $p_{succ}(\{\Psi_i\}, \{M_i\}, \rho)$  严格大于  $p_{succ}(\{\Psi_i\}, \{M_i\}, \sigma)$ , 其中  $\sigma \in \mathcal{T}(\mathcal{X})$  是任意的可分态. 最近, Takagi 等人<sup>[7]</sup>、Skrzypczyk 和 Linden<sup>[12]</sup>, 与 Bae 等人<sup>[3]</sup>建立了基于鲁棒性(robustness)的资源度量与操作区分任务之间的关系, 从而得到操作区分任务中资源态辅助下的最优概率比非资源态辅助时的优势最多可达到所选资源态的鲁棒值. 这个定量关系遍历了所有的量子信道类型.

## 3 操作区分中叠加资源的优势

利用 Holevo-Helstrom 定理<sup>[13,14]</sup>可知, 区分量子操

作  $\{\Psi_1, \Psi_2\}$  的最大成功概率是:

$$\max_{\{M_i\}} p_{succ}(\{\Psi_1, \Psi_2\}, \{M_i\}, \rho) = \frac{1}{2} + \frac{\|(\Psi_1 - \Psi_2)[\rho]\|_1}{4} \quad (2)$$

由于 Baumgratz 等人<sup>[4]</sup>证明发现任意的酉操作都可以利用该系统中的自由操作和相干态实现得到, 因此我们只需研究两量子比特系统中的两个最基本的自由操作:

$$\begin{aligned} \Psi_1 &= x|0\rangle\langle 0| + (1-x)|1\rangle\langle 1|, x \in [0, 1]; \\ \Psi_2 &= y|0\rangle\langle 1| + (1-y)|1\rangle\langle 0|, y \in [0, 1] \end{aligned} \quad (3)$$

作为比较对象, 我们选取最基本的非自由操作:

$$\Psi = (\sqrt{z}|0\rangle + \sqrt{1-z}|1\rangle)\langle 0|, z \in (0, 1) \quad (4)$$

### 3.1 最大叠加态辅助区分

对于式(3)中的两个自由操作, 可以计算得到:

$$\begin{aligned} \Psi_1 |+\rangle\langle +| \Psi_1^\dagger &= \frac{1}{2}(x|0\rangle + (1-x)|1\rangle) \\ &\quad \cdot (x\langle 0| + (1-x)\langle 1|) \\ \Psi_2 |+\rangle\langle +| \Psi_2^\dagger &= \frac{1}{2}(y|0\rangle + (1-y)|1\rangle) \\ &\quad \cdot ((1-y)\langle 0| + y\langle 1|) \end{aligned} \quad (5)$$

其中  $|+\rangle = \frac{(|0\rangle + |1\rangle)}{\sqrt{2}}$ .

由式(2)和(5)可得:

$$\begin{aligned} \max_{\{M_i\}} p_{succ}(\{\Psi_1, \Psi_2\}, \{M_i\}, |+\rangle\langle +|) \\ = \frac{1}{2} + \frac{1 - 2(x+y) + 2(x^2 + y^2)}{8}, \end{aligned} \quad (6)$$

$$\max_{\{M_i\}} p_{succ}(\{\Psi_1, \Psi_2\}, \{M_i\}, |0\rangle\langle 0|)$$

$$= \max_{\{M_i\}} p_{succ}(\{\Psi_1, \Psi_2\}, \{M_i\}, |1\rangle\langle 1|) = \frac{1}{2}$$

其中, 当  $x = y = \frac{1}{2}$  时, 即使区分辅助态是最大相干态,

也有  $\max_{\{M_i\}} p_{succ}(\{\Psi_1, \Psi_2\}, \{M_i\}, |+\rangle\langle +|) = \frac{1}{2}$ , 即完全混合态总是不可区分的(参见图1).

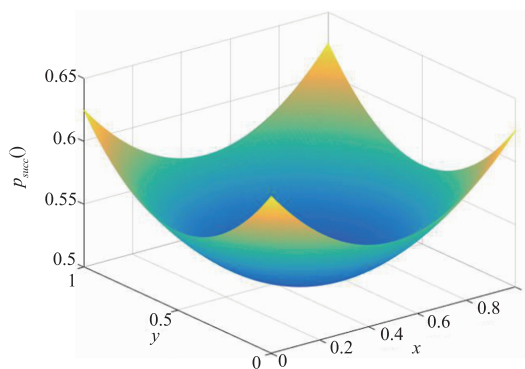


图1 相干态辅助下不同类型自由操作区分时的最优概率关于  $x, y$  的趋势

对于式(4)中的非自由操作,可以计算得到:

$$\begin{aligned} \Psi|+\rangle\langle+|\Psi^\dagger &= \frac{1}{2}(z|0\rangle\langle 0| + \sqrt{z(1-z)}|0\rangle\langle 1| \\ &+ \sqrt{z(1-z)}|1\rangle\langle 0| + (1-z)|1\rangle\langle 1|) \end{aligned} \quad (7)$$

由式(2)、(5)和(7)可得(参见图2)

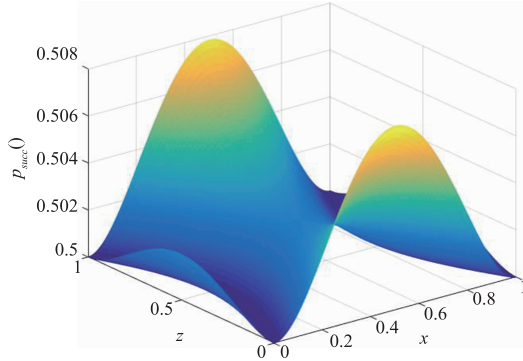


图2 相干态辅助下自由操作与非自由操作区分时的最优概率关于x,z的趋势

$$\begin{aligned} \max_{\{M_i\}} p_{succ}(\{\Psi_1, \Psi\}, \{M_i\}, |+\rangle\langle+|) \\ &= \frac{1}{2} + \frac{|\sqrt{z(1-z)} - x(1-x)|}{4}, \\ \max_{\{M_i\}} p_{succ}(\{\Psi_1, \Psi\}, \{M_i\}, |0\rangle\langle 0|) \\ &= \max_{\{M_i\}} p_{succ}(\{\Psi_1, \Psi\}, \{M_i\}, |1\rangle\langle 1|) = \frac{1}{2} \end{aligned} \quad (8)$$

由式(2)和(7)可得(参见图3)

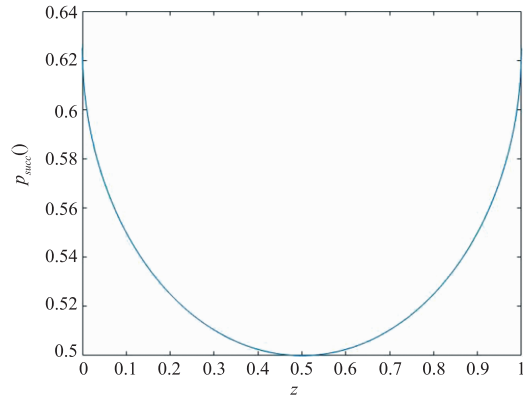


图3 相干态辅助下不同非自由操作区分时的最优概率关于z的趋势

$$\begin{aligned} \max_{\{M_i\}} p_{succ}(|+\rangle\langle 0|, \Psi, \{M_i\}, |+\rangle\langle+|) \\ &= \frac{1}{2} + \frac{|1 - 2\sqrt{z(1-z)}|}{8}, \\ \max_{\{M_i\}} p_{succ}(|+\rangle\langle 0|, \Psi, \{M_i\}, |0\rangle\langle 0|) \\ &= \max_{\{M_i\}} p_{succ}(|+\rangle\langle 0|, \Psi, \{M_i\}, |1\rangle\langle 1|) = \frac{1}{2} \end{aligned} \quad (9)$$

其中,  $z=1/2$  时非自由操作  $\Psi=|+\rangle\langle 0|$ , 所以这时两

个非自由操作不可区分。

为了比较方便,分别取  $x=1/3, y=z=1/4$ 。从而,对于式(3)中的两个自由操作,由式(2)可得:

$$\begin{aligned} \max_{\{M_i\}} p_{succ}(\{\Psi_1, \Psi_2\}, \{M_i\}, |+\rangle\langle+|) &\approx 0.5087, \\ \max_{\{M_i\}} p_{succ}(\{\Psi_1, \Psi_2\}, \{M_i\}, |0\rangle\langle 0|) \\ &= \max_{\{M_i\}} p_{succ}(\{\Psi_1, \Psi_2\}, \{M_i\}, |1\rangle\langle 1|) = \frac{1}{2} \end{aligned} \quad (10)$$

对于式(4)中的非自由操作,由式(2)可得:

$$\begin{aligned} \max_{\{M_i\}} p_{succ}(\{\Psi_1, |+\rangle\langle 0|, \Psi\}, \{M_i\}, |+\rangle\langle+|) &\approx 0.5694, \\ \max_{\{M_i\}} p_{succ}(\{\Psi_1, |+\rangle\langle 0|, \Psi\}, \{M_i\}, |0\rangle\langle 0|) \\ &= \max_{\{M_i\}} p_{succ}(\{\Psi_1, |+\rangle\langle 0|, \Psi\}, \{M_i\}, |1\rangle\langle 1|) = \frac{1}{2} \end{aligned} \quad (11)$$

并且

$$\begin{aligned} \max_{\{M_i\}} p_{succ}(|+\rangle\langle 0|, \Psi, \{M_i\}, |+\rangle\langle+|) &\approx 0.5168 \\ \max_{\{M_i\}} p_{succ}(|+\rangle\langle 0|, \Psi, \{M_i\}, |0\rangle\langle 0|) \\ &= \max_{\{M_i\}} p_{succ}(|+\rangle\langle 0|, \Psi, \{M_i\}, |1\rangle\langle 1|) = \frac{1}{2} \end{aligned} \quad (12)$$

在最大叠加态辅助以及上述选定的量子操作下,不同类型的待区分操作最易于区分,这时的最优区分概率为 0.5694;待区分的量子操作类型相同时,非自由操作的最优区分概率 0.5168 大于自由操作的最优区分概率 0.5087。在下一节我们将说明,辅助态为任意二维的叠加纯态时有类似的结果。

### 3.2 叠加纯态的辅助区分

本节研究下述纯的叠加态  $\rho = (\sqrt{p}|0\rangle + \sqrt{1-p}|1\rangle)(\sqrt{p}\langle 0| + \sqrt{1-p}\langle 1|)$ , 其中  $p \in (0, 1)$ 。

对于式(3)中的两个自由操作,可以计算得到:

$$\begin{aligned} \Psi_1 \rho \Psi_1^\dagger &= x^2 p |0\rangle\langle 0| + x(1-x)\sqrt{p(1-p)}|0\rangle\langle 1| \\ &+ x(1-x)\sqrt{p(1-p)}|1\rangle\langle 0| + (1-x)^2(1-p)|1\rangle\langle 1|, \\ \Psi_2 \rho \Psi_2^\dagger &= y^2(1-p)|0\rangle\langle 0| + y(1-y)\sqrt{p(1-p)}|0\rangle\langle 1| \\ &+ y(1-y)\sqrt{p(1-p)}|1\rangle\langle 0| + (1-y)^2 p |1\rangle\langle 1| \end{aligned} \quad (13)$$

由式(2)和(13)可得:

$$\begin{aligned} \max_{\{M_i\}} p_{succ}(\{\Psi_1, \Psi_2\}, \{M_i\}, \rho) \\ &= \frac{1}{2} + \frac{\sqrt{p(1-p)}}{2} |x(1-x) - y(1-y)|, \\ \max_{\{M_i\}} p_{succ}(\{\Psi_1, \Psi_2\}, \{M_i\}, |0\rangle\langle 0|) \\ &= \max_{\{M_i\}} p_{succ}(\{\Psi_1, \Psi_2\}, \{M_i\}, |1\rangle\langle 1|) = \frac{1}{2} \end{aligned} \quad (14)$$

其中,当  $x=y$  或  $x=1-y$  时,两个自由操作不可区分。

对于式(4)中的非自由操作,可以计算得到:

$$\begin{aligned} \Psi \rho \Psi^\dagger &= pz|0\rangle\langle 0| + p\sqrt{z(1-z)}|0\rangle\langle 1| \\ &\cdot \langle 1| + p\sqrt{z(1-z)}|1\rangle\langle 0| + p(1-z)|1\rangle\langle 1| \end{aligned} \quad (15)$$

由式(2)和式(15)可得:

$$\begin{aligned} & \max_{\{M_i\}} p_{succ}(\{\Psi_1, |+\rangle\langle 0|\}, \{M_i\}, \rho) \\ &= \frac{1}{2} + \frac{|2x(1-x)\sqrt{p(1-p)} - p|}{4}, \\ & \max_{\{M_i\}} p_{succ}(\{\Psi_1, |+\rangle\langle 0|\}, \{M_i\}, |0\rangle\langle 0|) \\ &= \max_{\{M_i\}} p_{succ}(\{\Psi_1, |+\rangle\langle 0|\}, \{M_i\}, |1\rangle\langle 1|) = \frac{1}{2}; \\ & \max_{\{M_i\}} p_{succ}(\{|+\rangle\langle 0|\}, \Psi, \{M_i\}, \rho) \\ &= \frac{1}{2} + \frac{|2\sqrt{z(1-z)} - 1|}{4} p, \\ & \max_{\{M_i\}} p_{succ}(\{|+\rangle\langle 0|\}, \Psi, \{M_i\}, |0\rangle\langle 0|) \\ &= \max_{\{M_i\}} p_{succ}(\{|+\rangle\langle 0|\}, \Psi, \{M_i\}, |1\rangle\langle 1|) = \frac{1}{2} \end{aligned} \quad (16)$$

为了比较方便(见图4),分别取  $x=1/3$ ,  $y=z=1/4$  并且  $p \in (1/3, 1)$ . 从而,由式(2)和(13)可得:

$$\begin{aligned} & \max_{\{M_i\}} p_{succ}(\{\Psi_1, \Psi_2\}, \{M_i\}, \rho) \\ &= \frac{1}{2} + \frac{5}{288} \sqrt{p(1-p)}, \\ & \max_{\{M_i\}} p_{succ}(\{\Psi_1, \Psi_2\}, \{M_i\}, |0\rangle\langle 0|) \\ &= \max_{\{M_i\}} p_{succ}(\{\Psi_1, \Psi_2\}, \{M_i\}, |1\rangle\langle 1|) = \frac{1}{2} \end{aligned} \quad (17)$$

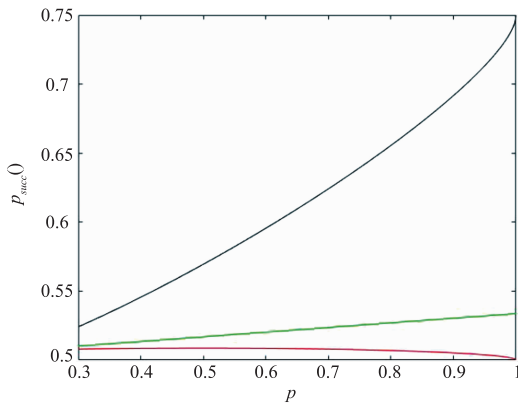


图4 区分不同类型操作时的最优概率关于  $p$  的趋势比较  
红色线表示:  $\max_{\{M_i\}} p_{succ}(\{\Psi_1, \Psi_2\}, \{M_i\}, \rho)$  关于  $p$  的曲线, 绿色线表示:  $\max_{\{M_i\}} p_{succ}(\{|+\rangle\langle 0|\}, \Psi, \{M_i\}, \rho)$  关于  $p$  的曲线, 黑色线表示:  $\max_{\{M_i\}} p_{succ}(\{\Psi_1, |+\rangle\langle 0|\}, \{M_i\}, \rho)$  关于  $p$  的曲线

由式(2)和式(15)可得:

$$\begin{aligned} & \max_{\{M_i\}} p_{succ}(\{\Psi_1, |+\rangle\langle 0|\}, \{M_i\}, \rho) \\ &= \frac{1}{2} + \left| \frac{\sqrt{p(1-p)}}{9} - \frac{p}{4} \right|, \\ & \max_{\{M_i\}} p_{succ}(\{\Psi_1, |+\rangle\langle 0|\}, \{M_i\}, |0\rangle\langle 0|) \end{aligned}$$

$$= \max_{\{M_i\}} p_{succ}(\{\Psi_1, |+\rangle\langle 0|\}, \{M_i\}, |1\rangle\langle 1|) = \frac{1}{2};$$

$$\max_{\{M_i\}} p_{succ}(\{|+\rangle\langle 0|\}, \Psi, \{M_i\}, \rho) \approx \frac{1}{2} + 0.0337p,$$

$$\max_{\{M_i\}} p_{succ}(\{|+\rangle\langle 0|\}, \Psi, \{M_i\}, |0\rangle\langle 0|)$$

$$= \max_{\{M_i\}} p_{succ}(\{|+\rangle\langle 0|\}, \Psi, \{M_i\}, |1\rangle\langle 1|) = \frac{1}{2} \quad (18)$$

结合上述结果、图4以及叠加资源封闭与下凸的性质<sup>[6]</sup>,不难得到下述命题:在任意二维叠加态辅助下,不同类型的待区分操作最易于区分;待区分的量子操作类型相同时,非自由操作的最优区分概率大于自由操作的最优区分概率。

## 4 总结与讨论

现有的量子操作区分问题只关注不同类型的量子态(资源态与非资源态)在任务执行过程中发挥的作用,而忽略了待区分的量子操作本身的特征对问题的影响.在二维量子系统中,本文详细研究了这个问题,结果发现不同类型的待区分操作最易于区分,并且非自由操作的最优区分概率大于自由操作的最优区分概率。

这些结果蕴含的信息论意义和可以延展的问题包括:

(1)在量子信息的处理过程中,不仅仅量子态中的量子资源,量子操作中的量子资源同样可以在信息处理过程中带来量子优势.因此,众多基于非正交态不可区分的量子密码协议<sup>[15-18]</sup>,理论上都可以设计出基于量子操作区分的秘密协议.这一思想为新型的量子信源编码方案提供了思路。

(2)根据信源与信道的属性,一个完整的通信过程可分为全经典通信、全量子通信和经典-量子混合通信.其中,全经典通信过程是指信源与信道都是经典通信,全量子通信是指信源与信道都是量子通信,混合通信是指信源是经典通信而信道是量子通信.在相同的信源编码下,为了使得通信过程更安全,应该首选全量子通信方式,这是因为全部的非自由操作最难于区分。

(3)一个重要的问题是:本文结论在高维辅助系统以及多操作区分下是否仍然成立?

## 参考文献

- [1] Chitambar E, Gour G. Quantum resource theories [J]. Rev Mod Phys, 2019, 91(2):025001.
- [2] Horodecki R, Horodecki P, Horodecki M, et al. Quantum entanglement [J]. Rev Mod Phys, 2009, 81(2):865-942.
- [3] Bae J, Chruściński D, Piani M. More entanglement implies higher performance in channel discrimination tasks [J]. Phys Rev Lett, 2019, 122(14):140404.
- [4] Baumgratz T, Cramer M, Plenio M B. Quantifying coher-

- ence[J]. Phys Rev Lett, 2014, 113(14):140401.
- [5] Streltsov A, Adesso G, Plenio M B. Quantum coherence as a resource[J]. Rev Mod Phys, 2017, 89(4):041003.
- [6] Theurer T, Killoran N, Egloff D, et al. Resource theory of superposition[J]. Phys Rev Lett, 2017, 119(23):230401.
- [7] Takagi R, Regula B, Bu K, et al. Operational advantage of quantum resources in subchannel discrimination[J]. Phys Rev Lett, 2019, 122(14):140402.
- [8] Nielsen M A, Chuang I L. Quantum Computation and Quantum Information[M]. England, Cambridge University Press: 2010. 362 – 370.
- [9] Duan R Y, Feng Y, Ying M S. Perfect distinguishability of quantum operations[J]. Phys Rev Lett, 2009, 103(21):210501.
- [10] Cao T Q, Gao F, Yang Y H, et al. Determination of locally perfect discrimination for two-qubit unitary operations[J]. Quantum Inf Process, 2016, 15(1):529 – 549.
- [11] Piani M and Watrous J. All entangled states are useful for channel discrimination[J]. Phys Rev Lett, 2009, 102(25):250501.
- [12] Skrzypczyk P, Linden N. Robustness of measurement, discrimination games, and accessible information[J]. Phys Rev Lett, 2019, 122(14):140403.
- [13] Holevo A. Statistical decision theory for quantum systems[J]. J Multivariate Anal, 1973, 3(4):337 – 394.
- [14] Helstrom C W. Quantum Detection and Estimation Theory[M]. New York, Academic Press: 1976. 55 – 70.
- [15] Gao F, Qin S J, Huang W, et al. Quantum private query: a new kind of practical quantum cryptographic protocols[J]. Sci CHINA Phys Mech, 2019, 62(7):07030.
- [16] Wei C Y, Cai X Q, Liu B, et al. A generic construction of quantum-oblivious-key-transfer-based private query with ideal database security and zero failure[J]. IEEE T Comput, 2018, 67(1):2 – 8.
- [17] 胡文斌, 聂聪, 邱振宇, 等. 一种城市交通路网实时动态多路口路径导航量子搜索方法[J]. 电子学报, 2018, 46(1):104 – 109.  
Hu W B, Nie C, Qiu Z Y, et al. A route guidance method based on quantum searching for real-time dynamic multi-intersections in urban traffic networks[J]. Acta Electronica Sinica, 2018, 46(1):104 – 109. (in Chinese)
- [18] Song T, Tan X, Wen J. Statistical fluctuation analysis of measurement-device-independent quantum random-number generation[J]. Phys Rev A, 2019, 99(2):022333.

#### 作者简介



刘 锋(通信作者) 男, 1980 年出生, 山东单县人, 山东工商学院数学与信息科学学院教授、硕士生导师, 研究方向为量子信息处理。  
E-mail: liufeng23490@126.com



高冬梅 女, 1979 年出生, 山东单县人, 山东工商学院数学与信息科学学院讲师, 研究方向为量子密码学与量子信息处理。  
E-mail: gaomei8006@126.com