基于单向 LOCC 的正交两体态区分算法

司萌萌,李志慧,刘成基

(陕西师范大学 数学与信息科学学院,西安 710119)

摘要: 针对 $d \otimes d$ 两体系统中正交态的区分问题,利用判断其对应的正交补空间的维数,进而判断正交补空间是否包含一个最大交换子空间,基于单向 LOCC,提出一种新的态区分算法。对于 $4 \otimes 4$ 上的广义正交 Bell 态,通过系统研究其单向可区分性,给出其可单向区分的快速算法。实验结果表明, $d \otimes d$ 上的区分算法适用于任何正交两体态的区分,比起该算法, $4 \otimes 4$ 上快速算法的复杂度更小。

关键词: 谱分解;局域区分;正交两体态;纠缠态;特征向量

中文引用格式: 司萌萌,李志慧,刘成基. 基于单向 LOCC 的正交两体态区分算法[J]. 计算机工程,2018,44(2):182-186.

英文引用格式: SI Mengmeng, LI Zhihui, LIU Chengji. Orthogonal Bipartite States Distinguish Algorithm Based on One-way LOCC[J]. Computer Engineering, 2018, 44(2): 182-186.

Orthogonal Bipartite States Distinguish Algorithm Based on One-way LOCC

SI Mengmeng, LI Zhihui, LIU Chengji

(School of Mathematics and Information Science, Shaanxi Normal University, Xi'an 710119, China)

【Abstract】 In the topic of distinguishment of orthogonal states in $d \otimes d$ bipartite system, with the way of judging dimension of there corresponding orthogonal complement, and then determine whether the orthogonal complement space contains a maximally Abelian subspace, at last propose a new algorithm to distinguish states based on one-way LOCC. For generalized orthogonal Bell states in $4 \otimes 4$ bipartite system, by studying their distinguishment, this paper propose a faster algorithm based on one way LOCC. Experimental results show that the algorithm in $d \otimes d$ bipartite system can be applies in distinguishing any orthogonal bipartite states. What's more, the algorithm in $4 \otimes 4$ bipartite system is less complicated.

【Key words】 spectral decomposition; local distinguish; orthogonal bipartite states; entanglement; feature vector

DOI: 10.3969/j.issn.1000-3428.2018.02.032

0 概述

随着量子信息理论的发展,量子密码学相比经典密码学越来越体现出更多优势的同时,也提出了许多挑战性的课题^[1-3],其中量子态的局域区分就是量子通信领域一个基本问题。在局域操作和经典通信(Local Operation and Classical Communication, LOCC)的限制下,正交态并不是总可以精确区分的^[4-6]。一组正交量子态不一定可局域区分,是量子非局域性的一个表现。研究区域区分的规律不仅有利于理解量子非局域性,还可使人们能从新的角度去研究其他的量子信息理论问题^[7-9]。两体正交量子态的局域区分方案如下:在许多可能的正交两体量子态中选出一个分发给 Alice 和 Bob,他们只利用

LOCC 就可以找出他们共享的是哪一个态。文献[10]构造了一组乘积纯态,获得的结论是来自于不可扩张乘积基的成员之间是不能通过 LOCC 被完全区分的;文献[11]证明了任意 2 个多体正交纯态可以精确局域区分,此结果说明了在 LOCC 下量子态的纠缠与否与其精确区分的关系不大,也说明了此问题的复杂性;文献[12]的结果是得出了类 Holevo 上界对于局部的可访问的信息来自于一个两体系统的量子态系综;文献[13]的结果表明了几乎所有来自于 N 个 d 维多体系统的 $d+1$ 个正交量子态集合通过 LOCC 是不可以完全被区分的。

近期,文献[14]提出了一个利用单向 LOCC (one-way LOCC, 1-LOCC) 来区分两体正交态的框架,并在理论上给出了两体正交态的集合通过单向

基金项目: 国家自然科学基金(61373150,61602291);陕西省科学技术研究发展计划工业攻关项目(2013K0611);中央高校基本科研业务费专项资金(GK201603087)。

作者简介: 司萌萌(1994—),女,硕士研究生,主研方向为密码学;李志慧,教授、博士;刘成基,硕士研究生。

收稿日期: 2016-12-08 **修回日期:** 2017-04-06 **E-mail:** 1016011722@qq.com

LOCC 可区分性的判定,但文献[5]并没有给出区分两体正交态的一般性算法。本文给出基于单向 LOCC 的一类正交两体态区分算法,并在此算法的基础上,对 $4 \otimes 4$ 上的广义正交 Bell 态给出其可单向区分的一个充分条件,此充分条件可作为一个快速算法判断正交态是否可单向 LOCC 区分,最后对此结论给予实例验证。

1 文献[14]主要结论回顾

文献[14]得到了如下结果:在一个 $d_A \otimes d_B$ 的两体系统中,其中, d_A, d_B 是子系统 A 和 B 的维数,如果第 i 部分(其中 $i = A$ 或 B)开始一个单向 LOCC 协议以完全区分一个正交两体态的集合,那么这样的单向 LOCC 协议存在的信息取决于一个 $d_i \times d_i$ 阶的 Hermitian 矩阵组成的子空间是否包含一个最大交换子空间。根据这一结论,对于 $d_A \otimes d_B$ 中的所有正交两体态集合,其单向 LOCC 的可区分性便可以得到判定^[15]。

1.1 密度矩阵 $\rho_{AB}^{(i)}$ 的谱分解

令 Alice 和 Bob 各有一个 d 维 Hilbert 空间上量子系统,分别记为 H_A 和 H_B 。设 Alice 和 Bob 共享 n 个正交量子态中的一个,这些正交量子态的密度矩阵 $\rho_{AB}^{(1)}, \rho_{AB}^{(2)}, \dots, \rho_{AB}^{(n)}$ 在 $H_A \otimes H_B$ 上是可测量的。他们想要建立一个由 Alice 开始的单向 LOCC 协议来区分他们共享的态。

定义 1 密度矩阵 $\rho_{AB}^{(i)}$ 的谱分解表示为:

$$\rho_{AB}^{(i)} = \sum_{j=1}^{r_i} \lambda_{ij} |\psi_{ij}\rangle \langle \psi_{ij}| \quad (1)$$

其中, $r_i = \text{rank}(\rho_{AB}^{(i)})$, $\{\lambda_{ij}\}_{j=1}^{r_i}$ 是密度矩阵 $\rho_{AB}^{(i)}$ 的非 0 特征值,并且 $\langle \psi_{ij} | \psi_{i'j'} \rangle = \delta_{i'i} \delta_{j'j} \forall 1 \leq i \leq i' \leq n, 1 \leq j \leq r_i$ 。

1.2 标准正交基和复矩阵

定义 2 令 $\{|s_j\rangle_A\}_{j=1}^d$ 和 $\{|s_j\rangle_B\}_{j=1}^d$ 分别是 H_A 和 H_B 上的标准正交基。 $\forall 1 \leq i \leq n, 1 \leq j \leq r_i$, 通过 $|\psi_{ij}\rangle_{AB}$ 在一组基 $\{|s_j\rangle_A |s_k\rangle_B\}_{j,k=1}^d$ 中的扩张来定义 $d \times d$ 维复矩阵 W_{ij} , 其中:

$$|\psi_{ij}\rangle_{AB} = \sum_{k,l=1}^d (W_{ij})_{kl} |s_l\rangle_A |s_k\rangle_B \quad (2)$$

因此, $\langle \psi_{ij} | \psi_{i'j'} \rangle = \text{Tr}(W_{ij}^\dagger W_{i'j'}) = \delta_{i'i} \delta_{j'j}, \forall 1 \leq i \leq i' \leq n, 1 \leq j \leq r_i, 1 \leq j' \leq r_{i'}$ 。

1.3 主要符号及说明

定义指标集 $I = \{(i, i', j, j'), | 1 \leq i < i' \leq n, 1 \leq j \leq r_i, 1 \leq j' \leq r_{i'}\}$, 令 $\hat{i} = (i, i', j, j') \in I$; 定义 $W_{\hat{i}}$ 为迹为 0 的 $d \otimes d$ 复矩阵, 且 $W_{\hat{i}} = W_{ij}^\dagger W_{i'j'}$, 令矩阵 $H_{\hat{i}} = \frac{1}{2} [W_{\hat{i}} + (W_{\hat{i}})^\dagger]$, $A_{\hat{i}} = \frac{1}{2i} [W_{\hat{i}} - (W_{\hat{i}})^\dagger]$ 。

例 1 令指标集 $I = \{(i, i', j, j'), | 1 \leq i < i' \leq 2, 1 \leq j \leq 2, 1 \leq j' \leq 3\}$, 则 I 中的元素为 $(1, 2, 1, 1), (1, 2, 1, 2), (1, 2, 1, 3), (1, 2, 2, 1), (1, 2, 2, 2), (1, 2,$

$2, 3)$ 。当 $\hat{i} = (1, 2, 1, 1)$ 时, $W_{\hat{i}} = W_{11}^\dagger W_{21}, H_{\hat{i}} = \frac{1}{2} [W_{\hat{i}} + (W_{\hat{i}})^\dagger] = \frac{1}{2} [W_{11}^\dagger W_{21} + W_{21}^\dagger W_{11}]$, $A_{\hat{i}} = \frac{1}{2i} [W_{\hat{i}} - (W_{\hat{i}})^\dagger] = \frac{1}{2} [W_{11}^\dagger W_{21} - W_{21}^\dagger W_{11}]$ 。以此类推得到 $W_{\hat{i}} \sim W_{\hat{j}}, H_{\hat{i}} \sim H_{\hat{j}}, A_{\hat{i}} \sim A_{\hat{j}}$ 。

设 S 为所有 $d \otimes d$ 上的 Hermitian 矩阵组成的一个实向量空间; $T = \{\sum_{i \in I} a_i H_i + b_i A_i, \forall a_i, b_i \in \mathbb{R}\}$ 为 S 的一个子空间; $T_\perp$ 为 S 中 T 的正交补空间, $\mathbf{1}_d \in T_\perp$, 其中, $\mathbf{1}_d$ 是 $d \otimes d$ 的单位矩阵。

1.4 最大交换子空间

定义 3 如果实向量空间 S 中一个维数为 d 的子空间中的任意 2 个矩阵都可交换, 那么这个子空间称作一个最大交换子空间 (Maximally Abelian Subspace, MAS)。

注释 1 任意一个 MAS 和唯一一组共同的特征向量相对应, 且这组共同的特征向量可以使得 MAS 中所有 Hermitian 矩阵在这组基下对角化。

1.5 $d \otimes d$ 上的广义正交两体量子态

定义 4 在 $d \otimes d$ 中, d^2 维的广义的正交两体量子态可以表示为^[6]:

$$|\psi_{nm}\rangle_{AB} \equiv \sum_{j=0}^{n-1} (W_{nm})_{kj} |s_j\rangle_A |s_k\rangle_B \quad (3)$$

其中, $n, m = 0, 1, \dots, d-1, (W_{ij})_{kj} \equiv \frac{e^{i\pi jn/d}}{\sqrt{d}} \delta_{j \oplus_{dm}, k}, \forall j, k = 0, 1, \dots, n-1$ 注意到, W_{nm} 中的任意 2 个矩阵正交。

文献[14]对来自 $d \otimes d$ 双体系统中的一个给定的正交双体混合态的密度矩阵集合 $\{\rho_{AB}^{(1)}, \rho_{AB}^{(2)}, \dots, \rho_{AB}^{(n)}\}$, 建立了一个可由 Alice 发起的协议, 该协议的目的是利用单向 LOCC 来区分给定的正交双体态 $\rho_{AB}^{(1)}, \rho_{AB}^{(2)}, \dots, \rho_{AB}^{(n)}$ 中的哪一个为他们所共享的量子态。

进一步, 文献[14]就密度矩阵 $\rho_{AB}^{(1)}, \rho_{AB}^{(2)}, \dots, \rho_{AB}^{(n)}$ 是否可单向 LOCC 给出了如下结论:

引理 1 密度矩阵 $\rho_{AB}^{(1)}, \rho_{AB}^{(2)}, \dots, \rho_{AB}^{(n)}$ 仅用空间 H_A 和 H_B 上的投影测量就可单向 LOCC 可区分, 当且仅当 $T_\perp$ 包含一个 MAS^[14]。

引理 2 当 $\dim T_\perp = d+1$ 时, $T_\perp$ 包含一个 MAS 当且仅当矩阵 Ω_j 是秩 2 的且 $\cap_{j=1}^{\dim \mathfrak{R}} \text{Supp}(\Omega_j)$ 是一维的, $j = 1, 2, \dots, \dim \mathfrak{R}$ ^[14]。

注释 2 设 $\{T_i\}_{i=1}^{d+t}$ 是 $T_\perp$ 的一个 MAS。令 C 是由矩阵 $\{i[T_j, T_k] | 1 \leq j < k \leq d+t\}$ 张成的实向量空间, 其中 $[T_j, T_k] \equiv T_j T_k - T_k T_j$ 。令矩阵 $\{G_i\}_{i=1}^{\dim C}$ 是 C 的标准正交基。对于每一个 $j \in \{1, 2, \dots, \dim C\}$, Γ_j 是 $(d+1) \times (d+1)$ 的实反对称矩阵, 其 (i, j) 元素由如下方式给出:

$$(\Gamma_j)_{kj} = i \text{Tr}(G_j [T_k, T_i])$$

令 $\mathfrak{R}$ 是由矩阵 $\{\Gamma_j\}_j$ 张成的实向量空间, 矩阵 $\{\Omega_j\}_{j=1}^{\dim \mathfrak{R}}$ 是 $\mathfrak{R}$ 的标准正交基。

利用引理 1 可对 n 个正交态的密度矩阵 $\rho_{AB}^{(1)}$, $\rho_{AB}^{(2)}, \dots, \rho_{AB}^{(n)}$ 的单向可区分性进行判定, 引理 2 是对 $\dim T_{\perp} = d + 1$ 时的特殊情况给出判定。但这个判定在执行时太复杂, 现将上述正交量子态换为式(3)中的态, 给出基于单向 LOCC 的式(3)中态的区分算法, 并提出一种在 $d = 4$ 时判断态可区分的快速算法。

2 $d \otimes d$ 上的纠缠态区分算法

本文主要考虑式(3)中的态在由 Alice 开始的单向 LOCC 可区分问题。现给出在 $d \otimes d$ 中, 任意 $N(2 \leq N \leq d^2)$ 个纠缠态的局域区分算法。

2.1 纠缠态区分算法内容

步骤 1 在 $d \otimes d$ 上任意选取 $N(2 \leq N \leq d^2)$ 个纠缠态。

步骤 2 计算矩阵 $W_{\hat{i}}$, 进而得到矩阵 $H_{\hat{i}}, A_{\hat{i}}$ 以及集合 T 。

步骤 3 计算 $\dim T_{\perp}$, 作如下判断:

1) 当 $\dim T_{\perp} \leq d - 1$ 时, 该 N 个态不能由 Alice 开始一个单向 LOCC 协议来区分, 算法终止。

2) 当 $\dim T_{\perp} = d$ 时, 进一步检查: 该 $T_{\perp}$ 是否为一个 MAS。如果是, 则该 N 个态可以由 Alice 开始一个单向 LOCC 协议来区分, 转入步骤 4; 否则, 算法终止。

3) 当 $\dim T_{\perp} \geq d + 1$ 时, 进一步检查: 如果 $T_{\perp}$ 包含一个 MAS 在 S 中, 那么该 N 个态可以由 Alice 开始一个单向 LOCC 协议来区分, 转入步骤 4; 否则, 算法终止。

步骤 4 计算 MAS 中非单位矩阵的特征向量。

注释 3 若步骤 1 中的 N 个态可单向 LOCC 区分, 则以上算法求得的 MAS 的特征向量便可作为相应的投影算子对所选的纠缠态进行区分;

步骤 2 中, 由指标集 I 和 $\hat{i}$ 的定义可知 I 的势为 $\frac{d(d-1)}{2}$, 因此, 由 $W_{\hat{i}} = W_{ij}^{\dagger} W_{ij}$ 可以得到 $\frac{d(d-1)}{2}$ 个 $W_{\hat{i}}$, 从而求得 $H_{\hat{i}}$ 和 $A_{\hat{i}}$, 其中线性无关的 $H_{\hat{i}}$ 和 $A_{\hat{i}}$ 的个数即为 T 的维数。

步骤 3 中, 由 $\dim T_{\perp} = d^2 - \dim T$ 得到 $T_{\perp}$ 的维数, 基于 $T_{\perp}$ 的维数值, 可以将这些正交两体态分成不同类。

2.2 纠缠态区分算法分析

该算法是判断正交两体态是否可单向 LOCC 的一般性算法, 虽与文献[14]算法性能相似, 但却优于原算法, 其原因是本文算法适用于任何一组正交两体态是否可区分的判定; 其次, 该算法将判断正交态是否可区分转化为判断正交态组的正交补空间是否包含有一个 MAS, 区分时只需进行一次投影测量, 该算法同时兼顾了算法复杂度和算法性能, 因此, 更具有实际应用价值。

3 $4 \otimes 4$ 上的纠缠态快速区分算法

3.1 算法原理

利用 2.1 节算法, 对式(3)中 $d = 4$ 的情况, 得到快速判断纠缠态单向 LOCC 区分的一个结论。

由式(3), 当 $d = 4$ 时, $4 \otimes 4$ 上广义的正交两体态为:

$$|\psi_{nm}\rangle_{AB} = \sum_{j,k=0}^3 (W_{nm})_{kj} |s_j\rangle_A |s_k\rangle_B \quad (4)$$

其中, $(W_{nm})_{kj} = \frac{e^{i\pi jn/2}}{2} \delta_{j \oplus 4m, k}, \forall j, k = 0, 1, 2, 3$ 。

令集合:

$$U_1 = \left\{ T_1 = W_{00}, T_2 = W_{02}, T_3 = \frac{W_{23} - W_{21}}{2}, \right.$$

$$\left. T_4 = \frac{W_{21} + W_{23}}{2i}, T_5 = W_{22} \right\}$$

$$U_2 = \left\{ T_1 = W_{00}, T_2 = W_{02}, T_3 = \frac{W_{01} + W_{03}}{2}, \right.$$

$$\left. T_4 = \frac{W_{01} - W_{03}}{2i}, T_5 = W_{20} \right\}$$

$$U_3 = \left\{ T_1 = W_{00}, T_2 = \frac{W_{10} + W_{30}}{2}, T_3 = \frac{W_{10} - W_{30}}{2i}, \right.$$

$$\left. T_4 = W_{20}, T_5 = W_{22} \right\}$$

$$U_4 = \left\{ T_1 = W_{00}, T_2 = W_{22}, T_3 = \frac{W_{33} - iW_{11}}{2i}, \right.$$

$$\left. T_4 = \frac{W_{33} + iW_{11}}{2}, T_5 = W_{20} \right\}$$

$$U_5 = \left\{ T_1 = W_{00}, T_2 = \frac{W_{32} - W_{12}}{2}, T_3 = W_{20}, \right.$$

$$\left. T_4 = i \frac{W_{32} + W_{12}}{2}, T_5 = W_{22} \right\}$$

$$U_6 = \left\{ T_1 = W_{00}, T_2 = \frac{W_{13} - iW_{31}}{2}, T_3 = \frac{W_{13} + iW_{31}}{2i}, \right.$$

$$\left. T_4 = W_{22}, T_5 = W_{20} \right\}$$

定理 1 对式(4)中的广义正交两体态, 设其正交补空间为 $T_{\perp}$, 若 $T_{\perp} \supset U_i (i = 1, 2, \dots, 6)$, 则这组正交两体态一定可单向 LOCC 区分。

证明: 以第一种情况为例, 若 $T_{\perp} \supset U_1$, 则 $T_{\perp}$ 是由

$$\left\{ T_1 = W_{00}, T_2 = W_{02}, T_3 = \frac{W_{23} - W_{21}}{2}, T_4 = \frac{W_{21} + W_{23}}{2i}, T_5 = W_{22}, T_6, T_7, \dots \right\} \text{张成的。}$$

考虑集合:

$$U_1 = \left\{ T_1 = W_{00}, T_2 = W_{02}, T_3 = \frac{W_{23} - W_{21}}{2}, \right.$$

$$\left. T_4 = \frac{W_{21} + W_{23}}{2i}, T_5 = W_{22} \right\}$$

计算 $i[T_i, T_j] (i, j = 1, 2, \dots, 5)$ 可得, C 是由矩阵 G_1 和 G_2 张成的, 其中:

$$G_1 = \frac{1}{2\sqrt{2}} \begin{pmatrix} 0 & 1 & 0 & 1 \\ -1 & 0 & -1 & 0 \\ 0 & -1 & 0 & -1 \\ -1 & 0 & -1 & 0 \end{pmatrix}$$

$$G_2 = \frac{i}{2\sqrt{2}} \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

$\mathfrak{R}$ 是由矩阵 Ω_1 和 Ω_2 张成的, 其中:

$$\Omega_1 \propto \Gamma_1 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \end{pmatrix}$$

$$\Omega_2 \propto \Gamma_2 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & -1 & 0 \end{pmatrix}$$

矩阵 Ω_1 和 Ω_2 是秩 2 的且 $Supp(\Omega_1) \cap Supp(\Omega_2)$ 是由 $(0, 0, 0, 0, 1)^T$ 张成的。

因此, 由引理 2, U_1 包含一个 MAS, 又 $U_1 \subset T_\perp$, 因此 $T_\perp$ 包含一个 MAS, 从而由引理 1 可知, 对应的这组纠缠态可单向 LOCC 区分。

其他情况可类似证明。

注释 4 实际上, $U_i (1, 2, \dots, 6)$ 中包含一个 MAS, 且涵盖了由 T 可能组成的所有含 MAS 的集合。因此, 一组纠缠态对应的 $T_\perp$ 若包含其一, 该 $T_\perp$ 就包含一个 MAS, 这些纠缠态就一定可单向 LOCC 区分。

当然, 利用 2.1 节算法也可以区分式 (4) 中的态, 但判断 $T_\perp$ 是否包含一个 MAS 有时是困难的。

3.2 快速算法内容

步骤 1 在 $4 \otimes 4$ 上任意选取 $N (2 \leq N \leq 16)$ 个纠缠态。

步骤 2 计算 W_{ij} , 进而得到 $H_{ij}, A_{ij}, T, T_\perp$ 。

步骤 3 根据 $T_\perp$ 作如下判断:

1) 若 $T_\perp$ 满足定理 1, 则该 N 个态可以由 Alice 开始一个单向 LOCC 协议来区分, 转入步骤 4。

2) 若 $T_\perp$ 不满足定理 1, 则该 N 个态不可以由 Alice 开始一个单向 LOCC 协议来区分, 算法结束。

步骤 4 计算 MAS 中非单位矩阵的特征向量。

3.3 算法分析

首先容易看出 2.1 节算法和 3.2 节算法的步骤 1、步骤 2 和步骤 4 均是一致的, 即在判断一组纠缠态是否可单向 LOCC 区分时, 都需要计算 W_{ij}, H_{ij} ,

A_{ij} 和 T 的值。主要区别在步骤 3, 当 $d=4$ 时, 本文提出的快速算法不论 $\dim T_\perp$ 是否为 5, 只需要判断这组纠缠态的 $T_\perp$ 是否满足 $T_\perp \supseteq U_i (i=1, 2, \dots, 6)$ 即可判断该组态是否可区分。而文献 [5] 中的算法在 $d=4$ 时, 需计算 $\dim T_\perp$ 且要对 $\dim T_\perp$ 进行判断: 1) 当 $\dim T_\perp = 5$ 时, 需继续判断 Ω_j 的秩是否为 2、 $\cap_{j=1}^{\dim \mathfrak{R}} Supp(\Omega_j)$ 的维数是否为 1; 2) 当 $\dim T_\perp \neq 5$ 时, 还需进一步寻找 MAS。

因此本文提出的算法计算复杂度较小, 给纠缠态的区分带来了方便。

基于以上快速算法 (3.2 节), 现给出实例验证。

例 2 判断 $4 \otimes 4$ 上的一组纠缠态 $\{|\psi_{01}\rangle, |\psi_{10}\rangle, |\psi_{11}\rangle, |\psi_{23}\rangle\}$ 是否可单向 LOCC 区分。

$$W_{ij} = W_{ij}^\dagger W_{i'j'}$$

$$W_1 = W_{01}^\dagger W_{10} = W_{13}, W_2 = W_{01}^\dagger W_{11} = W_{10}$$

$$W_3 = W_{01}^\dagger W_{23} = W_{22}, W_4 = W_{10}^\dagger W_{11} = W_{01}$$

$$W_5 = W_{10}^\dagger W_{23} = W_{13}, W_6 = W_{11}^\dagger W_{23} = W_{12}$$

通过计算矩阵 H_{ij} 和 A_{ij} 可得, T 是由以下

Hermitian 矩阵生成:

$$\left\{ W_{22}, \frac{W_{01} + W_{03}}{2}, \frac{W_{01} - W_{03}}{2i}, i \frac{W_{32} + W_{12}}{2}, \frac{W_{32} - W_{12}}{2}, \frac{W_{13} - iW_{31}}{2}, \frac{W_{13} + iW_{31}}{2i}, \frac{W_{10} + W_{30}}{2}, \frac{W_{10} - W_{30}}{2i} \right\}$$

因此, $T_\perp$ 是由:

$$\left\{ T_1 = W_{00}, T_2 = W_{02}, T_3 = \frac{W_{23} - W_{21}}{2}, T_4 = \frac{W_{21} + W_{23}}{2i}, T_5 = W_{22}, T_6 = \frac{W_{33} - iW_{11}}{2i}, T_7 = \frac{W_{33} + iW_{11}}{2} \right\}$$

生成。

符合定理 1, 因此该 4 个态一定可单向 LOCC 区分。

接下来讨论如何区分这组态。通过计算 $[T_j, T_k] (j, k = 1, 2, 3, 4, 5, 6, 7)$:

$$[T_1, T_2] = 0, [T_1, T_3] = 0, [T_1, T_4] = 0$$

$$[T_1, T_5] = 0, [T_1, T_6] = 0, [T_1, T_7] = 0$$

$$[T_2, T_3] = 0, [T_2, T_4] = 0, [T_2, T_5] = 0$$

$$[T_2, T_6] \neq 0, [T_2, T_7] \neq 0$$

$$[T_3, T_4] = 0, [T_3, T_5] \neq 0, [T_3, T_6] \neq 0$$

$$[T_3, T_7] \neq 0$$

$$[T_4, T_5] \neq 0, [T_4, T_6] \neq 0, [T_4, T_7] \neq 0$$

$$[T_5, T_6] \neq 0, [T_5, T_7] \neq 0; [T_6, T_7] = 0$$

可得, $\{T_i\}_{i=1}^4$ 张成了一个 MAS 在 $T_\perp$ 中, 因此, $T_\perp$ 包含一个 MAS。

故 $T_\perp$ 包含的 MAS 集合为:

$$\left\{ T_1 = W_{00}, T_2 = W_{02}, T_3 = \frac{W_{23} - W_{21}}{2}, T_4 = \frac{W_{23} + W_{21}}{2i} \right\}$$

计算 MAS 的共同正交基得到对应的投影测量基为:

$$\left\{ \begin{array}{l} \frac{|0\rangle_A + |1\rangle_A + |2\rangle_A + |3\rangle}{2}, \\ \frac{|0\rangle_A - |1\rangle_A - |2\rangle_A + |3\rangle}{2}, \\ \frac{|0\rangle_A + |1\rangle_A - |2\rangle_A - |3\rangle}{2}, \\ \frac{|0\rangle_A - |1\rangle_A + |2\rangle_A - |3\rangle}{2} \end{array} \right\}$$

分别记为 $\gamma_1, \gamma_2, \gamma_3, \gamma_4$ 。

因此:

$$\begin{aligned} |\psi_{01}\rangle &= \frac{1}{2} \left[\gamma_1 \otimes \frac{|0\rangle - |1\rangle - |2\rangle + |3\rangle}{2} + \right. \\ &\quad \left. \gamma_2 \otimes \frac{-|0\rangle + |1\rangle + |2\rangle + |3\rangle}{2} + \right. \\ &\quad \left. \gamma_3 \otimes \frac{|0\rangle + |1\rangle - |2\rangle + |3\rangle}{2} + \right. \\ &\quad \left. \gamma_4 \otimes \frac{-|0\rangle - |1\rangle - |2\rangle + |3\rangle}{2} \right] \\ |\psi_{10}\rangle &= \frac{1}{2} \left[\gamma_1 \otimes \frac{|0\rangle + i|1\rangle - |2\rangle - i|3\rangle}{2} + \right. \\ &\quad \left. \gamma_2 \otimes \frac{|0\rangle - i|1\rangle + |2\rangle - i|3\rangle}{2} + \right. \\ &\quad \left. \gamma_3 \otimes \frac{|0\rangle + i|1\rangle + |2\rangle + i|3\rangle}{2} + \right. \\ &\quad \left. \gamma_4 \otimes \frac{|0\rangle - i|1\rangle - |2\rangle + i|3\rangle}{2} \right] \\ |\psi_{11}\rangle &= \frac{1}{2} \left[\gamma_1 \otimes \frac{|0\rangle + i|1\rangle - |2\rangle - i|3\rangle}{2} + \right. \\ &\quad \left. \gamma_2 \otimes \frac{-|0\rangle - i|1\rangle - |2\rangle - i|3\rangle}{2} + \right. \\ &\quad \left. \gamma_3 \otimes \frac{|0\rangle - i|1\rangle + |2\rangle - i|3\rangle}{2} + \right. \\ &\quad \left. \gamma_4 \otimes \frac{-|0\rangle + i|1\rangle + |2\rangle - i|3\rangle}{2} \right] \\ |\psi_{23}\rangle &= \frac{1}{2} \left[\gamma_1 \otimes \frac{|0\rangle + |1\rangle + |2\rangle - |3\rangle}{2} + \right. \\ &\quad \left. \gamma_2 \otimes \frac{|0\rangle + |1\rangle - |2\rangle + |3\rangle}{2} + \right. \\ &\quad \left. \gamma_3 \otimes \frac{-|0\rangle + |1\rangle + |2\rangle + |3\rangle}{2} + \right. \\ &\quad \left. \gamma_4 \otimes \frac{-|0\rangle + |1\rangle - |2\rangle - |3\rangle}{2} \right] \end{aligned}$$

显然, $\{|\psi_{01}\rangle, |\psi_{10}\rangle, |\psi_{11}\rangle, |\psi_{23}\rangle\}$ 可单向 LOCC 区分。

4 结束语

基于文献[14]利用单向 LOCC 区分两体正交态的框架,本文提出一类 $d \otimes d$ 上广义正交两体态基于

单向 LOCC 的区分算法,并主要研究了 $4 \otimes 4$ 上的可分态,得到了一种快速且有效判断纠缠态是否可单向 LOCC 区分的算法。但对于 $\dim T_{\perp} = d+t$ 的情况,还有许多与 MAS 相关的规律需要发现,因此,后期将继续探索其他维上纠缠态的区分规律,例如量子密码、量子秘密共享、量子信道的经典容量、量子纠缠的鲁棒性以及束缚纠缠态等。

参考文献

- [1] GHOSH S, KAR G, ROY A, et al. Distinguishability of Bell States[J]. Physical Review Letters, 2001, 87(27): 277902.
- [2] 杨小东, 高国娟, 周其旭, 等. 基于代理重签名的电子政务数据安全交换方案[J]. 计算机工程, 2017, 43(2): 183-188.
- [3] RAHAMAN R, PARKER M G. Quantum Scheme for Secret Sharing Based on Local Distinguishability[J]. Physical Review A, 2015, 91(2).
- [4] 姜伟. 正交量子态的局域区分问题[D]. 合肥: 中国科学技术大学, 2009.
- [5] CHEGLES A. Condition Unambiguous State Distinction Using LOCC[J]. Physical Review A, 2003, 69(5): 521-524.
- [6] HORODECKI M, DE S A, SEN U. Local Distinguishability: More Nonlocality with Less Entanglement[J]. Physical Review Letters, 2003, 90(4): 047902.
- [7] ZHANG Z C, WEN Q Y, GAO F. One-way LOCC Indistinguishability of Maximally Entangled States[J]. Quantum Information Processing, 2014, 13: 795-804.
- [8] FAN H. Distinguishability and Indistinguishability by Local Operations and Classical Communication[J]. Physical Review Letters, 2004, 92(17): 177905.
- [9] HAYASHI M, MARJHAM D, MURAO M, et al. Bounds on Multipartite Orthogonal State Discrimination Using Local Operations and Classical Communication[J]. Physical Review Letters, 2006, 96(4): 040501.
- [10] BENNETT C H, DIVINCENZO D P, MOR T, et al. Unextendible Product Bases and Bound Entanglement[J]. Physical Review Letters, 1999, 82: 5385-5488.
- [11] WAGATE J, HARDY L. Nonlocality, Asymmetry and Distinguishing Bipartite States[J]. Physical Review Letters, 2002, 89(14): 147901.
- [12] BADZIAG P, HORODECKI M, DE S A, et al. Locally Accessible Information: How Much Can the Parties Gain by Cooperating[J]. Physical Review Letters, 2003, 91: 117901.
- [13] COHEN S M. Almost Every Set of $N \geq d+1$ Orthogonal States on $d^{\otimes n}$ is Locally Indistinguishable[J]. Physical Review A, 2008, 77: 060309.
- [14] TANMAY S. Framework for Distinguishability of Orthogonal Bipartite States by One-way Local Operations and Classical Communication[J]. Physical Review A, 2016, 93(3): 757-758.
- [15] NATHANSON M. Distinguishing Bipartite Orthogonal States by LOCC: Best and Worst Cases[J]. Journal of Mathematical Physics, 2005, 46(6): 901-933.

编辑 刘冰