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

构造纠缠目击的一般方法

杨莹　曹怀信

General method of constructing entanglement witness

Yang Ying　Cao Huai-Xin

引用信息 Citation: Acta Physica Sinica, 67, 070303 (2018)　DOI: 10.7498/aps.67.20172697
在线阅读 View online: http://dx.doi.org/10.7498/aps.67.20172697
当期内容 View table of contents: http://wulixb.iphy.ac.cn/CN/Y2018/V67/I7

物理学报 Acta Phys. Sin. Vol. 67, No. 7 (2018) 070303

构造纠缠目击的一般方法*

杨莹[1)2)] 曹怀信[1)†]

1) (陕西师范大学数学与信息科学学院, 西安 710119)

2) (运城学院数学与信息技术学院, 运城 044000)

(2017 年 10 月 10 日收到; 2018 年 1 月 3 日收到修改稿)

量子纠缠作为量子通信和量子计算过程中不可缺少的资源, 在量子信息领域中有着广泛的应用. 如何判定一个给定的量子态是否为纠缠态仍然是一个重要的课题. 纠缠目击是一种特殊的自伴算子, 它可以用来判断一个量子态是否为纠缠态. 本文首先从纠缠目击的定义入手, 给出构造纠缠目击的一般方法, 证明了当一个可测量 A 在可分纯态上的最大期望 C_A 严格小于它的最大特征值 $\lambda_{\max}(A)$ 时, 对任何满足条件 $C_A \leqslant C < \lambda_{\max}(A)$ 的参数 C, 算子 $W_C = CI - A$ 都是一个纠缠目击; 然后, 作为应用得到了利用图态的稳定子构造纠缠目击的一系列方法.

关键词: 纠缠目击, 图态, 稳定子

PACS: 03.67.Mn, 03.65.Db, 03.65.Ud, 02.30.Sa **DOI:** 10.7498/aps.67.20172697

1 引 言

随着量子理论与信息科学的交叉融合, 量子信息理论成为物理学、信息科学及数学等领域的研究者共同关注的研究热点. 大部分量子信息处理任务都需要一个共同的物理资源, 即量子纠缠. 因此, 对量子信息处理任务的研究在某种程度上可以说是对量子纠缠的研究. 量子纠缠作为量子通信和量子计算的载体, 已被广泛用于量子计算、量子隐形传态 [1]、量子密码术 [2]、量子容错计算 [3]、量子超密编码 [4]、量子秘密共享 [5]、量子安全直接通信 [6] 和分布式量子机器学习 [7] 等领域. 这显示了量子纠缠的强大功能和作用. 例如: Deng 等 [8] 提出了量子超纠缠并研究了它在量子信息处理中的应用; 从美艳等 [9] 研究了在不同初态下 Dzyaloshinskii-Moriya 相互作用及内禀退相干对海森伯系统的量子纠缠的影响; 任宝藏和邓富国 [10] 介绍了光子系统两自由度量子态在量子信息中的一些新应用, 包括超并行量子计算、超纠缠态分析、超纠缠浓缩和纯化三个部分; 宗晓岚和杨名 [11] 提出了一种可以保护多粒子纠缠不受振幅衰减影响的有效物理方案. 尽管量子纠缠有如此广泛的应用, 但是如何来判断给定量子纠缠性问题仍是一项相当有难度的任务 [12]. 有一种类型的纠缠判据——纠缠目击, 是探测纠缠的有效的工具, 并且也是迄今为止在实验中探测纠缠最有效的工具. 因此, 人们对纠缠目击进行了大量的研究. 例如, 考虑它们的可分解性与优化问题 [13,14]; 对局域测量纠缠目击的优化设置 [15,16] 以及在刻画纠缠中的应用 [17−19]. 特别是文献 [20] 研究了如何使用稳定子理论构造纠缠的充分条件, 提出了针对图态的纠缠目击的构造方法. 文献 [21—26] 从另一个不同的观点说明线性规划是构造纠缠目击的一个非常有用的方法. 从理论上而言, 对于每一个纠缠态, 至少存在一个纠缠目击来探测它. 然而, 如何具体构造纠缠目击仍是一个非常重要的问题.

近年来, 人们试图通过机器学习理论与技术研究量子纠缠问题. 随着深度学习技术在量子多体

* 国家自然科学基金 (批准号: 11371012, 11601300, 11571213, 11771009) 和中央高校基本科研业务费专项资金 (批准号: GK201703093) 资助的课题.

† 通信作者. E-mail: caohx@snnu.edu.cn

 http://wulixb.iphy.ac.cn

系统中的应用, 通过量子纠缠透镜出现了一种新的深度学习方式, 纠缠量化了机器学习中真实数据集的复杂性, 可以指导人工神经网络体系的结构设计[27]. Deng等[28]通过随机采样RBM的权重参数, 进一步考察了一般RBM态的纠缠特性, 证明了RBM能够找到具有远距离相互作用的模型哈密顿量的基态(带幂律纠缠). Levine等[29]在题为《深度学习与量子纠缠》的研究中提出了由深度卷积算法电路实现的函数和量子多体波函数之间的等价性, 以期通过量子纠缠度量来量化深层网络模拟输入的复杂关联结构的能力. Carleo等[30]提出了基于神经网络的量子态表示方案, 并展示了它在多个经典量子多体问题上的高精度和表达能力. Gao和Duan[31]发现深度神经网络和量子多体问题存在紧密关联, 证明了利用深度神经网络模型可以有效表示几乎所有多体量子系统的波函数, 展示了神经网络和深度学习算法在量子多体问题研究中的巨大潜力.

受文献[20]的启发, 本文首先提出构造纠缠目击的一般方法, 然后将这种构造方法应用于图态, 得到相应的结论, 并将这些结论与文献[20]中给出的纠缠目击进行比较, 发现文献[20]中已给出的纠缠目击是本文给出的一般纠缠目击的特例, 这说明本文构造的纠缠目击更具一般性.

2 纠缠目击的构造

考虑复合系统 $\mathcal{H}^{(n)} := \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_n$, 用 $L(\mathcal{H}^{(n)})$ 表示 $\mathcal{H}^{(n)}$ 上线性算子之集; $B(\mathcal{H}^{(n)})$ 表示 $\mathcal{H}^{(n)}$ 上有界线性算子之集; $B_{\text{her}}(\mathcal{H}^{(n)})$ 表示 $\mathcal{H}^{(n)}$ 上自伴算子之集; $S(\mathcal{H}^{(n)})$ 表示 $\mathcal{H}^{(n)}$ 上纯态之集; $D(\mathcal{H}^{(n)})$ 表示 $\mathcal{H}^{(n)}$ 上混合态之集.

下面给出完全可分态和纠缠态的定义.

定义1[20] 1) 若复合量子系统 $\mathcal{H}^{(n)}$ 上的 n 体纯态 $|\psi\rangle$ 可以表示为分量子系统 $\mathcal{H}_i$ 上的态 $|\psi_i\rangle (i = 1, 2, \cdots, n)$ 的张量积, 即

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle,$$

则称 $|\psi\rangle$ 是完全可分纯态, 否则为纠缠态.

2) 复合量子系统 $\mathcal{H}^{(n)}$ 上的 n 体混合态 ρ 可以表示为分量子系统 $\mathcal{H}_k$ 上的态 $\rho_i^k (k = 1, 2, \cdots, n)$ 的张量积的凸组合, 即

$$\rho = \sum_{i=1}^{m} p_i \rho_i^1 \otimes \rho_i^2 \otimes \cdots \otimes \rho_i^n,$$

则称 ρ 是完全可分态, 否则为纠缠态.

$\mathcal{P}$ 表示 $\mathcal{H}^{(n)}$ 上全体完全可分纯态之集; $D_{\text{sep}}(\mathcal{H}^{(n)})$ 表示 $\mathcal{H}^{(n)}$ 上完全可分混合态之集. 容易证明: $D_{\text{sep}}(\mathcal{H}^{(n)})$ 是 $\mathcal{P}$ 的闭凸包.

定义2[20] 设 $W \in B_{\text{her}}(\mathcal{H}^{(n)})$, 若

1) 对任意的 $\rho \in D_{\text{sep}}(\mathcal{H}^{(n)})$, 有 $\text{tr}(W\rho) \geqslant 0$;

2) 存在 $\rho_0 \in D(\mathcal{H}^{(n)})$, 使得 $\text{tr}(W\rho_0) < 0$,

则称 W 为纠缠目击.

设 W 是一个纠缠目击, 则当 $\text{tr}(W\rho) < 0$ 时, ρ 一定是纠缠态. 这时, 称 ρ 可被 W 探测.

理论上每一个纠缠态都至少存在一个纠缠目击来探测它. 事实上, 纠缠目击的构造并不是一件容易的事情. 因此, 纠缠目击的构造成为大家关注的热点问题. 下面我们给出构造纠缠目击的一般方法.

一般来说, 若 $A \in B_{\text{her}}(\mathcal{H}^{(n)}), \rho \in D(\mathcal{H}^{(n)})$, 则

$$\lambda_{\min}(A) \leqslant \langle A\rangle_\rho \leqslant \lambda_{\max}(A),$$

其中 $\lambda_{\min}(A), \lambda_{\max}(A)$ 分别为 A 的最小特征值与最大特征值. 事实上, 由于 $A = A^\dagger$, 则 A 有谱分解 $A = \sum_i \lambda_i |\psi_i\rangle\langle\psi_i|$ 且 $\sum_i |\psi_i\rangle\langle\psi_i| = I$, 从而 $\lambda_{\min}(A) I \leqslant A \leqslant \lambda_{\max}(A) I$. 于是, 对任量子态 $\rho \in D(\mathcal{H}^{(n)})$, 有 $\lambda_{\min}(A)\rho \leqslant \sqrt{\rho} A \sqrt{\rho} \leqslant \lambda_{\max}(A)\rho$. 所以

$$\lambda_{\min}(A) \leqslant \text{tr}(\rho A) = \text{tr}(\sqrt{\rho} A \sqrt{\rho}) \leqslant \lambda_{\max}(A).$$

因此 $\lambda_{\min}(A) \leqslant \langle A\rangle_\rho \leqslant \lambda_{\max}(A)$.

另外, 对于给定的 $A \in B_{\text{her}}(\mathcal{H}^{(n)})$, 令

$$C_A = \max_{\rho \in \mathcal{P}} \langle A\rangle_\rho,$$

于是, 有 $C_A \leqslant \lambda_{\max}(A)$.

当 $C_A < \lambda_{\max}(A)$ 时, 我们给出构造纠缠目击的一般方法.

定理1 设 $A \in B_{\text{her}}(\mathcal{H}^{(n)})$, $\lambda_{\max}(A)$ 为 A 的最大特征值, 且 $C_A \leqslant C < \lambda_{\max}(A)$, 则

1) $W_C = CI - A$ 是纠缠目击;

2) 当 $|\psi\rangle \in S(\mathcal{H}^{(n)})$ 满足条件 $A|\psi\rangle = \lambda|\psi\rangle$ $(C < \lambda)$ 时, W_C 可以探测 $|\psi\rangle\langle\psi|$;

3) 当 $\rho \in D(\mathcal{H}^{(n)})$ 满足条件 $A\rho = \lambda\rho (C < \lambda)$ 时, W_C 可以探测 ρ.

证明 1) 当 $\rho \in \mathcal{P}$ 时, 由 C_A 的定义知

$$\text{tr}(W_C\rho) = C - \text{tr}(A\rho) = C - \langle A\rangle_\rho \geqslant C_A - \langle A\rangle_\rho \geqslant 0,$$

从而, 当 ρ 完全可分时, $\mathrm{tr}(W_C\rho) \geqslant 0$. 设 A 的最大特征值 $\lambda_{\max}(A)$ 所对应的特征态为 $|\psi_{\max}\rangle$, 则

$$\begin{aligned}&\mathrm{tr}(W_C|\psi_{\max}\rangle\langle\psi_{\max}|)\\ =\ & C - \mathrm{tr}(A|\psi_{\max}\rangle\langle\psi_{\max}|) = C - \lambda_{\max}(A) < 0.\end{aligned}$$

可见, W_C 是纠缠目击且可以探测 $|\psi_{\max}\rangle\langle\psi_{\max}|$.

2) 当存在 $|\psi\rangle \in S(\mathcal{H}^{(n)})$ 使得 $A|\psi\rangle = \lambda|\psi\rangle$ $(C < \lambda)$ 时, 有

$$\mathrm{tr}(W_C|\psi\rangle\langle\psi|) = C - \mathrm{tr}(A|\psi\rangle\langle\psi|) = C - \lambda < 0.$$

可见, $|\psi\rangle\langle\psi|$ 是纠缠态且可以被 W_C 探测.

3) 当 $\rho \in D(\mathcal{H}^{(n)})$ 满足 $A\rho = \lambda\rho(C < \lambda)$ 时, 有

$$\mathrm{tr}(W_C\rho) = C - \mathrm{tr}(A\rho) = C - \lambda < 0.$$

可见, ρ 是纠缠态且可以被 W_C 探测.

注1 由定理1知:

1) 介于 C 与 $\lambda_{\max}(A)$ 之间的所有特征值 $\lambda(C < \lambda \leqslant \lambda_{\max}(A))$ 所对应的特征态 $|\psi\rangle$ 都是纠缠的, 并且这些纠缠态都可以被 $W_C = CI - A(C_A \leqslant C < \lambda_{\max}(A))$ 探测到.

2) 由 W_C 探测到的那些纠缠态进行凸组合后得到的混合态也是纠缠的, 并且仍然可以由 W_C 探测到.

3) 对于某些自伴算子 A, 确实存在 $\rho \in D(\mathcal{H}^{(n)})$ 满足 $A\rho = \lambda\rho(C < \lambda)$. 例如, 当 A 有两个特征态 $|\psi_1\rangle$,$|\psi_2\rangle$ 满足条件

$$A|\psi_i\rangle = \lambda|\psi_i\rangle (i = 1, 2)\ (C < \lambda)$$

时, 令

$$\rho = t|\psi_1\rangle\langle\psi_1| + (1 - t)|\psi_2\rangle\langle\psi_2|(t \in (0, 1)),$$

则 $A\rho = \lambda\rho$.

4) 若自伴算子 A 的特征值 λ 所对应的特征态 $|\psi\rangle$ 都是可分态, 则称此 λ 为可分特征值, 否则称为纠缠特征值. 如图1, 在数轴上, 可分特征值 λ_{s} 都分布在 C_A 的左侧, 即 $\lambda_{\mathrm{s}} \leqslant C_A$. 若存在一个纠缠特征值 λ_{e} 满足 $C_A < \lambda_{\mathrm{e}} \leqslant \lambda_{\max}(A)$, 则 λ_{e} 右边的所有特征值都是纠缠特征值. 但是 C_A 的左侧有可能存在纠缠特征值. 例如, 若 $A = \boldsymbol{X} \otimes \boldsymbol{X}$($\boldsymbol{X}$ 为Pauli阵), 则 $\lambda_{\min}(A) = -1, \lambda_{\max}(A) = 1$, 于是 $-1 \leqslant C_A \leqslant 1$. 因为

$$C_A = \max_{\rho\in\mathcal{P}}\langle A\rangle_\rho = \langle \boldsymbol{X} \otimes \boldsymbol{X}\rangle_{|+\rangle\langle+|\otimes|+\rangle\langle+|} = 1,$$

其中

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

所以特征值 $\lambda_{\min}(A) = -1$ 位于 C_A 的左侧, 但是它所对应的特征态 $(|00\rangle - |11\rangle)/\sqrt{2}$ 与 $(|01\rangle - |10\rangle)/\sqrt{2}$ 都是纠缠的. 这说明 C_A 的左侧有可能存在纠缠特征值.

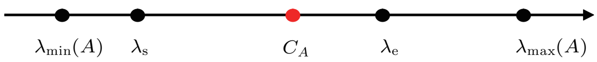

图1 可分特征值与部分纠缠特征值的分布示意图

Fig. 1. Distribution schematic of separable eigenvalues and entangled eigenvalues.

注2 设 W 是纠缠目击, 且 $f(\rho) < 0$, 其中 $f(\rho) := \mathrm{tr}(W\rho)(\rho \in D(\mathcal{H}^{(n)}))$ 是连续函数, 从而存在 $\delta > 0$, 使得 $\forall\sigma \in D(\mathcal{H}^{(n)})$, 当 $\|\sigma - \rho\| < \delta$ 时, 有 $f(\sigma) < 0$, 从而 σ 是纠缠态. 因此如果 W 可以探测 ρ, 那么 W 也可以探测到 ρ 周围的纠缠态 σ.

容易看出: 对于给定的纠缠目击 W 和它能探测的纠缠态 ρ, δ 的取法并不唯一. 特别地, 我们可以给出 δ 的一个取法, 取 $\delta = -f(\rho)/\|W\|_1$, 当 $\|\sigma - \rho\| < \delta$ 时, 有 $f(\sigma) < 0$, 从而 σ 是纠缠态. 事实上, $\delta = -f(\rho)/\|W\|_1$ 可由

$$\begin{aligned}f(\sigma) =\ & \mathrm{tr}(W(\sigma - \rho)) + f(\rho)\\ \leqslant\ & \|W\|_1\|\sigma - \rho\| + f(\rho) < 0\end{aligned}$$

得到, 其中 $\|W\|_1 = \mathrm{tr}\sqrt{W^\dagger W}$, $\|\cdot\| = \|\cdot\|_\infty$. 对于给定的纠缠目击 W 和它能探测的纠缠态 ρ, 不同的 δ 反映出纠缠目击可以探测到 ρ 的不同范围内的纠缠态.

对于不同的纠缠目击, 它们探测到的量子态会有所不同. 下面我们由纠缠目击探测到的量子态之集给出较优纠缠目击的定义.

给定纠缠目击 W. 令

$$D_W = \{\rho \in D(\mathcal{H}^{(n)}) : \mathrm{tr}(W\rho) < 0\},$$

即纠缠目击 W 所能探测到的所有量子态.

定义3[13] 设 W_1, W_2 是纠缠目击, 若 $D_{W_2} \subseteq D_{W_1}$, 则称 W_1 比 W_2 优.

定义4[13] 设 W 是纠缠目击, 若没有其他纠缠目击比 W 优, 则称 W 是最优纠缠目击.

引理1[13] 设 W_1, W_2 是纠缠目击, W_1 比 W_2 优当且仅当存在正数 ε 和不为0的正算子 P 使得 $W_2 = (1 - \varepsilon)W_1 + \varepsilon P$.

在定理1中, 当 $C_A \leqslant C < \lambda_{\max}(A)$ 时, $W_C = CI - A$(C 是参数)是一类纠缠目击, 对于这类纠缠目击, 很容易得到较优的纠缠目击.

定理2　设 $A \in B_{\mathrm{her}}(\mathcal{H}^{(n)})$, $\lambda_{\max}(A)$ 为 A 的最大特征值, 且 $C_A < C < \lambda_{\max}(A)$, 则 W_{C_A} 优于 W_C.

证明　利用引理1, 要证 W_{C_A} 优于 W_C, 只需要证存在正数 ε 和不为0的正算子 P 使得

$$W_C = (1-\varepsilon)W_{C_A} + \varepsilon P. \tag{1}$$

因为 $W_C = CI - A, W_{C_A} = C_A I - A$, 所以将 W_C 与 W_{C_A} 代入(1)式得

$$P = \frac{C - C_A}{\varepsilon} I + W_{C_A}.$$

要使 P 是正算子, 只需要 $\dfrac{C - C_A}{\varepsilon} > \|W_{C_A}\|$. 因此, 取

$$\varepsilon = \frac{C - C_A}{2\|W_{C_A}\|},\quad P = \frac{C - C_A}{\varepsilon} I + W_{C_A},$$

有 $W_C = (1-\varepsilon)W_{C_A} + \varepsilon P$. 从而, 由引理1知, 当 $C_A < C < \lambda_{\max}(A)$ 时, W_{C_A} 优于 W_C.

注3　定理2表明: 在形如 $W_C = CI - A(C_A \leqslant C < \lambda_{\max}(A))$($C$ 是参数)的纠缠目击中, W_{C_A} 是最优纠缠目击, 即对于任意的 $C(C_A < C < \lambda_{\max}(A))$ 有 W_{C_A} 优于 W_C.

注4　由定理1知: 介于 C_A 与 $\lambda_{\max}(A)$ 之间的所有特征值 $\lambda(C_A < \lambda \leqslant \lambda_{\max}(A))$ 所对应的特征态 $|\psi\rangle$ 都是纠缠的, 并且这些纠缠态都可以由 W_{C_A} 探测到. 但是 $W_C(C_A < C < \lambda_{\max}(A))$ 只能探测到介于 C 与 $\lambda_{\max}(A)$ 之间的所有特征值 $\lambda(C < \lambda \leqslant \lambda_{\max}(A))$ 所对应的特征态 $|\psi\rangle$. 由此间接地说明了 W_{C_A} 探测到的纠缠态比 W_C 探测到的纠缠态多, 因此, W_{C_A} 优于 W_C.

注5　若纠缠目击 $W_C, W_{C_A}(C_A < C < \lambda_{\max}(A))$ 都能探测到态 ρ, 由注2可知, 当

$$\|\sigma - \rho\| < \frac{-\operatorname{tr}(W_C\rho)}{\|W_C\|_1}$$

时, 纠缠目击 W_C 可以探测到满足此条件的纠缠态 σ, 而当

$$\|\sigma - \rho\| < \frac{-\operatorname{tr}(W_{C_A}\rho)}{\|W_{C_A}\|_1}$$

时, 纠缠目击 W_{C_A} 可以探测到满足此条件的纠缠态 σ. 计算可得

$$-\operatorname{tr}(W_C\rho) = \operatorname{tr}(A\rho) - C,$$
$$-\operatorname{tr}(W_{C_A}\rho) = \operatorname{tr}(A\rho) - C_A.$$

因为 $C_A < C$, 所以

$$-\operatorname{tr}(W_C\rho) < -\operatorname{tr}(W_{C_A}\rho),\quad \|W_C\|_1 > \|W_{C_A}\|_1.$$

从而

$$\frac{-\operatorname{tr}(W_C\rho)}{\|W_C\|_1} < \frac{-\operatorname{tr}(W_{C_A}\rho)}{\|W_{C_A}\|_1}.$$

这说明 W_{C_A} 探测到 ρ 周围的态比 W_C 探测到 ρ 周围的态多. 这又从另一方面说明了 W_{C_A} 优于 W_C.

注6　虽然 W_{C_A} 探测到的态比 W_C 多, 但是在具体问题中, 计算 C_A 的精确值是特别困难的, 而估计 C_A 的范围是比较容易的, 那么我们可以退而求其次, 构造纠缠目击 W_C.

3　图态的纠缠目击的构造

图态, 顾名思义, 是一类可以通过数学图形以简洁直观并且有效的方式进行刻画的特殊量子纠缠态. 图态的描述方式不同, 与之相对应的定义方式也不尽相同. 下面给出图态的稳定化算子形式的定义.

定义5[32]　设 V 是一个有限集, E 是 V 的二元素子集, 称 $G = (V, E)$ 是一个(无向有限)图. 并且 V 中的元素称为图 G 的顶点, V 称为图 G 的顶点集, 常用 $\{1, 2, \cdots, n\}$ 表示. E 中的元素可以视为连接相应顶点的边, 且 E 称为图 G 的边集. 对于顶点 $i \in V$, 用 $N(i)$ 表示与顶点 i 相连的顶点之集, 称为 i 的邻域.

若 $\mathcal{H}^{(n)}$ 为Hilbert空间 $\mathbb{C}^2$ 的 n 重张量积, 即

$$\mathcal{H}^{(n)} = \underbrace{\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}_{n}.$$

对2阶矩阵 $T_1, T_2, \cdots, T_n$(视为Hilbert空间 $\mathbb{C}^2$ 上的线性算子), 用 $\bigotimes_{k=1}^{n} T_k$ 表示它们的张量积($\mathcal{H}^{(n)}$ 上的算子), 即

$$\bigotimes_{k=1}^{n} T_k = T_1 \otimes T_2 \otimes \cdots \otimes T_n.$$

特别是当 $T_i = T, T_j = I(j \neq i)$ 时, 将张量积算子 $\bigotimes_{k=1}^{n} T_k$ 简记为 $T^{(i)}$. 例如, 当 $\boldsymbol{X}, \boldsymbol{Z}$ 为Pauli矩阵:

$$\boldsymbol{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\quad \boldsymbol{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

时, 有

$$X^{(i)} = \boldsymbol{I} \otimes \cdots \otimes \boldsymbol{I} \otimes \underbrace{\boldsymbol{X}}_{i} \otimes \boldsymbol{I} \otimes \cdots \otimes \boldsymbol{I},$$

$$Z^{(i)} = \boldsymbol{I} \otimes \cdots \otimes \boldsymbol{I} \otimes \underbrace{\boldsymbol{Z}}_{i} \otimes \boldsymbol{I} \otimes \cdots \otimes \boldsymbol{I},$$

其中$\boldsymbol{I}$为2阶单位阵. 显然, 对任意的i, j, $Z^{(i)}$与$Z^{(j)}$可交换: $Z^{(i)}Z^{(j)} = Z^{(j)}Z^{(i)}$, 且$X^{(i)}$与$X^{(j)}$可交换: $X^{(i)}X^{(j)} = X^{(j)}X^{(i)}$. 当$i \neq j$时, $X^{(i)}$与$Z^{(j)}$可交换: $X^{(i)}Z^{(j)} = Z^{(j)}X^{(i)}$. 这就保证了下面的算子$S_i$定义合理.

定义6[32] 给定一个图$G = (V, E)$, 顶点个数即V的元素个数为n, 对该图的任意一个顶点i, 定义算子

$$S_i = X^{(i)} \prod_{j \in N(i)} Z^{(j)}, \tag{2}$$

其中, 当$N(i) = \emptyset$时, 规定$S_i = X^{(i)}$; 并称S_1, $S_2, \cdots$, S_n为图$G = (V, E)$的稳定化算子.

注7 由定义6可知: $\forall i, j \in V$, 有$[S_i, S_j] = 0$.

定义7[32] 给定一个具有n个顶点的图$G = (V, E)$, 称满足条件

$$S_i|G\rangle = |G\rangle (\forall i = 1, 2, \cdots, n) \tag{3}$$

的n-体态$|G\rangle \in S(\mathcal{H}^{(n)})$为图$G = (V, E)$的图态.

可以证明[33]: 图态存在且唯一, 其解析式为

$$|G\rangle = \prod_{(a,b)\in E} U^{\{a,b\}} \underbrace{|+\rangle|+\rangle\cdots|+\rangle|+\rangle}_{n},$$

其中

$$U^{\{a,b\}} = P^{(a)}_{Z,+} + P^{(a)}_{Z,-}Z^{(b)},$$
$$P^{(a)}_{Z,\pm} = \frac{I \pm Z^{(a)}}{2},$$
$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle).$$

由此可得: 如图2, 具有n个顶点的空图(任意两点都不相连)所对应的图态为$\underbrace{|+\rangle|+\rangle\cdots|+\rangle|+\rangle}_{n}$. 如图3, 具有$n$个顶点的图中只有1, 2顶点相连, 此图所对应的图态为

$$\begin{aligned}|G\rangle &= U^{\{1,2\}}\underbrace{|+\rangle|+\rangle\cdots|+\rangle|+\rangle}_{n}\\ &= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)\underbrace{|+\rangle|+\rangle\cdots|+\rangle|+\rangle}_{n-2}\\ &= \frac{1}{\sqrt{2}}(|\beta_{01}\rangle + |\beta_{10}\rangle)\underbrace{|+\rangle|+\rangle\cdots|+\rangle|+\rangle}_{n-2},\end{aligned}$$

其中

$$|\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle),$$
$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle).$$

定义8[32] 给定一个具有n个顶点的图$G = (V, E)$, 由稳定化算子$S_1, S_2, \cdots, S_n$生成的交换群

$$\widetilde{S} = \langle S_1, S_2, \cdots, S_n\rangle$$

称为图$G = (V, E)$的稳定子.

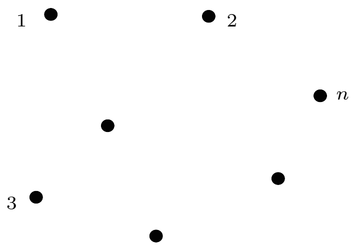

图2 空图

Fig. 2. Empty graph.

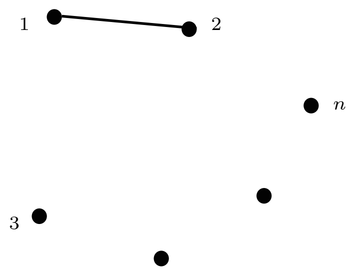

图3 只有1, 2顶点相连的图

Fig. 3. A graph connected by a 1,2 vertex.

注8 $\widetilde{S}$有2^n个元素, 可以表示为

$$\widetilde{S} = \{\widetilde{S}_j : j = 1, 2, \cdots, 2^n\},$$

其中

$$\widetilde{S}_j = \prod_{i \in I_j} S_i = O^1_j \otimes \cdots \otimes O^n_j, \tag{4}$$

其中I_j是V的子集, $O^k_j \in \{I, \pm X, \pm Y, \pm Z\}$.

容易得到$\widetilde{S}_j|G\rangle = |G\rangle (j = 1, 2, \cdots, 2^n)$, 即$|G\rangle$为$\widetilde{S}$中每一个元素的不动点. 进一步可以得出: $|G\rangle$是$\widetilde{S}$中元素进行线性组合以后所得算子的特征态.

注9[32] 可以证明

$$\sum_{j=1}^{2^n} \widetilde{S}_j = 2^n |G\rangle\langle G|.$$

给定一个具有n个顶点的图$G = (V, E)$, $S_i (i = 1, 2, \cdots, n)$为图$G$的稳定化算子, $\widetilde{S}$为图G的稳定子, $|G\rangle$为图G的图态. 下面探讨图态的纠缠目击的构造. 着重讨论使用稳定子的元素构造一类纠缠目击来探测图态周围的纠缠态. 这类纠缠目击我们称为稳定子目击.

若在定理1中取A为$\widetilde{S}$中的某一个元素$\widetilde{S}_j$. 图态$|G\rangle\langle G|$能被形如$W_C=CI-\widetilde{S}_j(\widetilde{S}_j\in\widetilde{S})$的纠缠目击探测吗?

我们构造的纠缠目击是基于满足条件$C_A\leqslant C<\lambda_{\max}(A)$的$C$的存在性. 若$C_A=\lambda_{\max}(A)$, 则不存在满足条件的$C$, 也就构造不了$W_C$. 例如: 当$A=\widetilde{S}_j$时, 由于$A$是自伴算子, 且它的最大特征值$\lambda_{\max}(A)=1$, 相应的特征态为$|G\rangle$, 所以$C_A\leqslant 1$. 由注8知, 可设$\widetilde{S}_j=O_j^1\otimes\cdots\otimes O_j^n$, 其中$O_j^k\in\{I,\pm X,\pm Y,\pm Z\}$. 取$O_j^k$的特征值为1的特征态为$|\psi^0\rangle_k(k=1,2,\cdots,n)$, 令$\rho_k^0=|\psi^0\rangle_{kk}\langle\psi^0|, k=1,2,\cdots,n$. 容易计算

$$\begin{aligned}C_A&=\max_{\rho=\rho_1\otimes\cdots\otimes\rho_n\in\mathcal{P}}\langle\widetilde{S}_j\rangle_\rho\\&=\max_{\rho=\rho_1\otimes\cdots\otimes\rho_n\in\mathcal{P}}\prod_{k=1}^n\langle O_j^k\rangle_{\rho_k}\\&=\prod_{k=1}^n\langle O_j^k\rangle_{\rho_k^0}=1.\end{aligned}$$

因此$C_A=\lambda_{\max}(A)$. 于是, 满足$C_A\leqslant C<\lambda_{\max}(A)$的$C$不存在, 可知图态$|G\rangle\langle G|$不能被形如$W_C=CI-\widetilde{S}_j(\widetilde{S}_j\in\widetilde{S})$的纠缠目击探测.

若在定理1中取A为$\widetilde{S}$中任意两个元素做线性组合以后得到的算子, 情况会如何呢? 也就是图态$|G\rangle\langle G|$能被形如W_C的纠缠目击探测吗? 为了简单起见, 不妨取$A=\widetilde{S}_i+\widetilde{S}_j(\widetilde{S}_i\neq\widetilde{S}_j,\widetilde{S}_i,\widetilde{S}_j\in\widetilde{S})$. 由于讨论的需要, 给出下面的定义与结论.

定义9[20]　设自伴算子

$$\begin{aligned}K&=K^{(1)}\otimes K^{(2)}\otimes\cdots\otimes K^{(n)},\\L&=L^{(1)}\otimes L^{(2)}\otimes\cdots\otimes L^{(n)}.\end{aligned}$$

若$K^{(i)}L^{(i)}=L^{(i)}K^{(i)}(\forall i=1,2,\cdots,n)$, 则称$K$与$L$是局域交换的.

在一般的图$G=(V,E)$中, 相连的两个顶点所对应的稳定化算子不是局域交换的, 不相连的两个顶点所对应的稳定化算子是局域交换的. 因此, 对于一般的图$G=(V,E)$来说, $\widetilde{S}_i$与$\widetilde{S}_j$可能是局域交换的, 也可能不是局域交换的. 例如, 在图4中, S_1与S_2是局域交换的, S_1与S_3不是局域交换的.

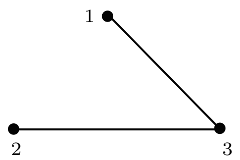

图4　图G

Fig. 4.　Graph G.

注10　由定义可知: $\widetilde{S}_i=O_i^1\otimes\cdots\otimes O_i^n$与$\widetilde{S}_j=O_j^1\otimes\cdots\otimes O_j^n$是局域交换的, 当且仅当对任一$k=1,2,\cdots,n$, 要么$O_i^k=\pm O_j^k$, 要么$O_i^k$与$O_j^k$中至少有一个为$I$.

引理2[20]　两个自伴算子

$$\begin{aligned}K&=K^{(1)}\otimes K^{(2)}\otimes\cdots\otimes K^{(n)},\\L&=L^{(1)}\otimes L^{(2)}\otimes\cdots\otimes L^{(n)}\end{aligned}$$

是局域交换的, 当且仅当K和L有一组共同的纯的乘积特征态构成空间$\mathcal{H}^{(n)}$的基.

在定理1中, 当$A=\widetilde{S}_i+\widetilde{S}_j(\widetilde{S}_i\neq\pm\widetilde{S}_j,\widetilde{S}_i,\widetilde{S}_j\in\widetilde{S})$且$\widetilde{S}_i$与$\widetilde{S}_j$局域交换时, 有$C_A=\lambda_{\max}(A)=2$. 于是, 满足$C_A\leqslant C<\lambda_{\max}(A)$的$C$不存在, 可知图态$|G\rangle\langle G|$不能被形如$W_C=CI-\widetilde{S}_i-\widetilde{S}_j(\widetilde{S}_i\neq\pm\widetilde{S}_j,\widetilde{S}_i,\widetilde{S}_j\in\widetilde{S})$的纠缠目击探测. 事实上, 由于$A$是自伴算子, 且它的最大特征值$\lambda_{\max}(A)=2$, 相应的特征态为$|G\rangle$, 所以$C_A\leqslant 2$. 若$\widetilde{S}_i$与$\widetilde{S}_j$是局域交换的, 由引理2知, $\widetilde{S}_i$与$\widetilde{S}_j$有一组共同的纯的乘积特征态构成空间$\mathcal{H}^{(n)}$的基. 又因为$\widetilde{S}_i\neq\pm\widetilde{S}_j$, 所以取$\widetilde{S}_i$与$\widetilde{S}_j$的特征值均为1的那个纯的乘积特征态为$|\psi^0\rangle$. 令$\rho^0=|\psi^0\rangle\langle\psi^0|$. 计算可得

$$C_A=\max_{\rho=\rho_1\otimes\cdots\otimes\rho_n\in\mathcal{P}}\langle\widetilde{S}_i+\widetilde{S}_j\rangle_\rho=\langle\widetilde{S}_i+\widetilde{S}_j\rangle_{\rho^0}=2,$$

因此$C_A=\lambda_{\max}(A)=2$. 但是当$\widetilde{S}_i$与$\widetilde{S}_j$不是局域交换时, 结果有所不同. 可得如下结论.

推论1　设

$$A=\widetilde{S}_i+\widetilde{S}_j(\widetilde{S}_i,\widetilde{S}_j\in\widetilde{S}),$$

且$\widetilde{S}_i$与$\widetilde{S}_j$不是局域交换的, 则$C_A<2$且

$$W_C=CI-\widetilde{S}_i-\widetilde{S}_j(C_A\leqslant C<2)$$

是一个纠缠目击, 能探测图态$|G\rangle\langle G|$.

证明　由注8知, 可设

$$\widetilde{S}_i=O_i^1\otimes\cdots\otimes O_i^n,\quad\widetilde{S}_j=O_j^1\otimes\cdots\otimes O_j^n,$$

其中$O_i^k,O_j^k\in\{I,\pm X,\pm Y,\pm Z\}$. 因为$\widetilde{S}_i$与$\widetilde{S}_j$不是局域交换的, 所以存在$k_0\in\{1,2,\cdots,n\}$使得$O_i^{k_0}$与$O_j^{k_0}$不可换. 由于$A$是自伴算子, 且它的最大特征值$\lambda_{\max}(A)=2$, 相应的特征态为$|G\rangle$, 所以$C_A\leqslant 2$. 下证$C_A\neq 2$. 反证法. 若$C_A=2$, 则存在纯的乘积态$\rho_0=|\psi_1\rangle\langle\psi_1|\otimes\cdots\otimes|\psi_n\rangle\langle\psi_n|$使得$\langle\widetilde{S}_i+\widetilde{S}_j\rangle_{\rho_0}=2$. 于是, 计算可得

$$\begin{aligned}\langle\widetilde{S}_i+\widetilde{S}_j\rangle_{\rho_0}=&\langle O_i^1\rangle_{|\psi_1\rangle\langle\psi_1|}\cdots\langle O_i^n\rangle_{|\psi_n\rangle\langle\psi_n|}\\&+\langle O_j^1\rangle_{|\psi_1\rangle\langle\psi_1|}\cdots\langle O_j^n\rangle_{|\psi_n\rangle\langle\psi_n|}=2.\end{aligned}$$

由于

$$-1 \leqslant \langle O_i^k \rangle_{|\psi_k\rangle\langle\psi_k|} \leqslant 1, -1 \leqslant \langle O_j^k \rangle_{|\psi_k\rangle\langle\psi_k|} \leqslant 1,$$

$k = 1, 2, \cdots, n$, 所以

$$\begin{aligned} & \langle O_i^1 \rangle_{|\psi_1\rangle\langle\psi_1|} \cdots \langle O_i^n \rangle_{|\psi_n\rangle\langle\psi_n|} \\ = \ & \langle O_j^1 \rangle_{|\psi_1\rangle\langle\psi_1|} \cdots \langle O_j^n \rangle_{|\psi_n\rangle\langle\psi_n|} = 1. \end{aligned}$$

因此, $\forall k = 1, 2, \cdots$, 我们有

$$\langle O_i^k \rangle_{|\psi_k\rangle\langle\psi_k|} = \pm 1, \langle O_j^k \rangle_{|\psi_k\rangle\langle\psi_k|} = \pm 1.$$

特别地,

$$\langle O_i^{k_0} \rangle_{|\psi_{k_0}\rangle\langle\psi_{k_0}|} = \pm 1, \quad \langle O_j^{k_0} \rangle_{|\psi_{k_0}\rangle\langle\psi_{k_0}|} = \pm 1.$$

由此可见, $O_i^{k_0}$ 与 $O_j^{k_0}$ 有共同的特征态 $|\psi_{k_0}\rangle$. 又因为 $O_i^{k_0}, O_j^{k_0} \in \{I, \pm X, \pm Y, \pm Z\}$, 从而算子组 $\{O_i^{k_0}, O_j^{k_0}\}$ 必为

$$\{I, \pm X\}, \{I, \pm Y\}, \{I, \pm Z\}$$

之一. 不论哪种情况, $O_i^{k_0}$ 与 $O_j^{k_0}$ 都可交换. 这与 $O_i^{k_0}$ 和 $O_j^{k_0}$ 不交换矛盾. 故 $C_A < 2$. 于是, 满足条件 $C_A \leqslant C < \lambda_{\max}(A) = 2$ 的 C 存在, 由定理1知,

$$W_C = CI - \widetilde{S}_i - \widetilde{S}_j (C_A \leqslant C < 2)$$

是一个纠缠目击, 且能探测图态 $|G\rangle\langle G|$.

注11 由推论1知, 若 $\widetilde{S}_i$ 与 $\widetilde{S}_j$ 不是局域交换的, 则图态 $|G\rangle\langle G|$ 及其周围态能被形如 $W_C = CI - \widetilde{S}_i - \widetilde{S}_j (C_A \leqslant C < 2)$ 的纠缠目击探测. 例如, 令

$$\rho = \frac{1}{2^n}(I + \widetilde{S}_i + \widetilde{S}_j + \widetilde{S}_i \widetilde{S}_j).$$

容易计算 $\mathrm{tr}(W_C \rho) = C - 2 < 0$. 因此, 纠缠目击 $W_C = CI - \widetilde{S}_i - \widetilde{S}_j$ 能探测量子态

$$\rho = \frac{1}{2^n}(I + \widetilde{S}_i + \widetilde{S}_j + \widetilde{S}_i \widetilde{S}_j).$$

进一步, 可以构造更一般的态

$$\rho' = \frac{1}{2^n}(I + a_1 \widetilde{S}_i + a_2 \widetilde{S}_j + a_1 a_2 \widetilde{S}_i \widetilde{S}_j).$$

其中 $-1 \leqslant a_i \leqslant 1 (i = 1, 2), a_1 + a_2 > C$. 类似可证: 纠缠目击 $W_C = CI - \widetilde{S}_i - \widetilde{S}_j$ 能探测量子态 ρ'.

特别地, 在推论1中, 当 $\widetilde{S}_i$ 与 $\widetilde{S}_j$ 分别取稳定化算子 S_i, S_j 时, 若 S_i 与 S_j 是局域交换的, 则图态 $|G\rangle\langle G|$ 不能被形如 $W_C = CI - S_i - S_j$ 的纠缠目击探测; 若 S_i 与 S_j 不是局域交换的, 则有下列推论.

推论2 设 $A = S_i + S_j$, 且 S_i 与 S_j 不是局域交换的, 则 $C_A \leqslant 1$ 且 $W_C = CI - S_i - S_j (1 \leqslant C < 2)$ 是一个纠缠目击, 且能探测图态 $|G\rangle\langle G|$.

证明 在推论1中, 令 $\widetilde{S}_i = S_i, \widetilde{S}_j = S_j$. 若 S_i 与 S_j 不是局域交换的, 则图态 $|G\rangle\langle G|$ 能被形如 $W_C = CI - S_i - S_j$ 的纠缠目击探测, 其中 $C_A \leqslant C < 2$. 由于 S_i, S_j 为图 $G = (V, E)$ 的稳定化算子, 所以有

$$S_i = X^{(i)} \prod_{k \in N(i)} Z^{(k)},$$

$$S_j = X^{(j)} \prod_{k \in N(j)} Z^{(k)}.$$

若 S_i 与 S_j 不是局域交换的, 则顶点 i 与 j 相连, 即 $\{i, j\} \in E$, 因此 $j \in N(i), i \in N(j)$. 当 $\rho = \rho_1 \otimes \cdots \otimes \rho_n \in \mathcal{P}$ 时, 计算可得

$$\begin{aligned} & \langle S_i + S_j \rangle_\rho \\ = \ & \left\langle X^{(i)} \prod_{k \in N(i)} Z^{(k)} + X^{(j)} \prod_{k \in N(j)} Z^{(k)} \right\rangle_\rho \\ \leqslant \ & |\langle X \rangle_{\rho_i}| \cdot \prod_{k \in N(i)} |\langle Z \rangle_{\rho_k}| + |\langle X \rangle_{\rho_j}| \cdot \prod_{k \in N(j)} |\langle Z \rangle_{\rho_k}| \\ \leqslant \ & |\langle X \rangle_{\rho_i}| |\langle Z \rangle_{\rho_j}| + |\langle Z \rangle_{\rho_i}| |\langle X \rangle_{\rho_j}| \\ \leqslant \ & \sqrt{|\langle X \rangle_{\rho_i}|^2 + |\langle Z \rangle_{\rho_i}|^2} \sqrt{|\langle Z \rangle_{\rho_j}|^2 + |\langle X \rangle_{\rho_j}|^2} \\ \leqslant \ & 1. \end{aligned}$$

从而

$$C_A = \max_{\rho = \rho_1 \otimes \cdots \otimes \rho_n \in \mathcal{P}} \langle S_i + S_j \rangle_\rho \leqslant 1. \tag{5}$$

因此, 当 $1 \leqslant C < 2$ 时, 纠缠目击 $W_C = CI - S_i - S_j$ 是一个纠缠目击, 且能探测图态 $|G\rangle\langle G|$.

注12 在推论2中令 $C = 1, S_i = S_1$, 则 $W_1 = I - S_1 - S_j$ 为文献[20]中提到的可以探测图态 $|G\rangle\langle G|$ 的纠缠目击. 而我们构造的纠缠目击 W_C 是一类探测图态 $|G\rangle\langle G|$ 的纠缠目击, 包含 W_1.

在定理1中取 A 为 $\widetilde{S}$ 中任意三个元素做线性组合以后得到的算子, 情况会如何呢? 也就是图态 $|G\rangle\langle G|$ 能被形如 W_C 的纠缠目击探测吗? 为了简单起见, 不妨取 $A = \widetilde{S}_i + \widetilde{S}_j + \widetilde{S}_m (\widetilde{S}_i, \widetilde{S}_j, \widetilde{S}_m \in \widetilde{S})$.

在定理1中, 当 $A = \widetilde{S}_i + \widetilde{S}_j + \widetilde{S}_m$ 且 $\widetilde{S}_i, \widetilde{S}_j, \widetilde{S}_m$ 是两两局域交换时, 由于 A 是自伴算子, 且它的最大特征值 $\lambda_{\max}(A) = 3$, 相应的特征态为 $|G\rangle$, 所以 $C_A \leqslant 3$. 由注8知, 可设

$$\widetilde{S}_i = O_i^1 \otimes \cdots \otimes O_i^n,$$

$$\widetilde{S}_j = O_j^1 \otimes \cdots \otimes O_j^n,$$

$$\widetilde{S}_m = O_m^1 \otimes \cdots \otimes O_m^n,$$

其中$O_i^k, O_j^k, O_m^k \in \{I, \pm X, \pm Y, \pm Z\}$. 由于$\widetilde{S}_i$, $\widetilde{S}_j$, $\widetilde{S}_m$是两两局域交换的, 所以$\forall k \in \{1, 2, \cdots, n\}$, 有

$$\begin{aligned} O_i^k O_j^k &= O_j^k O_i^k, \\ O_i^k O_m^k &= O_m^k O_i^k, \\ O_m^k O_j^k &= O_j^k O_m^k. \end{aligned}$$

利用引理2容易知道$\widetilde{S}_i, \widetilde{S}_j, \widetilde{S}_m$有一组共同的纯的乘积特征态构成空间$\mathcal{H}^{(n)}$的基. 若存在纯的乘积特征态使得$\widetilde{S}_i, \widetilde{S}_j, \widetilde{S}_m$的特征值均为1, 则取$\widetilde{S}_i, \widetilde{S}_j, \widetilde{S}_m$的特征值均为1的纯的乘积特征态为$|\psi^0\rangle$. 令$\rho^0 = |\psi^0\rangle\langle\psi^0|$. 计算可得

$$\begin{aligned} C_A &= \max_{\rho=\rho_1\otimes\cdots\otimes\rho_n\in\mathcal{P}} \langle \widetilde{S}_i + \widetilde{S}_j + \widetilde{S}_m \rangle_\rho \\ &= \langle \widetilde{S}_i + \widetilde{S}_j + \widetilde{S}_m \rangle_{\rho^0} = 3, \end{aligned}$$

因此$C_A = \lambda_{\max}(A) = 3$. 于是, 满足$C_A \leqslant C < \lambda_{\max}(A)$的$C$不存在, 可知图态$|G\rangle\langle G|$不能被形如$W_C = CI - \widetilde{S}_i - \widetilde{S}_j - \widetilde{S}_m$的纠缠目击探测. 但是当$\widetilde{S}_i, \widetilde{S}_j, \widetilde{S}_m$不是两两局域交换时, 结果有所不同, 可得如下结论.

推论3 设

$$A = \widetilde{S}_i + \widetilde{S}_j + \widetilde{S}_m (\widetilde{S}_i, \widetilde{S}_j, \widetilde{S}_m \in \widetilde{S}),$$

且$\widetilde{S}_i, \widetilde{S}_j, \widetilde{S}_m$不是两两局域交换的, 则$C_A < 3$且

$$W_C = CI - \widetilde{S}_i - \widetilde{S}_j - \widetilde{S}_m (C_A \leqslant C < 3)$$

是一个纠缠目击, 且能探测图态$|G\rangle\langle G|$.

证明 由注8知, 可设

$$\begin{aligned} \widetilde{S}_i &= O_i^1 \otimes \cdots \otimes O_i^n, \\ \widetilde{S}_j &= O_j^1 \otimes \cdots \otimes O_j^n, \\ \widetilde{S}_m &= O_m^1 \otimes \cdots \otimes O_m^n, \end{aligned}$$

其中$O_i^k, O_j^k, O_m^k \in \{I, \pm X, \pm Y, \pm Z\}$. 因为$\widetilde{S}_i, \widetilde{S}_j, \widetilde{S}_m$不是两两局域交换的, 所以存在$k_0 \in \{1, 2, \cdots, n\}$使得$O_i^{k_0}$,$O_j^{k_0}$, $O_m^{k_0}$不两两可换. 由于A是自伴算子, 且它的最大特征值$\lambda_{\max}(A) = 3$, 相应的特征态为$|G\rangle$, 所以$C_A \leqslant 3$. 下证$C_A \neq 3$. 反证法. 若$C_A = 3$, 则存在纯的乘积态$\rho_0 = |\psi_1\rangle\langle\psi_1| \otimes \cdots \otimes |\psi_n\rangle\langle\psi_n|$使得$\langle \widetilde{S}_i + \widetilde{S}_j + \widetilde{S}_m \rangle_{\rho_0} = 3$. 于是, 计算可得

$$\begin{aligned} & \langle \widetilde{S}_i + \widetilde{S}_j + \widetilde{S}_m \rangle_{\rho_0} \\ = \ & \langle O_i^1 \rangle_{|\psi_1\rangle\langle\psi_1|} \cdots \langle O_i^n \rangle_{|\psi_n\rangle\langle\psi_n|} \\ & + \langle O_j^1 \rangle_{|\psi_1\rangle\langle\psi_1|} \cdots \langle O_j^n \rangle_{|\psi_n\rangle\langle\psi_n|} \\ & + \langle O_m^1 \rangle_{|\psi_1\rangle\langle\psi_1|} \cdots \langle O_m^n \rangle_{|\psi_n\rangle\langle\psi_n|} = 3. \end{aligned}$$

由于$\langle O_x^k \rangle_{|\psi_k\rangle\langle\psi_k|} (x = i, j, m)$介于$-1$与$+1$之间, 所以$\langle O_x^k \rangle_{|\psi_k\rangle\langle\psi_k|} = \pm 1$ $(x = i, j, m;\ k = 1, 2, \cdots, n)$. 特别地, $\langle O_x^{k_0} \rangle_{|\psi_{k_0}\rangle\langle\psi_{k_0}|} = \pm 1$ $(x = i, j, m)$. 由此可见, $O_i^{k_0}, O_j^{k_0}, O_m^{k_0}$有共同的特征态$|\psi_{k_0}\rangle$. 又因为

$$O_i^{k_0}, O_j^{k_0}, O_m^{k_0} \in \{I, \pm X, \pm Y, \pm Z\},$$

从而算子组$\{O_i^{k_0}, O_j^{k_0}, O_m^{k_0}\}$必为

$$\{I, \pm X\}, \{I, \pm Y\}, \{I, \pm Z\}$$

之一. 不论哪种情况, 算子$O_i^{k_0}, O_j^{k_0}, O_m^{k_0}$都是两两可换的. 这与$O_i^{k_0}, O_j^{k_0}, O_m^{k_0}$不两两可换矛盾. 故$C_A < 3$. 于是, 满足条件$C_A \leqslant C < \lambda_{\max}(A) = 3$的$C$存在, 由定理1知,

$$W_C = CI - \widetilde{S}_i - \widetilde{S}_j - \widetilde{S}_m (C_A \leqslant C < 3)$$

是一个纠缠目击, 且能探测图态$|G\rangle\langle G|$.

特别地, 在推论3中, 当$\widetilde{S}_i, \widetilde{S}_j$分别取稳定化算子$S_i, S_j$和$\widetilde{S}_m$取$S_i S_j$时, 有下列推论.

推论4 设$A = S_i + S_j + S_i S_j$, 且S_i与S_j不是局域交换的, 则$C_A \leqslant 1$且$W_C = CI - S_i - S_j - S_i S_j (1 \leqslant C < 3)$是一个纠缠目击, 且能探测图态$|G\rangle\langle G|$.

证明 在推论3中, 令$\widetilde{S}_i = S_i, \widetilde{S}_j = S_j, \widetilde{S}_m = S_i S_j$. 由于$S_i, S_j$为图$G$的稳定化算子, 有

$$S_i = X^{(i)} \prod_{k\in N(i)} Z^{(k)},$$

$$S_j = X^{(j)} \prod_{k\in N(j)} Z^{(k)}.$$

若S_i与S_j不是局域交换的, 则顶点i与j相连, 即$\{i, j\} \in E$, 因此$j \in N(i), i \in N(j)$. 从而

$$S_i S_j = Y^{(i)} Y^{(j)} \prod_{k\in(N(i)\Delta N(j))\backslash\{i,j\}} Z^{(k)},$$

其中$N(i)\Delta N(j) = N(i) \cup N(j) - N(i) \cap N(j)$. 于是, 容易得出$S_i, S_j, S_i S_j$不是两两局域交换的. 由推论3得, $C_A < 3$且$W_C = CI - S_i - S_j - S_i S_j (C_A \leqslant C < 3)$是一个纠缠目击, 且能探测图态$|G\rangle\langle G|$. 另外, 当$\rho = \rho_1 \otimes \cdots \otimes \rho_n \in \mathcal{P}$时, 计算可得

$$\begin{aligned} & \langle S_i + S_j + S_i S_j \rangle_\rho \\ = & \Big\langle X^{(i)} \cdot \prod_{k\in N(i)} Z^{(k)} + X^{(j)} \cdot \prod_{k\in N(j)} Z^{(k)} \\ & + Y^{(i)} Y^{(j)} \cdot \prod_{k\in(N(i)\Delta N(j))\backslash\{i,j\}} Z^{(k)} \Big\rangle_\rho \end{aligned}$$

$$\begin{aligned}
&\leqslant |\langle X\rangle_{\rho_i}\cdot|\prod_{k\in N(i)}|\langle Z\rangle_{\rho_k}|+|\langle X\rangle_{\rho_j}\cdot|\prod_{k\in N(j)}|\langle Z\rangle_{\rho_k}|\\
&\quad+|\langle Y\rangle_{\rho_i}||\langle Y\rangle_{\rho_j}|\cdot\prod_{k\in(N(i)\Delta N(j))\backslash\{i,j\}}|\langle Z\rangle_{\rho_k}|\\
&\leqslant |\langle X\rangle_{\rho_i}||\langle Z\rangle_{\rho_j}|+|\langle Z\rangle_{\rho_i}||\langle X\rangle_{\rho_j}|+|\langle Y\rangle_{\rho_i}||\langle Y\rangle_{\rho_j}|\\
&\leqslant \sqrt{|\langle X\rangle_{\rho_i}|^2+|\langle Z\rangle_{\rho_i}|^2+|\langle Y\rangle_{\rho_i}|^2}\\
&\quad\times\sqrt{|\langle Z\rangle_{\rho_j}|^2+|\langle X\rangle_{\rho_j}|^2+|\langle Y\rangle_{\rho_j}|^2}\\
&\leqslant 1.
\end{aligned}$$

从而$C_A=\max_{\rho=\rho_1\otimes\cdots\otimes\rho_n\in\mathcal{P}}|\langle S_i+S_j+S_iS_j\rangle_\rho|\leqslant 1$. 因此, 当$1\leqslant C<3$时, 纠缠目击$W_C=CI-S_i-S_j-S_iS_j$是一个纠缠目击, 且能探测图态$|G\rangle\langle G|$.

注13 在推论4中令$C=1, S_i=S_1$, 则$W_1=I-S_1-S_j-S_1S_j$为文献[20]中提到的可以探测图态$|G\rangle\langle G|$的纠缠目击. 而我们构造的纠缠目击W_C是一类探测图态$|G\rangle\langle G|$的纠缠目击, 包含W_1.

类似地, 在定理1中取A为$\widetilde{S}$中任意k个元素作线性组合以后得到的算子, 情况会如何呢? 为了简单起见, 不妨取$A=\sum\limits_{i=1}^{k}\widetilde{S}_i$, 可得如下结论.

推论5 设$A=\sum\limits_{i=1}^{k}\widetilde{S}_i$, 且$\widetilde{S}_1,\widetilde{S}_2,\cdots,\widetilde{S}_k$不是两两局域交换的, 则$C_A<k$且$W_C=CI-\sum\limits_{i=1}^{k}\widetilde{S}_i(C_A\leqslant C<k)$是一个纠缠目击, 且能探测图态$|G\rangle\langle G|$.

证明 由注8知, 可设

$$\widetilde{S}_i=O_i^1\otimes\cdots\otimes O_i^n(i=1,2,\cdots,k),$$

其中

$$O_i^s\in\{I,\pm X,\pm Y,\pm Z\}(s=1,2,\cdots,n).$$

因为$\widetilde{S}_1,\widetilde{S}_2,\cdots,\widetilde{S}_k$不是两两局域交换的, 所以存在$s_0\in\{1,2,\cdots,n\}$使得$O_1^{s_0},O_2^{s_0},\cdots,O_k^{s_0}$不两两可换. 由于$A$是自伴算子, 且它的最大特征值$\lambda_{\max}(A)=k$, 相应的特征态为$|G\rangle$, 所以$C_A\leqslant k$. 下证$C_A\neq k$. 反证法. 若$C_A=k$, 则存在纯的乘积态$\rho_0=|\psi_1\rangle\langle\psi_1|\otimes\cdots\otimes|\psi_n\rangle\langle\psi_n|$使得$\left\langle\sum\limits_{i=1}^{k}\widetilde{S}_i\right\rangle_{\rho_0}=k$. 于是, 计算可得

$$\begin{aligned}
\left\langle\sum_{i=1}^{k}\widetilde{S}_i\right\rangle_{\rho_0}&=\sum_{i=1}^{k}\langle O_i^1\rangle_{|\psi_1\rangle\langle\psi_1|}\cdots\langle O_i^n\rangle_{|\psi_n\rangle\langle\psi_n|}\\
&=k.
\end{aligned}\tag{6}$$

由于

$$-1\leqslant\langle O_i^s\rangle_{|\psi_s\rangle\langle\psi_s|}\leqslant 1$$
$$(s=1,2,\cdots,n,\ i=1,2,\cdots,k),$$

所以

$$\langle O_i^s\rangle_{|\psi_s\rangle\langle\psi_s|}=\pm1$$
$$(s=1,2,\cdots,n,\ i=1,2,\cdots,k).$$

特别地, $\langle O_x^{s_0}\rangle_{|\psi_{s_0}\rangle\langle\psi_{s_0}|}=\pm1(x=1,2,\cdots,k)$. 由此可见, $O_1^{s_0},O_2^{s_0},\cdots,O_k^{s_0}$有共同的特征态$|\psi_{s_0}\rangle$. 又因为

$$O_1^{s_0},O_2^{s_0},\cdots,O_k^{s_0}\in\{I,\pm X,\pm Y,\pm Z\},$$

所以算子组$\{O_1^{s_0},O_2^{s_0},\cdots,O_k^{s_0}\}$必为

$$\{I,\pm X\},\{I,\pm Y\},\{I,\pm Z\}$$

之一. 从而, 不论哪种情况, 算子$O_1^{s_0},O_2^{s_0},\cdots,O_k^{s_0}$都是两两可换的. 这与$O_1^{s_0},O_2^{s_0},\cdots,O_k^{s_0}$不两两可换矛盾. 故$C_A<k$. 于是, 满足条件$C_A\leqslant C<\lambda_{\max}(A)=k$的$C$存在, 由定理1知, $W_C=CI-\sum\limits_{i=1}^{k}\widetilde{S}_i(C_A\leqslant C<k)$是一个纠缠目击, 且能探测图态$|G\rangle\langle G|$.

注14 由推论5知, 若$\widetilde{S}_1,\widetilde{S}_2,\cdots,\widetilde{S}_k$不是两两局域交换的, 则图态$|G\rangle\langle G|$及其周围态能被形如$W_C=CI-\sum\limits_{i=1}^{k}\widetilde{S}_i(C_A\leqslant C<k)$的纠缠目击探测. 例如, 令

$$\rho''=\frac{1}{2^n}\prod_{i=1}^{k}(I+\widetilde{S}_i).$$

容易计算

$$\mathrm{tr}(W_C\rho'')=C-k<0.$$

因此, 纠缠目击$W_C=CI-\sum\limits_{i=1}^{k}\widetilde{S}_i$能探测$\rho''=\frac{1}{2^n}\prod\limits_{i=1}^{k}(I+\widetilde{S}_i)$. 进一步, 可以构造更一般的态

$$\rho'''=\frac{1}{2^n}\prod_{i=1}^{k}(I+a_i\widetilde{S}_i),$$

其中

$$-1\leqslant a_i\leqslant 1(i=1,2,\cdots,k),\sum_{i=1}^{k}a_i>C.$$

类似可证: 纠缠目击$W_C=CI-\sum\limits_{i=1}^{k}\widetilde{S}_i$能探测$\rho'''$.

注15 在注14中令

$$\widetilde{S}_i = S_i, k = n, a_i = 1 (i = 1, 2, \cdots, n),$$

得 $\rho''' = |G\rangle\langle G|$, 因此间接可得图态 $|G\rangle\langle G|$ 能被 $W_C = CI - \sum_{i=1}^{n} S_i$ 探测, 其中 $C_A \leqslant C < n$. 与推论5结论符合. 特别地, 在定理1中, 当 A 取为图 G 的 n 个稳定化算子的和时, 还可得下列结论.

推论6 设 $A = \sum_{i=1}^{n} S_i$, 且 $S_1, S_2, \cdots, S_n$ 不是两两局域交换的, 则 $C_A \leqslant n-1$ 且当 $n-1 \leqslant C < n$ 时, $W_C = CI - \sum_{i=1}^{n} S_i$ 是一个纠缠目击, 且能探测图态 $|G\rangle\langle G|$.

证明 在推论5中, 令

$$k = n, \widetilde{S}_1 = S_1, \widetilde{S}_2 = S_2, \cdots, \widetilde{S}_n = S_n.$$

由推论5知: $C_A < n$ 且当 $C_A \leqslant C < n$ 时, $W_C = CI - \sum_{i=1}^{n} S_i$ 是一个纠缠目击, 且能探测图态 $|G\rangle\langle G|$. 另外, 若 $S_1, S_2, \cdots, S_n$ 不是两两局域交换的, 则至少存在两个稳定化算子不是局域交换的, 不妨设为 S_1, S_2. 于是, 由(5)式可知

$$\begin{aligned} C_A &= \max_{\rho \in \mathcal{P}} \left| \left\langle \sum_{i=1}^{n} S_i \right\rangle_\rho \right| \\ &\leqslant \max_{\rho \in \mathcal{P}} |\langle S_1 + S_2 \rangle_\rho| + \max_{\rho \in \mathcal{P}} |\langle S_3 + \cdots + S_n \rangle_\rho| \\ &\leqslant 1 + (n-2) \\ &= n - 1. \end{aligned}$$

因此, 当 $n-1 \leqslant C < n$ 时, $W_C = CI - \sum_{i=1}^{n} S_i$ 是一个纠缠目击, 且能探测图态 $|G\rangle\langle G|$.

注16 由推论6可知, 若图 G 中至少有两个顶点相连, 则它所对应的图态是纠缠的, 即非平凡的图对应的图态都是纠缠的.

另外, 在定理1中, 当 A 取为图 G 的稳定子的全部元素之和时, 可得下列结论.

推论7 设 $A = \sum_{i=1}^{2^n} \widetilde{S}_i$, 若 $\widetilde{S}_1, \widetilde{S}_2, \cdots, \widetilde{S}_{2^n}$ 不是两两局域交换的, 则 $C_A \leqslant 2^{n-1}$, 且当 $2^{n-1} \leqslant C < 2^n$ 时, $W_C = CI - \sum_{i=1}^{2^n} \widetilde{S}_i$ 是一个纠缠目击, 且能探测图态 $|G\rangle\langle G|$.

证明 在推论5中, 令 $k = 2^n$. 由推论5可知: 若 $\widetilde{S}_1, \widetilde{S}_2, \cdots, \widetilde{S}_{2^n}$ 不是两两局域交换的, 则 $C_A \leqslant 2^n$ 且当 $C_A \leqslant C < 2^n$ 时, $W_C = CI - \sum_{i=1}^{2^n} \widetilde{S}_i$ 是一个纠缠目击, 且能探测图态 $|G\rangle\langle G|$. 另外, 由注9可得

$$\begin{aligned} C_A &= \max_{\rho \in \mathcal{P}} \left| \left\langle \sum_{i=1}^{2^n} \widetilde{S}_i \right\rangle_\rho \right| = 2^n \max_{\rho \in \mathcal{P}} |\langle |G\rangle\langle G| \rangle_\rho| \\ &= 2^n \max_{|\psi\rangle\langle\psi| \in \mathcal{P}} |\langle G|\psi\rangle|^2. \end{aligned}$$

由文献[32]知: $\max_{|\psi\rangle\langle\psi| \in \mathcal{P}} |\langle G|\psi\rangle|^2 \leqslant 1/2$. 所以, $C_A \leqslant 2^{n-1}$. 因此, 当 $2^{n-1} \leqslant C < 2^n$ 时,

$$W_C = CI - \sum_{i=1}^{2^n} \widetilde{S}_i$$

是一个纠缠目击, 且能探测图态 $|G\rangle\langle G|$.

注17 由推论7可知, 当 $1/2 \leqslant C < 1$ 时, $W_C = CI - |G\rangle\langle G|$ 是一个纠缠目击, 且能探测图态 $|G\rangle\langle G|$. 另外, 由定理2知, 在这类纠缠目击 $W_C = CI - |G\rangle\langle G|$ 中, $W_{1/2} = \frac{1}{2}I - |G\rangle\langle G|$ 是最优纠缠目击.

4 结 论

本文发现: 当一个可观测量 A 在可分纯态上的最大期望 C_A 严格小于其最大特征值 $\lambda_{\max}(A)$ 时, 算子 $W_C = CI - A$ 都是一个纠缠目击, 只要参数 C 满足条件 $C_A \leqslant C < \lambda_{\max}(A)$. 特别地, 当 A 由图态的一些稳定子构成时, 纠缠目击 W_{C_A} 就是文献[20]中得到的纠缠目击. 虽然 W_{C_A} 探测到的纠缠态比 W_C 能探测的更多, 但在具体问题中, 计算 C_A 的精确值是特别困难的, 而估计 C_A 的上界是比较容易的. 因此, 构造纠缠目击 W_C 比构造 W_{C_A} 更加方便一些. 作为应用, 得到了利用稳定子构造图态的纠缠目击的一系列方法. 由于我们构造的纠缠目击包含了文献[20]中给出的纠缠目击, 所以具有更广泛的应用价值.

参考文献

[1] Bennett C H, Brassard G, Crépeau C, Jozsa R, Peres A, Wootters W K 1993 *Phys. Rev. Lett.* **70** 1895

[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661

[3] Steane A 1998 *Rep. Prog. Phys.* **61** 117

[4] Mattle K, Weinfurter H, Kwiat P G, Zeilinger A 1996 *Phys. Rev. Lett.* **76** 4656

[5] Hillery M, Bužek V, Berthiaume A 1999 *Phys. Rev. A* **59** 1829

[6] Long G L, Liu X S 2002 *Phys. Rev. A* **65** 032302

[7] Sheng Y B, Zhou L 2017 *Sci. Bull.* **62** 1025

[8] Deng F G, Ren B C, Li X H 2017 *Sci. Bull.* **62** 46

[9] Cong M Y, Yang J, Huang Y X 2016 *Acta Phys. Sin.* **65** 170301 (in Chinese) [丛美艳, 杨晶, 黄燕霞 2016 物理学报 **65** 170301]

[10] Ren B C, Deng F G 2015 *Acta Phys. Sin.* **64** 160303 (in Chinese) [任宝藏, 邓富国 2015 物理学报 **64** 160303]

[11] Zong X L, Yang M 2016 *Acta Phys. Sin.* **65** 080303 (in Chinese) [宗晓岚, 杨名 2016 物理学报 **65** 080303]

[12] Yang F, Cong S 2011 *Chin. J. Quant. Elect.* **28** 391 (in Chinese) [杨霏, 丛爽 2011 量子电子学报 **28** 391]

[13] Lewenstein M, Kraus B, Cirac J I, Horodecki P 2000 *Phys. Rev. A* **62** 052310

[14] Lewenstein M, Kraus B, Horodecki P, Cirac J I 2001 *Phys. Rev. A* **63** 044304

[15] Tóth G, Gühne O 2005 *Phys. Rev. Lett.* **94** 060501

[16] Gühne O, Hyllus P, Bruss D, Ekert A, Lewenstein M, Macchiavello C, Sanpera A 2002 *Phys. Rev. A* **66** 062305

[17] Tóth G 2004 *Phys. Rev. A* **69** 052327

[18] Brukner C, Vedral V, Zeilinger A 2006 *Phys. Rev. A* **73** 012110

[19] Wu L A, Bandyopadhyay S, Sarandy M S, Lidar D A 2005 *Phys. Rev. A* **72** 032309

[20] Tóth G, Gühne O 2005 *Phys. Rev. A* **72** 022340

[21] Doherty A C, Parrilo P A, Spedalieri F M 2005 *Phys. Rev. A* **71** 032333

[22] Vianna R O, Doherty A C 2006 *Phys. Rev. A* **74** 052306

[23] Jafarizadeh M A, Rezaee M, Yagoobi S K A S 2005 *Phys. Rev. A* **72** 062106

[24] Jafarizadeh M A, Rezaee M, Ahadpour S 2006 *Phys. Rev. A* **74** 042335

[25] Jafarizadeh M A, Najarbashi G, Habibian H 2007 *Phys. Rev. A* **75** 052326

[26] Jafarizadeh M A, Sufiani R, Nami S, Golmohammadi M 2012 *Quantum. Inf. Process.* **11** 729

[27] Cheng S, Chen J, Wang L 2017 *Physics* **46** 416 (in Chinese) [程嵩, 陈靖, 王磊 2017 物理 **46** 416]

[28] Deng D L, Li X P, Sarma S D 2017 *Phys. Rev. X* **7** 021021

[29] Levine Y, Yakira D, Cohen N, Shashua A 2017 arXiv: 1704.01552

[30] Carleo G, Troyer M 2017 *Science* **355** 602

[31] Gao X, Duan L M 2017 *Nature Commun.* **8** 662

[32] Tóth G, Gühne O, Briegel H J 2005 *Phys. Rev. Lett.* **95** 120405

[33] Hein M, Eisert J, Briegel H J 2003 *Phys. Rev. A* **69** 062311

物理学报 Acta Phys. Sin. Vol. 67, No. 7 (2018) 070303

General method of constructing entanglement witness*

Yang Ying[1)2)] Cao Huai-Xin[1)†]

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

2) (School of Mathematics and Information Technology, Yuncheng College, Yuncheng 044000, China)

(Received 10 October 2017; revised manuscript received 3 January 2018)

Abstract

Quantum entanglement, as an indispensable resource in quantum communication and quantum computation, is widely used in the field of quantum information. However, people's understanding on entanglement is quite limited both theoretically and experimentally. How to determine whether a given quantum state is entangled is still an important task. The entanglement witness is a kind of special self-adjoint operator, it can be used to determine whether a quantum state is an entangled state. This provides a new direction for the determination of entangled states. Entanglement witness has its own unique characteristics in various kinds of entanglement criterion. It is the most effective tool for detecting multipartite entanglement, and the most useful method to detect entanglement in experiments. In the background of quantum theory, we use theory of operators to make a thorough and systematic study of the construction of entanglement witness in this paper. First, from the definition of an entanglement witness, a general method is given to construct an entanglement witness. It is proved that when the maximal expectation C_A of an observable A in the separable pure states is strictly less than its biggest eigenvalue $\lambda_{\max}(A)$, the operator $W_C = CI - A$ is an entanglement witness provided that $C_A \leqslant C < \lambda_{\max}(A)$. Although the entanglement witness W_{C_A} can detect more entangled states than W_C, but it is difficult to calculate the exact value of C_A, and the estimate of the upper bound of C_A is easier. Therefore, it is more convenient to construct entanglement witness W_C than W_{C_A}.

In quantum computation, a graph state is a special kind of multi-qubit state that can be represented by a graph. Each qubit is represented by a vertex of the graph, and there is an edge between every interacting pair of qubits. Graph states play a crucial role in many applications of quantum information theory, such as quantum error correcting codes, measurement-based quantum computation, and quantum simulation. Consequently, a significant effort is devoted to the creation and investigation of graph states. In the last part of this paper, as applications of our method, a series of methods for constructing an entanglement witness is obtained in the stabilizer formalism. It is also proved that how entanglement witnesses can be derived for a given graph state, provided some stabilizing operators of the graph state are known. Especially, when A is made up of some stabilizing operators of a graph state, entanglement witness W_{C_A} becomes one in literature.

Keywords: entanglement witness, graph state, stabilizer

PACS: 03.67.Mn, 03.65.Db, 03.65.Ud, 02.30.Sa **DOI:** 10.7498/aps.67.20172697

* Project supported by the National Natural Science Foundation of China (Grant Nos. 11371012, 11601300, 11571213, 11771009) and the Fundamental Research Funds for the Central Universities of Ministry of Education of China (Grant No. GK201703093).

† Corresponding author. E-mail: caohx@snnu.edu.cn