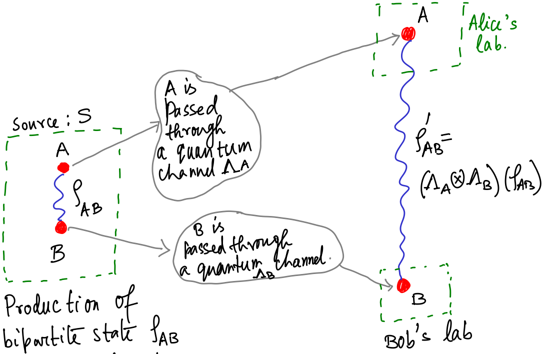
On witnessing arbitrary bipartite entanglement in measurement device independent way

Sibasish Ghosh

Optics & Quantum Information Group
The Institute of Mathematical Sciences
C. I. T. Campus, Taramani
Chennai - 600 113

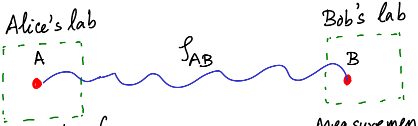
[In collaboration with A. Mallick]

(arXiv:1506.03985)



Production of bipartite state ρ_{AB} of two subsystems A and B in a lab by a source S

Fig.1: Preparation of a bipartite state on demand — to be shared by Alice and Bob — by a source



Measurement of one of the observables $A_1, A_2, \ldots$ is done on A

Measurement of one of the observables $B_1, B_2, \ldots$ is done on B

$$\mathrm{Tr}\left[W_{AB}\, \rho_{AB} \right] \equiv \sum_{i,j} \beta_{ij}\, \mathrm{Tr}\left[(A_i \otimes B_j)\, \rho_{AB} \right]$$

Fig. 2: Witnessing entanglement in ρ_{AB}

Detecting entanglement

- It is essential to have shared entangled states between distantly located parties prior to efficient performance of several quantum information processing tasks (like, teleportation, superdense coding, etc.).
- How to check that such a shared state – supplied *apriori* by some source – is indeed the state Alice and Bob are supposed to share? (preparation process)
- And how to check that such a shared state – supplied *apriori* by some source – is indeed entangled? (measurement process)
- No assumption regarding faithfulness of preparation process is needed for our purpose here as we will be dealing with arbitrary states.

Detecting entanglement (continued)

- The measurement process corresponds to *witnessing entanglement* in the shared state via measurement of the corresponding *entanglement witness operator* using measurements of local observables on the shared state.
- Erroneous measurements of the local observables may lead to witness a separable shared state to be entangled!
- How to avoid such a situation?
- It can be avoided if witnessing entanglement in the shared state can be made possible in a *measurement-device independent* (MDI) way.
- Shown to be possible by Branciard et al. recently [*Phys. Rev. Lett.* **110**, 060405 (2013)].

Detecting entanglement (continued)

- But their scheme requires *apriori* knowledge about the shared state – as the form of the EW operator depends, in general, on the entangled state itself.
- Here we discuss about witnessing entanglement in the shared state in an MDI way without such *apriori* knowledge.
- But we need to pay some extra price for that!
- We require more copies of the shared state.
- Moreover, knowledge of dimensions of individual subsystems is needed – as in the case of Branciard et al.

Outline

- Witnessing entanglement
- Non-locality vs. entanglement
- Measurement-device independent entanglement witness with *apriori* knowledge of state
- Universal entanglement witness process for two-qubits
- Witnessing entanglement in unknown two-qubit state in MDI way
- Witnessing NPT-ness of unknown state in any given bi-partite system in MDI way
- Conjecture about non-existence of universal MDI entanglement witness operator in any given bi-partite system other than two-qubits
- Conclusion

Witnessing entanglement

What is an entangled state?

- Given any density matrix ρ_{AB} of a bi-partite quantum system $S = A + B$ – described by the composite Hilbert space $\mathcal{H}_S = \mathcal{H}_A \otimes \mathcal{H}_B$ – will be *separable* iff $\rho_{AB} = \sum_i \omega_i \sigma_A^{(i)} \otimes \tau_B^{(i)}$, with $\sigma_A^{(i)}$'s ($\tau_B^{(i)}$'s) being density matrices of A (B) and $0 \leq \omega_i \leq 1$ with $\sum_i \omega_i = 1$.
- Otherwise ρ_{AB} is *entangled*.

What is an entanglement witness operator?

- Given any entangled state ρ_{AB} of a (given) bi-partite quantum system $S = A + B$, one can always (in principle) find out a hermitian operator W on $\mathcal{H}_S$ such that: (i) $\mathrm{Tr}[W\rho] < 0$ and (ii) $\mathrm{Tr}[W\sigma] \geq 0$ for *all* separable states σ_{AB} of the system.
- W is said to be an *entanglement witness* operator, witnessing the entanglement in ρ_{AB}.
- Given a different entangled state ρ'_{AB} of the system, it may happen that $\mathrm{Tr}[W\rho'] \geq 0$.
- Thus W does not have a *universal* character, in general.

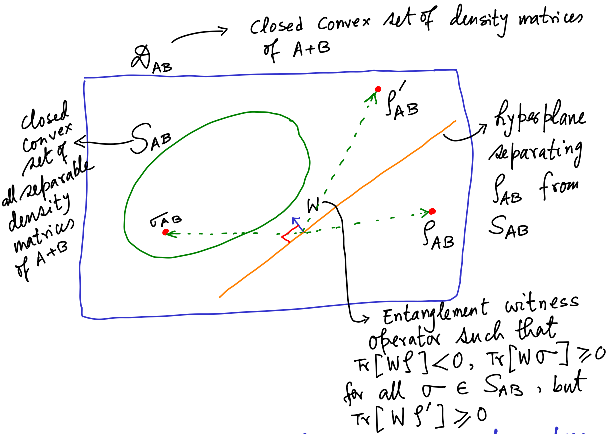


Fig 3: Entanglement witness operator

Local realization of entanglement witness operator

- One can *always* find out a set of observables $\{A_i : i = 1, 2, \ldots, N_A\}$ for A as well as a set of observables $\{B_j : j = 1, 2, \ldots, N_B\}$ (with $N_A \leq d_A^2 \equiv (\mathrm{dim}\mathcal{H}_A)^2$ and $N_B \leq d_B^2 \equiv (\mathrm{dim}\mathcal{H}_B)^2$) such that: $W = \sum_{i=1}^{N_A} \sum_{j=1}^{N_B} \beta_{ij} A_i \otimes B_j$ where β_{ij}'s are real numbers.
- So, given a state ρ_{AB} – shared between Alice and Bob – measurement of one of the observables A_i's on A (by Alice) and measurement of one of the observables B_j on B (by Bob) will give rise to the measurement statistics $\mathrm{Tr}[(A_i \otimes B_j)\rho]$.
- Using these measurement statistics, one can calculate: $\mathrm{Tr}[W\rho] = \sum_{i=1}^{N_A} \sum_{j=1}^{N_B} \beta_{ij}\ \mathrm{Tr}[(A_i \otimes B_j)\rho]$.

Local-realistic inequalities vs. entanglement witness

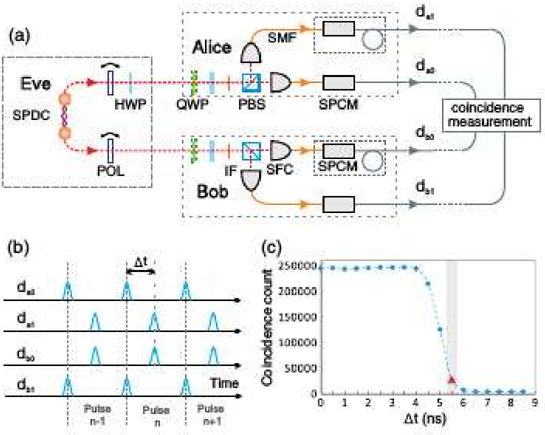
- *Every* local-realistic inequality can be expressed in the form: $\sum_{i=1}^{N_A} \sum_{j=1}^{N_B} \beta_{ij} \langle A_i B_j \rangle \geq k$, a constant.
- For any quantum state ρ_{AB}, satisfaction of such an inequality takes the form: $\sum_{i=1}^{N_A} \sum_{j=1}^{N_B} \beta_{ij} \, \mathrm{Tr}[(A_i \otimes B_j)\rho] \geq k$.
- This is equivalent to: $\mathrm{Tr}[W_{LR}\rho] \geq 0$ with $W_{LR} \equiv \sum_{i=1}^{N_A} \sum_{j=1}^{N_B} \beta_{ij}(A_i \otimes B_j) - kI_{d_A^2 \times d_B^2}$.
- As no separable state σ_{AB} of the system violates any local-realistic inequality, we must have: $\mathrm{Tr}[W_{LR}\sigma] \geq 0$.
- On the other hand, for any (entangled) state ρ_{AB}, violating the inequality, we must have: $\mathrm{Tr}[W_{LR}\rho] < 0$.
- Thus W_{LR} is an entanglement witness operator.
- The converse is not true, in general – otherwise, loophole-free test of BI would mean MDI witnessing of the corresponding EW operator.

Erroneous witnessing

- The two photon-polarization state: $\rho^{v}_{AB} \equiv (1-v)|\Psi^{-}\rangle_{AB}\langle\Psi^{-}| + (v/2)(|HH\rangle_{AB}\langle HH| + |VV\rangle_{AB}\langle VV|)$, with $|\Psi^{-}\rangle_{AB} \equiv (1/\sqrt{2})(|HV\rangle_{AB} - |VH\rangle_{AB})$, is entangled iff $0 \leq v < 1/2$.
- With the witness operator $W \equiv (1/2)I_{4\times 4} - |\Psi^{-}\rangle\langle\Psi^{-}|$, we have: $\mathrm{Tr}[W\rho^{v}_{AB}] = (2v-1)/2$ – which is negative iff $v < 1/2$.
- For any ρ_{AB}: $\mathrm{Tr}[W\rho_{AB}] = (1/4)(1 + \langle\sigma_x \otimes \sigma_x\rangle_{\rho} + \langle\sigma_y \otimes \sigma_y\rangle_{\rho} + \langle\sigma_y \otimes \sigma_y\rangle_{\rho})$ with $\sigma_x \equiv |H\rangle\langle V| + |V\rangle\langle H|$, etc.
- $\langle\sigma_j \otimes \sigma_j\rangle_{\rho} = \langle\sigma_j^{+} \otimes \sigma_j^{+}\rangle_{\rho} + \langle\sigma_j^{-} \otimes \sigma_j^{-}\rangle_{\rho} - \langle\sigma_j^{+} \otimes \sigma_j^{-}\rangle_{\rho} - \langle\sigma_j^{-} \otimes \sigma_j^{-}\rangle_{\rho}$ for $j = x, y, z$.
- $\sigma_j = \sigma_j^{+} - \sigma_j^{-}$ for all j (spectral decomposition).

Erroneous witnessing (continued)

- Experimental demonstration by Xu et al. [PRL **112**, 140506 (2014)]
- Using the time-shift attack of QKD, the coincidence counting rate – for calculating $\langle \sigma_j^+ \otimes \sigma_j^+ \rangle_\rho$ and $\langle \sigma_j^- \otimes \sigma_j^- \rangle_\rho$ – can be diminished for the separable state $\rho_{AB} = \rho_{AB}^{v=1}$, and thereby, giving: $\langle \sigma_j^\alpha \otimes \sigma_j^\alpha \rangle_\rho \equiv$ $N_{jA}^{(\alpha)} N_{jB}^{(\alpha)} / (N_{jA}^{(+)} N_{jB}^{(+)} + N_{jA}^{(+)} N_{jB}^{(-)} + N_{jA}^{(-)} N_{jB}^{(+)} + N_{jA}^{(-)} N_{jB}^{(-)}) \approx 0$ for $\alpha = +, -$ and $j = x, y, z$.
- Thus here: $\langle \sigma_j \otimes \sigma_j \rangle_\rho \approx$ $-(N_{jA}^{(+)} N_{jB}^{(-)} + N_{jA}^{(-)} N_{jB}^{(+)}) / (N_{jA}^{(+)} N_{jB}^{(-)} + N_{jA}^{(-)} N_{jB}^{(+)}) = -1$ for $j = x, y, z$.
- It then gives rise to: $\mathrm{Tr}[W \rho_{AB}^{v=1}] \approx -(1/2)$



Time-shift attack on conventional EW

Non-locality vs. entanglement

Entanglement does not imply non-locality, in general

- Two-qubit Werner state $\rho_x \equiv x|\psi^-\rangle\langle\psi^-| + \frac{1-x}{4} I_{4\times 4}$ (with $|\psi^-\rangle \equiv (1/\sqrt{2})(|01\rangle - |10\rangle)$ and $0 \leq x \leq 1$) is entangled for all x with $1/3 < x \leq 1$.
- But ρ_x is known to have a local-realistic model for its measurement statistics (even for measurements of POVMs) for certain range ($\mathcal{R}$, say) of values of x within the interval $(1/3, 1]$.
- Thus ρ_x can violate *no* local-realistic inequality for any such x in $\mathcal{R}$.
- There are plenty of such examples!
- But, can one utilize *every* entangled state for some information processing task in a way which is more efficient that having *any* separable state? ('operational' meaning of entanglement)

Winning two-party co-operative game

- In a two-party co-operative classical game $\mathcal{G}$, the players Alice and Bob are supplied with strategies $s \in \mathcal{S}$ and $t \in \mathcal{T}$ respectively with probabilities $p(s)$ and $q(t)$ by a referee (Charlie), and the players' job is to come up with respective (definite) outcomes $x \in \mathcal{X}$ and $y \in \mathcal{Y}$ so that the gain of the two players together will be $\mathcal{C}(s, t, x, y)$ (to be given by the referee).
- Thus the maximum average pay-off of the game: $\mathcal{P}(\mathcal{G}) \equiv \max \sum_{s \in \mathcal{S}, t \in \mathcal{T}, x \in \mathcal{X}, y \in \mathcal{Y}} p(s)q(t)\mathcal{C}(s, t, x, y)\mu(x, y|s, t)$, where maximization is taken over all $\mu(x, y|s, t)$ – the joint probability of occurance of the outcomes x and y for the inputs s and t.

Winning two-party co-operative game with shared quantum state

- Replacement of the strategies s (t) by pairwise orthogonal quantum states $\tau^{(s)}_{A_0}$ $(\omega^{(t)}_{B_0})$: does not really mean any change!
- But now the players start the game with an *apriori* shared entangled state ρ_{AB}.
- Alice (Bob) now performs a measurement using a POVM $\{E^{(x)}_{A_0A} : x \in \mathcal{X}\}$ $(\{E^{(y)}_{B_0B} : y \in \mathcal{Y}\})$ jointly on A_0 and A (B_0 and B) to comeup with a measurement outcome x (y).
- Maximum average pay-off: $\mathcal{P}(\mathcal{G};\rho) \equiv \max \sum_{s\in\mathcal{S},t\in\mathcal{T},x\in\mathcal{X},y\in\mathcal{Y}} p(s)q(t)\mathcal{C}(s,t,x,y)\mu_\rho(x,y|s,t)$, where maximization is taken over all POVMs.
- Here $\mu_\rho(x,y|s,t) \equiv \mathrm{Tr}[(E^{(s)}_{A_0A} \otimes E^{(t)}_{B_0B})(\tau^{(s)}_{A_0} \otimes \rho_{AB} \otimes \omega^{(t)}_{B_0})]$.

Winning two-party co-operative game with shared quantum state (continued)

- Is it true that for given *any* shared entangled state ρ_{AB}, there always exists at least one game plan $\mathcal{G}_\rho$ for which $\mathcal{P}(\mathcal{G}_\rho; \sigma) < \mathcal{P}(\mathcal{G}_\rho; \rho)$ for all separable states σ_{AB}?
- It was shown to be *untrue* by Buscemi [*Phys. Rev. Lett.* **108**, 200401 (2012)].
- But in case the game strategies are associated with non-orthogonal (in general) quantum inputs $\tau_{A_0}^{(s)}$ $(\omega_{B_0}^{(t)})$, the aforesaid fact was shown to be true for any given entangled state ρ_{AB} – shown in the same work of Buscemi.
- Note that, for any given game plan $\mathcal{G}$, $\mathcal{P}(\mathcal{G}; \sigma)$ is *one and the same* for all separable states σ_{AB}.
- Thus, every entangled state is more efficient to win a 'non-local' game compared to any separable state.

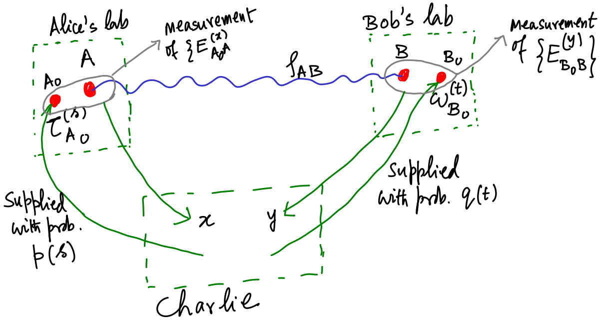


Fig. 4: Non-local game

Measurement-device independent entanglement witness with *apriori* knowledge of state

MDI-EW

- Although Buscemi's result prefers any entangled state over all possible separable states while winning a non-local game, it *does not explicitly provide* any scheme for detecting entanglement.
- Note that violation of a loophole-free local-realistic inequality by any state necessarily indicates entanglement in the state in a *device-independent* (DI) way within quantum theory: it guarantees the presence of entanglement, independently
  (i) of the measurements actually performed,
  (ii) of the functioning of any device used in the experiment, as well as
  (iii) of the dimension of the underlying shared quantum state.

MDI-EW (continued)

- But such a DI entanglement witness scheme does not work for *all* entangled states – some entangled states have local model.
- Based on Buscemi's result, Branciard et al. [*Phys. Rev. Lett.* **110**, 060405 (2013)] provided a MDI-EW scheme for all entangled state.
- In fact, denoting the quantities $p(s)q(t)\mathcal{P}(s,t,x,y)$ in Buscemi's scheme by $\tilde{\beta}_{s,t,x,y}$, one can find out the expression $I(\mu) \equiv \sum_{s\in\mathcal{S},t\in\mathcal{T},x\in\mathcal{X},y\in\mathcal{Y}} \tilde{\beta}_{s,t,x,y}\mu(x,y|s,t)$, where $I(\mu) \geq 0$ will *necessarily* mean the shared state to be separable.
- This holds irrespective of the choice as well as performance of measurement.
- Thus, $I(\mu) < 0$ implies entanglement in the shared state in a MDI way.

How does it work?

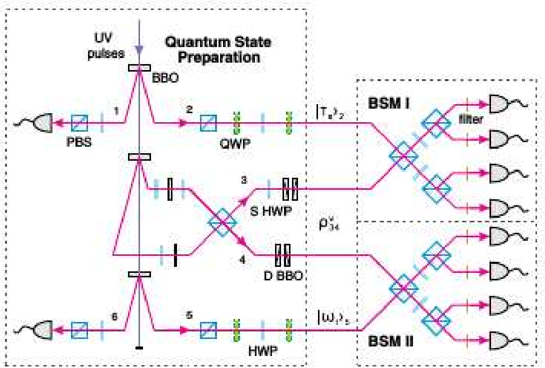
- Assuming that $\{(\tau^{(s)})^T : s \in \mathcal{S}\}$ $(\{(\omega^{(t)})^T : t \in \mathcal{T}\})$ can span $\mathcal{B}(\mathcal{H}_A)$ $(\mathcal{B}(\mathcal{H}_B))$, any EW operator W on $\mathcal{H}_A \otimes \mathcal{H}_B$ can be expressed as: $W = \sum_{s \in \mathcal{S}, t \in \mathcal{T}} \beta_{st} (\tau^{(s)})^T \otimes (\omega^{(t)})^T$.
- Here we take $\mathcal{X} = \{0, 1\} = \mathcal{Y}$.
- For any shared separable state $\sigma_{AB} = \sum_k p_k \sigma_A^{(k)} \otimes \eta_B^{(k)}$ and for any POVM effect A_1 (B_1) corresponding to outcomes 1: $\mu_\sigma(1, 1|\tau^{(s)}, \omega^{(t)}) = \mathrm{Tr}[(A_1 \otimes B_1)(\tau^{(s)} \otimes \sigma \otimes \omega^{(t)})] = \sum_k p_k \mathrm{Tr}[(A_1^{(k)} \otimes B_1^{(k)})(\tau^{(s)} \otimes \omega^{(t)})]$ with $A_1^{(k)} \equiv \mathrm{Tr}_A[A_1(I \otimes \sigma_A^{(k)})]$ and $B_1^{(k)} \equiv \mathrm{Tr}_B[B_1(\eta_B^{(k)} \otimes I)]$.
- Note that here: $\tilde{\beta}_{s,t,1,1} = \beta_{st}$ and $\tilde{\beta}_{s,t,x,y} = 0$ otherwise.

How does it work (continued)

- Here: $I(\mu_\sigma) = \sum_{s \in \mathcal{S}, t \in \mathcal{T}} \beta_{st} \mu_\sigma(1,1|\tau^{(s)}, \omega^{(t)}) = \sum_{s \in \mathcal{S}, t \in \mathcal{T}} \beta_{st} \sum_k p_k \, \mathrm{Tr}[(A_1^{(k)} \otimes B_1^{(k)})(\tau^{(s)} \otimes \omega^{(t)})] = \sum_k p_k \, \mathrm{Tr}[(A_1^{(k)} \otimes B_1^{(k)}) W^T] = \mathrm{Tr}[\{\sum_k p_k (A_1^{(k)})^T \otimes (B_1^{(k)})^T\} W] \geq 0$, as $\{\sum_k p_k (A_1^{(k)})^T \otimes (B_1^{(k)})^T\}$ is separable (possibly unnormalized).
- On the other hand, if W is an EW operator for a given entangled state ρ_{AB}, we have (for $A_1 = |\Phi\rangle_{AA}\langle\Phi|$ and $B_1 = |\Phi\rangle_{BB}\langle\Phi|$ with $|\Phi\rangle_{SS} \equiv (1/d_S) \sum_{i=1}^{d_S} |ii\rangle_{SS}$ for $S = A, B$): $\mu_\rho(1,1|\tau^{(s)}, \omega^{(t)}) = \mathrm{Tr}[(|\Phi\rangle_{AA}\langle\Phi| \otimes |\Phi\rangle_{BB}\langle\Phi|)(\tau^{(s)} \otimes \rho_{AB} \otimes \omega^{(t)})] = (1/(d_A d_B)) \, \mathrm{Tr}[((\tau^{(s)})^T \otimes (\omega^{(t)})^T) \rho_{AB}]$.
- Then $I(\mu_\rho) = \sum_{s \in \mathcal{S}, t \in \mathcal{T}} \beta_{st} \mu_\rho(1,1|\tau^{(s)}, \omega^{(t)}) = \mathrm{Tr}[W \rho_{AB}]/(d_A d_B) < 0$.

Experimental demonstration of MDI-EW

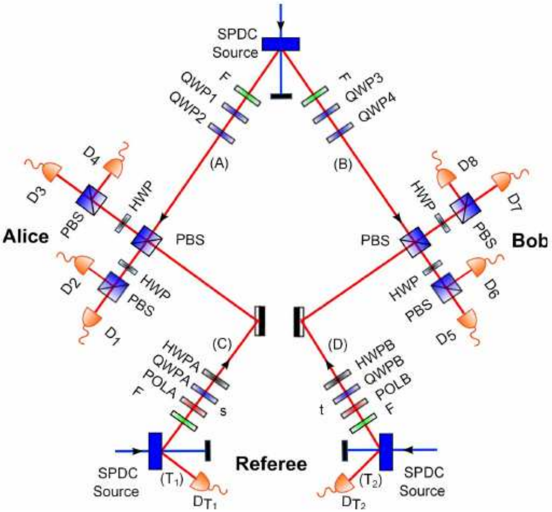
- Xu et al. [PRL **112**, 140506 (2014)] have experimentally demostrated the MDI-EW scheme successfully for the class of two-photon polarization states: $\rho^v_{AB} \equiv (1-v)|\Psi^-\rangle_{AB}\langle\Psi^-| + (v/2)(|HH\rangle_{AB}\langle HH| + |VV\rangle_{AB}\langle VV|)$ $(0 \leq v \leq 1)$, using a six photon interference process.



Experimental demonstration of MDIEW [Xu et al., PRL **112**, 140506 (2014)]

Experimental demonstration of MDI-EW (continued)

- On the other hand, Nawareg et al. [Scientific Reports, DOI: 10. 1038/srep08048] have experimentally demostrated the MDI-EW scheme successfully for the class of two-photon polarization states: $\rho_{AB}^{p} \equiv p|\Psi^{-}\rangle_{AB}\langle\Psi^{-}| + ((1-p)/4)I_{4\times 4}$ $(0 \leq p \leq 1)$, (again) using a six photon interference process.



Experimental demonstration of MDIEW [Nawareg et al., SR

Experimental demonstration of MDI-EW (continued)

- Other than the entangled state generation processes, the two experimental set-ups are similar.
- In both the experiments, the referee uses a two-photon interference process to generate the single photon polarization states τ_s for Alice, and similarly for the states ω_t to be supplied to Bob.
- This accounts for the six photon requirement in each of these experiments.
- The witness operator being used in both the experiments: $W \equiv (1/2) I_{4\times 4} - |\Psi^-\rangle\langle\Psi^-|$.
- Due to the supply of the single photon states τ_s and ω_t, supression of the positive results $\langle \sigma_j^{(\alpha)} \otimes \sigma_j^{(\alpha)} \rangle_\rho$ (for $\alpha = +, -$) – unlike in the case of standard EW experiments – have been avoided in the present experiments.

Experimental demonstration of MDI-EW under noise

- We have introduced noise (theoretically) in the Bell state measurement part of both the experiments – not explicitly considered in the experiments – and verified that the corresponding separable states get witnessed as separable even in the presence of noise.
- The optical gadgets being used in both the experiments for the Bell state measurements are mainly: HWP, PBS, and photo-detectors.
- We have taken here lossy PBS by introding white noise. Noisy HWP has been considered by introducing error in the angle of rotation of the polarization axis. Noise in the photo-detectors have been introduced by incorporating detection inefficiency.

Universal entanglement witness process for two-qubits

Universal EW operator for two-qubits

- In the case of two-qubits, Augusiak et al. [*Phys. Rev. A* **77**, 030301 (2008)] provided a *state-independent* (*i.e.*, *universal*) hermitian operator W_u, acting on $(\mathbb{C}^2)^{\otimes 4} \otimes (\mathbb{C}^2)^{\otimes 4}$, such that $\mathrm{Tr}[W_u \rho_{AB}^{\otimes 4}] \equiv \det(\rho_{AB}^{T_B}) \geq 0$ if and only if ρ_{AB} is a (two-qubit) separable state.
- A local realization of W_u is of the form: $W_u = (1/24) I_{256\times 256} - (1/8)(\tilde{V}^{(4)} \otimes (\tilde{V}^{(4)})^T + (\tilde{V}^{(4)})^T \otimes \tilde{V}^{(4)}) + (1/6) I_{4\times 4} \otimes (\tilde{V}^{(3)} \otimes (\tilde{V}^{(3)})^T + (\tilde{V}^{(3)})^T \otimes \tilde{V}^{(3)}) + (1/8) V^{(2)} \otimes V^{(2)} - (1/4) I_{16\times 16} \otimes V^{(2)}$.
- Here $V^{(k)}$ is the swap operator: $V^{(k)}(|\phi_1\rangle \otimes |\phi_2\rangle \otimes \ldots \otimes |\phi_k\rangle) = |\phi_k\rangle \otimes |\phi_1\rangle \otimes \ldots \otimes |\phi_{k-1}\rangle$ and $\tilde{V}^{(l)}$'s are permutations in the same subsystems of $\rho^{\otimes 4}$.

Witnessing entanglement in unknown two-qubit state in MDI way

Witnessing entanglement in unknown two-qubit state in MDI way

- Assume now that the referee supplies states $\tau^{(s)}$ on $(\mathbb{C}^2)^{\otimes 4}$ to Alice and $\omega^{(t)}$ on $(\mathbb{C}^2)^{\otimes 4}$ to Bob.
- And four copies of a *unknown* two-qubit state ρ_{AB} are shared.
- Express now: $W_u = \sum_{s \in \mathcal{S}, t \in \mathcal{T}} \beta_{st} (\tau^{(s)})^T \otimes (\omega^{(t)})^T$.
- For four copies of any two-qubit state σ_{AB}: $I(\mu_{\sigma^{\otimes 4}}) = \sum_{s \in \mathcal{S}, t \in \mathcal{T}} \beta_{st} \mu_{\sigma^{\otimes 4}}(1, 1 | \tau^{(s)}, \omega^{(t)}) = \mathrm{Tr}[W_u (\sigma_{AB})^{\otimes 4}]/256$.
- So, $I(\mu_{\sigma^{\otimes 4}}) \geq 0$ iff σ is separable.
- Bartkiewicz et al. [PRA **91**, 032315 (2015)] provided an implementation scheme for universally witnessing two-qubit photon polarization states using W_n – not in MDI way.

Witnessing NPT-ness of unknown state in any given bi-partite system in MDI way

Universally witnessing NPT-ness in MDI way

- A two-qudit state ρ_{AB} is said to have PPT iff $\rho_{AB}^{T_B} \geq 0$. Otherwise it is said to have NPT.
- The characteristic eqn. for $\rho_{AB}^{T_B}$: $\sum_{\alpha=0}^{d^2} a_\alpha \lambda^{d^2-\alpha} = 0$ where the coefficients a_0, a_1, ..., a_{d^2} are respectively 1, $-\sum_i \lambda_i = -1$, $\sum_{i>j} \lambda_i \lambda_j = (1/2)(1 - \sum_i \lambda_i^2)$, ... (Newton-Girad formula).
- In operational form: $a_2 = \mathrm{Tr}[W_2 \rho_{AB}^{\otimes 2}]$ where $W_2 = (1/2)(I_{d^4 \times d^4} - V^{(2)})$.
- $a_3 = -(1/6)(1 - 3\sum_i \lambda_i^2 + 2\sum_i \lambda_i^3) = \mathrm{Tr}[W_3 \rho_{AB}^{\otimes 3}]$.
- Here $W_3 = -(1/6)(I_{d^6 \times d^6} - 3 I_{d^2 \times d^2} \otimes V^{(2)} + (\tilde{V}^{(3)} \otimes (\tilde{V}^{(3)})^T + (\tilde{V}^{(3)})^T \otimes \tilde{V}^{(3)}))$.
- etc. etc.

Universally witnessing NPT-ness in MDI way (continued)

- In order to thus calculate a_k in MDI way, k copies of the state should be shared, and the referee should supply states $\tau^{(s)}$ ($\omega^{(t)}$) from $(\mathbb{C}^{d_A})^{\otimes k}$ ($(\mathbb{C}^{d_B})^{\otimes k}$) to Alice (Bob).
- By looking at the signs of a_k's, one can then easily figure out whether ρ has PPT or NPT.

Conjecture about non-existence of universal MDI-EW in higher dimension

Conjecture

- We conjecture that if $d_A d_B > 6$, there can not exist one (or a finitely many) universal entanglement witness which can be realized in a MDI way: (**Conjecture 1**)
- Note that there is *no* PPT entangled state whenever $d_A d_B \leq 6$. So, universally witnessing the NPT-ness of an arbitrary state ρ_{AB} – with $d_A d_B \leq 6$ – in an MDI way is enough to witness entanglement in ρ_{AB} in an MDI way.
- The reason behind the aforesaid conjecture is another conjecture:
- There can not exist a universal EW (or, a finitely many EW operators) for all PPT entangled states of any given bipartite system: (**Conjecture 2**).

Motivation about the second conjecture

- Consider a bi-partite quantum system $A+B$, described by the Hilbert space $\mathcal{H}_{AB} \equiv \mathcal{H}_A \otimes \mathcal{H}_B$ with $\dim\mathcal{H}_A = \dim\mathcal{H}_B = d$.
- $\mathcal{D}_{AB} \equiv$ set of all the density matrices of $A+B$.
- $\mathcal{S}_{AB} \equiv$ set of all separable density matrices of $A+B$.
- $\mathcal{P}_{AB} \equiv$ set of all density matrices ρ_{AB} of $A+B$ for which $\rho_{AB}^{T_B} \geq 0$.
- $\tilde{\mathcal{P}}_{AB} \equiv$ set of all ρ_{AB} in $\mathcal{P}_{AB}$ with ρ_{AB} being entangled.
- Note that $\mathcal{P}_{AB}$ is a convex subset of $\mathcal{D}_{AB}$, while $\mathcal{S}_{AB}$ is a convex subset of $\mathcal{P}_{AB}$.
- $\tilde{\mathcal{P}}_{AB}$ is not convex.
- $\mathcal{P}_{AB} = \mathcal{S}_{AB}$ for $d = 2$.
- Thus, for $d = 2$, $\tilde{\mathcal{P}}_{AB} = \phi$, the null set.

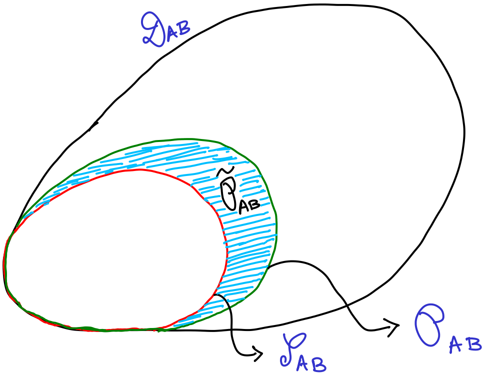
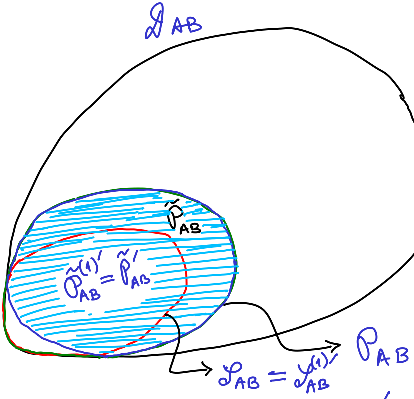


Fig. 5 : Structures of $\mathcal{P}_{AB}$, $\tilde{\mathcal{P}}_{AB}$, and $\mathcal{S}_{AB}$ in the presence of $\mathcal{D}_{AB}$

Motivation about the second conjecture (continued)

- $\mathcal{S}'_{AB} \equiv$ set of all convex combinations of elements of $\mathcal{S}_{AB}$.
- Thus we have: $\mathcal{S}'_{AB} = \mathcal{S}_{AB}$.
- $\tilde{\mathcal{P}}'_{AB} \equiv$ set of all convex combinations of elements of $\tilde{\mathcal{P}}_{AB}$.
- **Edge state:** ρ_{AB} in $\tilde{\mathcal{P}}_{AB}$ is an edge state iff the state $(\rho_{AB} + p\sigma_{AB})/(1+p)$ is in $\mathcal{S}_{AB}$ for all $p \in (0,1]$ and all $\sigma_{AB} \in \mathcal{P}_{AB}$.
- Edge states lie near the boundary of $\mathcal{S}_{AB}$.
- Edge states exist for all $d \geq 3$.
- This implies that $\tilde{\mathcal{P}}'_{AB}$ and $\mathcal{S}'_{AB}$ have non-null overlap: $\tilde{\mathcal{P}}'_{AB} \cap \mathcal{S}'_{AB} \neq \phi$ for $d \geq 3$.



$$\tilde{\rho}^{(1)'}_{AB} \cap \mathcal{S}^{(1)'}_{AB} \neq \phi$$

Fig. 6 : structures of $\mathcal{S}^{(1)'}_{AB}$ and $\tilde{\rho}^{(1)'}_{AB}$

Motivation about the second conjecture (continued)

- n is any positive integer.
- $\mathcal{S}_{AB}^{(n)'} \equiv$ set of all convex combinations of the states $\sigma_{AB}^{\otimes n}$ with $\sigma_{AB} \in \mathcal{S}_{AB}$.
- $\tilde{\mathcal{P}}_{AB}^{(n)'} \equiv$ set of all convex combinations of the states $\rho_{AB}^{\otimes n}$ with $\rho_{AB} \in \tilde{\mathcal{P}}_{AB}$.
- $\mathcal{S}_{A_n B_n} \equiv$ set of all separable states on $\mathcal{H}_A^{\otimes n} \otimes \mathcal{H}_B^{\otimes n}$.
- It is most likely that $\mathcal{S}_{A_n B_n} \cap \tilde{\mathcal{P}}_{AB}^{(n)'} \neq \phi$ for all n with $d \geq 3$ (possibly because of existence of edge states).
- **Conjecture 3:** $\mathcal{S}_{AB}^{(n)'} \cap \tilde{\mathcal{P}}_{AB}^{(n)'} \neq \phi$ for all n with $d \geq 3$.
- Conjecture 3 is true for $n = 1$.

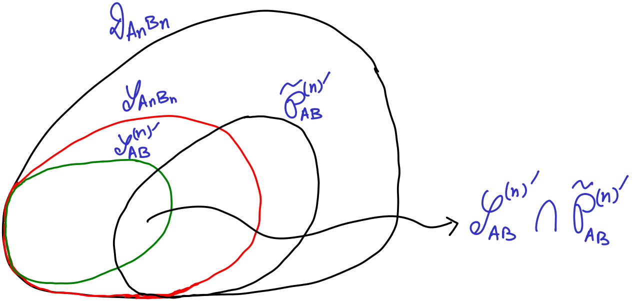
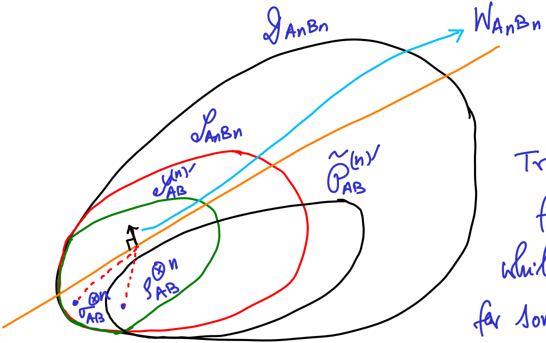


Fig. 7 : Structures of $\mathcal{S}_{A_nB_n}$, $\tilde{\mathcal{P}}_{AB}^{(n)'}$, $\mathcal{S}_{AB}^{(n)'}$ with respect to $\mathcal{D}_{A_nB_n}$: the set of all density matrices on $\mathcal{H}_A^{\otimes n} \otimes \mathcal{H}_B^{\otimes n}$

Implication of the 3rd conjecture

- Validity of conjecture 3 implies the *non-existence* of any hermitian operator $W_{A_nB_n} : \mathcal{H}_A^{\otimes n} \otimes \mathcal{H}_B^{\otimes n} \to \mathcal{H}_A^{\otimes n} \otimes \mathcal{H}_B^{\otimes n}$ for which $\mathrm{Tr}\left[\rho_{AB}^{\otimes n} W_{A_nB_n}\right] < 0$ for <u>some</u> $\rho_{AB} \in \tilde{\mathcal{P}}_{AB}$ together with $\mathrm{Tr}\left[\sigma_{AB}^{\otimes n} W_{A_nB_n}\right] \geq 0$ for <u>all</u> $\sigma_{AB} \in \mathcal{S}_{AB}$ – irrespective of the choice of n.
- Thus, validity of conjecture 3 implies that there can not exist a universal EW (or, a finitely many EWs) which can detect entanglement in all the PPT (bound) entangled states of $A + B$ whenever $d \geq 3$.
- Thus, validity of conjecture 3 automatically implies validity of conjecture 2, which, in turn, implies the non-existence of a MDI universal entanglement witness operator for all the PPT (bound) entangled states of $A + B$ – validity of conjecture 1.



$\mathrm{Tr}[W_{A_nB_n}\, \rho_{AB}^{\otimes n}] < 0$

for all $\rho_{AB} \in \tilde{P}_{AB}$

while $\mathrm{Tr}[W_{A_nB_n}\, \sigma_{AB}^{\otimes n}] < 0$

for some $\sigma_{AB} \in \mathcal{S}_{AB}$

Fig. 8: Location of $W_{A_nB_n}$

Verification of the 3rd conjecture

- It appears to be quite difficult to verify conjecture 3 directly.
- One may try to verify whether for any given $\rho_{A_nB_n} \in \tilde{\mathcal{P}}_{AB}^{(n)\prime}$, there exists some $\sigma_{A_nB_n} \in \mathcal{S}_{AB}^{(n)\prime}$ such that $\mathrm{Tr}\left[\mathcal{O}_{A_nB_n}\rho_{A_nB_n}\right] = \mathrm{Tr}\left[\mathcal{O}_{A_nB_n}\sigma_{A_nB_n}\right]$ for a complete set of linearly independent observables $\mathcal{O}_{A_nB_n} : \mathcal{H}_A^{\otimes n} \otimes \mathcal{H}_B^{\otimes n} \to \mathcal{H}_A^{\otimes n} \otimes \mathcal{H}_B^{\otimes n}$.
- Even verification of this one may turn out to be difficult.

Conclusion

Conclusion

- Based on the knowledge of the dimension of the individual sub-systems and relying on the supply of several copies of the state on demand, we provided here a prescription on how to detect NPT/PPT-ness of an arbitrary bi-partite state in a measurement device independent way.
- In case the bi-partite system is known *apriori* to be a two-qubit or a qubit-qutrit system, our method provided a scheme for universal entanglement detection in a measurement device independent way.
- In case the total dimension of the bi-partite system is higher than six and in case the unknown bi-partite state has PPT, we conjecture that its entanglement can not be detected in a measurement device independent way.

Conclusion (continued)

- Our noise analysis of the Bell-state measurent scenario in both the experimental demonstrations of MDIEW are in conformity with the demand of the measurement device independence of the entanglement witness scheme of Branciard et al. [*Phys. Rev. Lett.* **110**, 060405 (2013)].

Thanks!