Witnessing Single-System Steering for Quantum Information Processing

Che-Ming Li\textsuperscript{1,2}, Yueh-Nan Chen\textsuperscript{3}, Neill Lambert\textsuperscript{2}, Ching-Yi Chiu\textsuperscript{1}, and Franco Nori\textsuperscript{2,4}

\textsuperscript{1}Department of Engineering Science, National Cheng Kung University, Tainan 701, Taiwan
\textsuperscript{2}CEMS, RIKEN, Wako-shi, Saitama 351-0198, Japan
\textsuperscript{3}Department of Physics and National Center for Theoretical Sciences, National Cheng Kung University, Tainan 701, Taiwan
\textsuperscript{4}Department of Physics, University of Michigan, Ann Arbor, Michigan 48109-1040 USA

(Dated: November 13, 2014)

Einstein-Podolsky-Rosen (EPR) steering describes how different ensembles of quantum states can be remotely prepared by measuring one particle of an entangled pair. Here, inspired by this bipartite concept, we investigate quantum steering for single quantum d-level systems (qudits) and devise several quantum witnesses to efficiently verify the steerability therein, which are applicable both to single-system steering and EPR steering. In the single-system case our steering witnesses enable the unambiguous ruling-out of generic classical means of mimicking steering. Ruling out ‘false-steering’ scenarios has implications for securing channels against both cloning-based individual attack and coherent attacks when implementing quantum key distribution using qudits. In addition, we show that these steering witnesses also have applications in quantum information, in that they can serve as an efficient criterion for the evaluation of quantum logic gates of arbitrary size. Finally, we describe how the non-local EPR variant of these witnesses also function as tools for identifying faithful one-way quantum computation and secure entanglement-based quantum communication.

PACS numbers: 03.65.Ud, 03.67.Dd

\textit{Introduction}.—Einstein-Podolsky-Rosen (EPR) steering was originally introduced by Schrödinger\textsuperscript{2} in response to the EPR paradox. Such steering is the ability of one party, Alice, to affect the state of another remote party, Bob, through her choice of measurement. This relies on both the entanglement of the pair shared between Alice and Bob and the measurement settings chosen for each particle of the pair. Recently, the concept of EPR steering has been reformulated in terms of a task in quantum information\textsuperscript{3} showing that two parties can share entanglement even if the measurement devices of one of them are uncharacterized (or untrusted), and has applications in one-sided device-independent quantum key distribution (QKD).\textsuperscript{3} This new formulation illustrates an strict hierarchy between Bell non-locality, steering and entanglement. It is worth noting that, like Bell inequalities and entanglement witnesses, which have been widely used to verify quantum correlations, EPR steering inequalities\textsuperscript{4} and steering measures\textsuperscript{4} have been introduced to detect the steerability of bipartite quantum systems. In addition, EPR steering has stimulated investigations into a range of other types of quantum steering\textsuperscript{7,10}.

Here, we primarily focus on a new single-system analogue\textsuperscript{11} of EPR steering and map it to several quantum information tasks (see Fig.\textsuperscript{1}). In this work we devise two quantum witnesses to identify genuine single-system quantum steering in the presence of errors (either from the environment or third-party eavesdropping) and which can be applied to quantum computation and quantum communication using qudits (systems of arbitrary dimension). We conclude by discussing how these witnesses can also be applied in the standard non-local EPR setting.

\textbf{Quantum steering for single systems}.—In the scenario of single-system quantum steering, Alice’s ability to affect the quantum state Bob has access to is based on both her ability to prepare an arbitrary quantum state to send to Bob and her knowledge, if any, about the state Bob finally receives (which may differ from her prepared state, for various reasons). If Alice has full information about the quantum system Bob is holding, she is capable of steering this system into an arbitrary state. As
Alice can follow two steps to achieve this.

First, Alice prepares a specific state of a qudit, a multi-level particle, with a given initial state state $\rho_s$ generated from some quantum source, before sending it to Bob, by performing complementary measurements $A_i$ for $i = 1, 2$. Once the particle is measured with a chosen $A_i$, $\rho_s$ becomes $\hat{a}_i \equiv |a_i\rangle \langle a_i|$ for $a \in \{0, 1, ..., d - 1\}$, where the $d$ states constitutes an orthonormal basis $\{|a_i\rangle\}$. The set of states $\{|a_2\rangle\}$ is complementary to the state set $\{|a_1\rangle\}$ by defining $|a_2\rangle = 1/\sqrt{d} \sum_{a'=0}^{d-1} \omega^{a'a} |a'_1\rangle$, with $\omega = \exp(i2\pi/d)$. As with the role of entanglement played in EPR steering, the essence of single system steerability is the quantum characteristics of the states $\hat{a}_i$, for example, quantum coherence and uncertainty relations.

Second, the particle in the state $\hat{a}_i$ is then sent to Bob. Here Bob will not know the state of particle $\hat{a}_i$ sent from Alice unless he performs state tomography on the particle. To steer Bob’s state $\hat{a}_i$ into other quantum states $U(\hat{a}_i) \equiv U\hat{a}_i U^\dagger$, Alice can publicly, via a classical channel, ask Bob to apply the unitary operator $U$ on $|a_i\rangle$. While the quantum operation $U$ is announced publicly, the state $U(\hat{a}_i)$ is still unknown to Bob. It is clear that Alice has complete knowledge about the quantum system held by Bob since the state $\rho_s$, the measurement $A_i$ and the subsequent operation $U$ are designed by Alice. When Bob performs measurements on his particle after the operation $U$, his two complementary measurements $B_{a(i)}$ for $i = 1, 2$ are specified by the orthonormal bases $\{|b_{a(i)}\rangle\} \equiv U |b_i\rangle |b \in v\}$ with the set of results $\{b_{a(i)}\}$.

In normal EPR steering, Alice can steer Bob’s state into arbitrary target states only when the pair of particles are entangled and she knows the state structure of the entangled pair shared between them. The state information enables Alice to choose a proper measurement basis to demonstrate steering. This is the same for single-system steering. Such an equivalence means Bob cannot tell whether his quantum system is one part of the entangled pair or a single particle pre-prepared and sent from Alice (though a scheme can be devised to distinguish these two [10]).

In an ideal case, the state received by Bob is the same as the initial state $\hat{a}_i$ prepared by Alice under the transformation $U$. In practical situations, however, noise from the environment or other artificial effects (for example, interference from a third party) introduce an unknown source of randomness. In order to explicitly qualify whether Alice can steer the states of the particles eventually held by Bob, and rule out third-party eavesdropping, classical mimicry of the channel, or to qualify the quality of the channel itself, we consider the following generic classical means of describing state preparation, transitions between states, and the limits to which they can influence the measurement results of Bob.

First, we assume that the state of the particle sent by Alice possesses no steerability and can be described by a classical realistic theory which predicts the particle is in a state described by a fixed set $\{a_1, a_2\}$. In the quantum case these are complementary bases, but in the classical realism case they represent well defined sets of states of the system which can be independently measured. Under this assumption any measurement results will obey the standard relationship between marginal and conditional probabilities,

$$P(a_1)P(a_2|a_1) = P(a_2)P(a_1|a_2).$$

Second, we assume that the particle’s state can change, while it is being transmitted from Alice to Bob, from $a_i$ to an unknown state described by $\lambda$ with a transition probability $P(\lambda|a_i)$. We denote this unknown state as $\rho_\lambda$. The state Bob holds finally is then

$$\rho_B(i) = \sum_{a=0,1,...,d-1} \sum_{\lambda} P(a_i) P(\lambda|a_i) \rho_\lambda,$$

where $P(a_i)$ is the probability of observing $a$ under the measurement $A_i$.

Equation (1) can also be extended to cases involving state transitions. The joint probability of finding $(a_1, a_2)$ and observing $\lambda$ as the final state can be explicitly represented by

$$P[(a_1, a_2), \lambda] = P(a_1)P(\lambda|a_1)P(a_2|a_1, \lambda) = P(a_2)P(\lambda|a_2)P(a_1|\lambda, a_2),$$

When summing over all $a_1$ and $a_2$, Eq. (3) becomes

$$P(\lambda) = \sum_a P(a_i)P(\lambda|a_i),$$

as well as

$$\sum_a P(a_1)P(\lambda|a_1) = \sum_a P(a_2)P(\lambda|a_2).$$

With the above classical realistic description of Alice’s states, the state received by Bob becomes independent of the measurement setting (basis set) chosen by Alice, i.e.,

$$\rho_B(1) = \rho_B(2) = \sum_\lambda P(\lambda) \rho_\lambda,$$

implying that Bob always has the same state whatever measurement $A_i$ and operation $U$ Alice designs. This means Alice cannot steer Bob’s states. We call the states with the feature (9) unsteerable. The situations where this happens are when either Alice never had access to the particle sent to Bob in the first place, and was randomly generating her measurement results, or when either the interference of a third party, or noise from the environment, erased Alice’s influence. As we discuss below,
in some sense the above proof can be seen as equivalent to that used in the derivation of EPR steering inequalities, where Alice’s measurement results are not trusted and assumed to be equivalent to a classical distribution.

Finally, if Alice’s state and the unknown states \( \rho_\lambda \) are described by a classical theory of realism, and thus only classically correlated with Bob’s results, then the descriptions Eqs. (1), (3) and (4) are applicable to \( \rho_\lambda \) as well. However, here Bob’s measurement results are assumed to be based on measurements on a quantum particle. Thus the expectation values of the two mutually unbiased measurements \( B_{u(1)} \) and \( B_{u(2)} \) with respect to the unknown quantum states \( \rho_\lambda \) obey the quantum uncertainty relation in the entropic form

\[
H(B_{u(1)}|\lambda) + H(B_{u(2)}|\lambda) \geq \log_2(d),
\]

where \( H(B_{u(i)}|\lambda) = -\sum_{a=0}^{d-1} P(b_{u(i)}|\lambda) \log_2 P(b_{u(i)}|\lambda). \)

Quantum steering witnesses.—In order to distinguish steerability from the results mimicked by the methods based on the classical theories considered above, in what follows we will introduce two novel quantum witnesses which we call steering witnesses, of the from

\[
W > \alpha_R,
\]

where \( W \) is the kernel of the witness and \( \alpha_R \) is the maximum value of the kernel supported by classical theories. For ideal steering \( W \), will be maximized.

The kernel of our first steering witness is

\[
W_{\text{dU}} = \sum_{i=1}^{2} \sum_{a=0}^{d-1} P(a_i, b_{u(i)}).
\]

For ideal steering the maximum value for the kernel is \( W_{\text{dU}} = 2 \). Whereas, for the states described by Eq. (2), the expectation value of the kernel \( W_{\text{dU}} \) becomes

\[
W_{\text{dU},R} = \sum_{i=1}^{2} \sum_{a=0}^{d-1} \text{Tr} \left[ \hat{a}_{u(i)} \rho_\lambda | P(\lambda|a_i) P(a_i) \right],
\]

where \( \hat{a}_{u(i)} \equiv U(a_i). \) This can be further manipulated to give

\[
W_{\text{dU},R} \leq \sum_{\lambda} \sum_{a=0}^{d-1} P(\lambda) \left( \text{Tr}[\hat{m}_1 \rho_\lambda] + \text{Tr}[\hat{n}_2 \rho_\lambda] \right) \leq 1 + 1/\sqrt{d},
\]

where \( m, n \in \mathbf{v} \). The first inequality is derived from the relations (6) and (8), and the classical bound \( \alpha_R = 1 + 1/\sqrt{d} \) is obtained by determining the maximum eigenvalue of the operator \( \hat{m}_1 + \hat{n}_2 \). Thus the quantum steering witness reads

\[
W_{\text{dU}} > 1 + \frac{1}{\sqrt{d}}
\]

Thus, for any states sent from Alice which obey the realistic theory [Eq. (1)] the witness will not violate this bound.

Our second steering witness is based on the mutual information between Alice and Bob. From the point of view of information shared between sender and receiver, the ability for Alice to steer Bob’s state is confirmed if the mutual dependence between the measurement results of Alice and Bob is stronger than the dependence of Bob’s measurement outcomes on the unknown states \( \rho_\lambda \) [Eq. (2)]. This condition of steerability can be represented in terms of the mutual information as follows,

\[
I(B_{u(1)};A_1) + I(B_{u(2)};A_2) > I(B_{u(1)};\{\lambda\}) + I(B_{u(2)};\{\lambda\}).
\]

(11)

From the basic definition of mutual information, Eq. (11) implies that

\[
\sum_{i=1}^{2} \sum_{a=0}^{d-1} P(a_i) H(B_{u(i)}|a_i) < \sum_{i=1}^{2} \sum_{\lambda} P(\lambda) H(B_{u(i)}|\lambda).
\]

(12)

Imposing the condition (10) on the state \( \rho_\lambda \), we obtain the second steering witness of the form

\[
W_{\text{enpU}} = -\sum_{i=1}^{2} \sum_{a=0}^{d-1} P(a_i) H(B_{u(i)}|a_i) > \log_2 \left( \frac{1}{d} \right),
\]

(13)

In addition to the steering witnesses devised here, violating the temporal steering inequality (11) can serve as an indicator of single-system steering. In the Appendix, we show that this inequality can be derived from the classical conditions (1) and (2), which provides a strict meaning of violating that inequality.

Quantum cryptography.—Let us proceed to concretely illustrate how these steering witnesses behave when there exist external noise sources when a qudit is sent from Alice to Bob. When the state of the qudit sent from Alice to Bob changes from the state \( \hat{a}_i \) to a state \( U_{\text{cl}}(\hat{a}_i) \) through a channel \( U_{\text{cl}} \), the value of the witness kernel \( W_{\text{dU}} \) is

\[
W_{\text{dU}} = \sum_{i=1}^{2} \sum_{a=0}^{d-1} P(a_i) F(a, u(i)),
\]

(14)

where the probabilities \( P(a_i) = \text{Tr} \left[ \rho_a \hat{a}_i \right] \) and \( F(a, u(i)) = \text{Tr} \left[ U_{\text{cl}}(\hat{a}_i) \rho_a \hat{a}_i \right] \). Here, \( F(a, u(i)) \) is called the state fidelity between the ideal state \( \hat{a}_u(i) \) and the actual state \( U_{\text{cl}}(\hat{a}_i) \). If all the states before Bob’s measurements \( U_{\text{cl}}(\hat{a}_i) \) are identical to the states \( \hat{a}_u(i) \), i.e., \( F(a, u(i)) = 1 \), it is clear that \( W_{\text{dU}} = 2 \). Whereas, if there exists an error source which reduces the state fidelity \( F(a, u(i)) \), the value of the witness kernel will decrease as well. Let us assume that this error is introduced by a quantum cloning machine. The cloner makes all the state fidelities under the same measurement setting have the same value, say \( F(a, u(1)) = F \) and \( F(a, u(2)) = \bar{F} \), for all \( a \in \text{v} \). Then Eq. (14) becomes \( W_{dU} = F + \bar{F} \). When the cloning machine copies equally well the states of both bases, the state fidelities in both bases are identical, \( F = \bar{F} \). If Alice wants to demonstrate steering of Bob’s particle in the presence of such eavesdropping, they have to find \( W_{\text{dU}} = 2F > 1 + 1/\sqrt{d} \), or alternatively the state fidelity must satisfy the condition

\[
F > \frac{1}{2} \left( 1 + \frac{1}{\sqrt{d}} \right). \]
It is equivalent to saying that the disturbance, \( D = 1 - F \), or error rate, has to be lower than a certain upper bound

\[
D_{\text{ind}} = \frac{1}{2} \left( 1 - \frac{1}{\sqrt{d}} \right).
\]

This bound is exactly the same as the well-known security threshold derived from the condition on nonzero generating rate of secret keys under individual attacks using quantum cloning machines [11].

For the second steering witness [10], it is worth noting that the conditional entropy can be represented by \( H(B_{u(i)}|a_i) = -F(a, u(i)) \log_2 F(a, u(i)) - \sum_{a \neq a} \Omega(b_{u(i)}a_1) \log_2 \Omega(b_{u(i)}a_1) \), where \( \Omega(b_{u(i)}a_1) \) denotes the probability of error state transition from \( a_i \) to \( b_{u(i)} \) for \( b \neq a \). When taking the same condition on the quantum cloning machine as for the criterion [15] into consideration and assuming that the possible errors are equiprobable \( \Omega(b_{u(i)}a_1) = (1 - F)/(d - 1) \), we derive a second criterion on the state fidelity \( F \) from the second witness [14]

\[
\tilde{F} > \frac{1}{2} \log_2(d),
\]

where \( \tilde{F} \equiv F \log_2(F) + (1 - F) \log_2[(1 - F)/(d - 1)] \). This provides the upper bound, \( D_{\text{coh}} \), on the error rate under coherent attacks. If the disturbance \( D \) is smaller than \( D_{\text{coh}} \), then Alice can steer Bob’s state. For example, we have \( D_{\text{coh}} = 11.00\% \) and \( 15.95\% \) for \( d = 2 \) and \( 3 \), respectively. For large \( d \), the upper bound is closed to \( 50\% \). Interestingly, the upper bound \( D_{\text{coh}} \) derived from the steering witness [13] exactly coincides with the result obtained from the limit on the sum of Bob’s and the eavesdropper’s information for coherent attacks on a qudit sequence [11].

Quantum computation.—When the measured witness kernels are larger than the maximum values \( \alpha_R \) predicted by classical theories, the real process describing the state transitions \( \mathcal{U}_{rel} \) can be said to be close to the target unitary quantum operations \( \mathcal{U} \) that Alice and Bob expect. This evaluation is based on whether the process \( \mathcal{U}_{rel} \) goes beyond the classical descriptions of the input states [11] and their state evolution [14], and gives us a tool by which to evaluate a given real transformation. To consider how to evaluate such a transformation further, we rewrite the witness [10] as

\[
\frac{1}{d} \sum_{i=1}^{2} \sum_{a=0}^{d-1} \text{Tr}[\mathcal{U}_{rel}(\hat{a}_i)\check{a}_{u(i)}] > 1 + \frac{1}{\sqrt{d}}.
\]

Here, without losing any generality, we assume that \( \rho_s = I/d \), where \( I \) is the identity matrix. The quantity \( F_{\hat{a}_1 \rightarrow \check{a}_{u(i)}} = \frac{1}{2} \sum_{a=0}^{d-1} \text{Tr}[\mathcal{U}_{rel}(\hat{a}_1)\check{a}_{u(i)}] \) can be considered as an average fidelity between \( \mathcal{U}_{rel}(\hat{a}_1) \) and \( \check{a}_{u(i)} \) over all the \( d \) states. With the average state fidelities \( F_{\hat{a}_1 \rightarrow \check{a}_{u(i)}} \) for the complementary bases \( A_1 \) and \( A_2 \), one can obtain the lower bound of the process fidelity \( F_{\text{process}} = \text{Tr}[\mathcal{U}_{rel}d] \) by

\[
\frac{1}{d} \sum_{i=1}^{2} \sum_{a=0}^{d-1} \text{Tr}[\mathcal{U}_{rel}(\hat{a}_i)\check{a}_{u(i)}] > 1 + \frac{1}{\sqrt{d}}.
\]

Hence, using the criterion [12] together with the above relation, we obtain a condition for a faithful quantum process in terms of process fidelity

\[
F_{\text{process}} > \frac{1}{\sqrt{d}}.
\]

The above results [15] and [14] can be efficiently implemented with the minimum two measurement settings \((A_1, B_{u(1)})\) and \((A_2, B_{u(2)})\). This is especially useful to evaluate experimental implementations of quantum logic gates of arbitrary size. Let us take a two-qubit gate as an example. Two qubits can be considered or recast as a single system with a level number \( d = 2^2 = 4 \). The entanglement capability of a two-qubit entangling gate, like a controlled-NOT operation, can be defined by the minimal amount of entanglement that can be generated by the operation \( \mathcal{U}_{rel} \). In terms of the concurrence \( C \), it is found that \( C \geq 2F_{\text{process}} - 1 \). For a nontrivial gate, we require \( C > 0 \), which implies that \( F_{\text{process}} > 1/2 \) [12]. Our condition [13] derived from the steering witness coincides with this criterion. For three-qubit gate \( (d = 2^3) \), the criterion on the process fidelity is \( F_{\text{process}} > 1/\sqrt{8} \approx 35.36\% \). For example, the process fidelity of the experimental quantum Toffoli gate with trapped ions reported in [13] is \( F_{\text{process}} = 66.6(4)\% \), which can be identified as being functional according to our proposed criterion. When the number \( N \) of qubits increases, the classical bound will decrease with \( \sqrt{d} = 2^{N/2} \) and approach zero when \( N \) is large.

The second steering witness [13] can be used to evaluate experimental implementations of quantum gates. To do so one needs to consider the conditional entropy \( H(B_{u(i)}|a_i) \), which has no direct connection to the process fidelity like Eq. [15]. However, when using the same conditions as \( D_{\text{coh}} \), to consider the quality of gate operations under coherent attacks, one can obtain the condition on \( F_{\text{process}} \) in terms of \( D_{\text{coh}} \)

\[
F_{\text{process}} > 1 - 2D_{\text{coh}},
\]

which is tighter than the criterion [15]. Again, taking two-qubit gates as an example, we have the condition \( F_{\text{process}} > 62.14\% \). The relation \( F = F_{\hat{a}_1 \rightarrow \check{a}_{u(i)}} = F_{\hat{a}_2 \rightarrow \check{a}_{u(i)}} \) is used above. Alternatively, the gate can be also qualified if the average state fidelity satisfies \( F > 1 - D_{\text{coh}} \). Table I summarizes the above two conditions on \( F_{\text{process}} \).

EPR steering witnesses and applications.—As discussed above, traditional EPR-steering and single-system-steering scenarios mirror each other. In the language we use this can be understood from the fact that, by changing the role of \( \lambda \) (from that of variables for describing correlations between Bob and Alice’s results via unknown states to hidden random variables describing correlations between for Alice’s classical state and Bob’s
TABLE I. A summary of the steering witnesses for quantum information processing. The criteria derived from steering witnesses for secure quantum communications and faithful quantum computations are represented in terms of the state fidelity $F$ and process fidelity $F_{\text{process}}$, respectively.

| Witness \ Task | Quantum cryptography | Quantum computation |
|----------------|----------------------|--------------------|
| $W_{\text{det}} > 1 + \frac{1}{\sqrt{d}}$ | $F > \frac{1}{2}(1 + \frac{1}{\sqrt{d}})$ | $F_{\text{process}} > \frac{1}{\sqrt{d}}$ |
| $W_{\text{ent}} > -\log_2(d)$ | $\tilde{F} > -\frac{1}{2}\log_2(d)$ | $F_{\text{process}} > 1 - 2D_{\text{coh}}$ |

quantum one), both steering witnesses \cite{10} and \cite{13} can be used to detect EPR steering for bipartite $d$-level systems shared between Alice and Bob. However, the converse is also true, such that EPR steering inequalities, for example, the inequalities used in the experiments \cite{11}–\cite{13}, can serve as witnesses for single-system steering, as discussed with the linear and entropy temporal steering inequalities in our earlier work \cite{10} (Appendix).

When using the bipartite counterpart of steering witnesses \cite{10}–\cite{13} for quantum communication, one obtains security criteria for quantum channels that is the same as the single-system case, which can thus be considered as a $d$-level extension of one-sided device-independent QKD \cite{4}. Similarly, the EPR steering witnesses give criteria of computation performance for quantum gates realized in one-way modes \cite{16}. In this one-way computing model, a quantum gate $U$ can be encoded in a bipartite maximally-entangled state \cite{17}

$$\frac{1}{\sqrt{d}} \sum_{a=0}^{d-1} |a_i\rangle \langle Inu(i)|,$$

(21)

where $|Inu(i)\rangle \equiv U |Ina_i\rangle$, and $|Ina_i\rangle$ is the input state of the quantum gate $U$. A readout of the gate operation, $|Inu(i)\rangle$, depends on the measurement result $a_i$, which is just the effect of EPR steering. Hence our EPR steering witnesses are capable of indicating reliable gate operations implemented in the presence of uncharacterized measurement devices with output $a_i$.

Conclusion and outlook.—We discussed the concept of quantum steering for single quantum systems and pointed out its role in quantum information processing. We derived two quantum witnesses to detect such steering. These witnesses ensure secure quantum key distribution using qudits and provide novel criteria for efficiently evaluating experimentally quantum logic gates of arbitrary computing size (see Table I). Moreover, the bipartite counterparts of our steering witnesses can detect EPR steerability of bipartite $d$-level systems, and have novel uses for evaluating one-way quantum computing and quantum communication with entangled qudits. It may be interesting to investigate further the connection between single-system steering and other types of quantum steering such as one-way steering \cite{3}–\cite{6} and genuine multipartite EPR steering \cite{3}.

Appendix.—The kernel of the temporal steering inequality reads

$$S_N \equiv \sum_{i=1}^{N} E[(B_{i,t;a})^2_{A_i,t;A}],$$

(22)

where

$$E[(B_{i,t;b})^2_{A_i,t;A}] = \sum_{a=0}^{1} P(A_i,t;A) \langle B_{i,t;b} \rangle^2_{A_i,t;A} = a,$$

(23)

and $N = 2$ or $3$ is the number of measurement for Alice and Bob. Note that this kernel is originally introduced to show EPR steering \cite{12}. The probability of measuring $A_i = a$ at the time $t_A$ is denoted by $P(A_i,t;A)$. The expectation value about Bob’s measurement at the time $t_B$, conditioned on the measurement result of Alice, is defined by

$$\langle B_{i,t;b} \rangle_{A_i,t;A} = a = \sum_{b=0}^{1} (-1)^b P(B_{i,t;b} = b|A_i,t;A = a).$$

To obtain the upper bound derived from generic classical means, we firstly introduce the final state of Bob \cite{2} into the above equation and then have

$$\langle B_{i,t;b} \rangle_{A_i,t;A} = a = \sum_{b=0}^{1} (-1)^b \sum_{\lambda} P(B_{i,t;b} = b|\lambda)P(\lambda|A_i,t;A = a) \langle B_{i,t;b} \rangle_\lambda.$$

(24)

Then it is clear that

$$E[(B_{i,t;b})^2_{A_i,t;A}] \leq \sum_{a=0}^{1} \sum_{\lambda} P(A_i,t;A) \langle B_{i,t;b} \rangle^2_{A_i,t;A} = a \langle B_{i,t;b} \rangle^2_{A_i,t;A} = a.$$

Secondly, we use the realistic condition on the state description \cite{11} together with the state transition \cite{11} and \cite{12} to obtain

$$P(\lambda) = \sum_{a=0}^{1} P(A_i,t;A) = a P(\lambda|A_i,t;A = a,$$

(25)

for all measurements $i$. Thus the temporal inequality is

$$S_N \leq \sum_{1=1}^{N} \sum_{\lambda} P(\lambda) \langle B_{i,t;b} \rangle^2_{A_i,t;A} \leq \sum_{\lambda} P(\lambda) = 1.$$

(26)

* cmli@mail.ncku.edu.tw
A one-way quantum computer relies on genuine multipartite cluster states [16] to perform gate operations. Here the state $|\Psi\rangle$ for one-way quantum computing is the Schmidt form of cluster states with respect to a fixed bipartition which splits the total systems into measurement part and readout of quantum gate. The Schmidt rank of the state $|\Psi\rangle$, $d$, then represents the size of computation. For example [18], a four-qubit cluster state can be used to implement quantum circuit composed of two-qubit gates, and its Schmidt rank is $d = 4$ for such a bipartition.

1. E. Schrödinger, Proc. Cambridge Philos. Soc. 31, 553 (1935); 32, 446 (1936).
2. A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. 47, 777 (1935).
3. H. M. Wiseman, S. J. Jones, and A. C. Doherty, Phys. Rev. Lett. 98, 140402 (2007).
4. C. Branciard, E. G. Cavalcanti, S. P. Walborn, V. Scarani, and H. M. Wiseman, Phys. Rev. A 85, 010301(R) (2012).
5. E. G. Cavalcanti, S. J. Jones, H. M. Wiseman, and M. D. Reid, Phys. Rev. A 80, 032112 (2009).
6. P. Skrzypczyk, M. Navascues, and D. Cavalcanti, Phys. Rev. Lett. 112, 180404 (2014).
7. S. L. W. Midgley, A. J. Ferris, and M. K. Olsen, Phys. Rev. A 81, 022101 (2010).
8. J. Bowles, T. Vértesi, M. T. Quintino, and N. Brunner, Phys. Rev. Lett. 112, 200403 (2014).
9. Q. Y. He and M. D. Reid, Phys. Rev. Lett. 111, 250403 (2013).
10. Y.-N. Chen, C.-M. Li, N. Lambert, S.-L. Chen, Y. Ota, G.-Y. Chen, and F. Nori, Phys. Rev. A 89, 032112 (2014).
11. N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. 88, 127902 (2002).
12. H. F. Hofmann, Phys. Rev. Lett. 94, 160504 (2005).
13. T. Monz, K. Kim, W. Hnsel, M. Riebe, A. S. Villar, P. Schindler, M. Chwalla, M. Hennrich, and R. Blatt, Phys. Rev. Lett. 102, 040501 (2009).
14. D. J. Saunders, S. J. Jones, H. M. Wiseman, and G. J. Pryde, Nat. Phys. 6, 845 (2010).
15. D.-H. Smith, G. Gillett, M. P. de Almeida, C. Branciard, A. Fedrizzi, T. J. Weinhold, A. Lita, B. Calkins, T. Gerrits, H. M. Wiseman, S. W. Nam, and A. G. White, Nat. Commun. 3, 625 (2012).
16. H. J. Briegel and R. Raussendorf, Phys. Rev. Lett. 86, 910 (2001); R. Raussendorf and H. J. Briegel, ibid. 86, 5188 (2001).
17. A one-way quantum computer relies on genuine multipartite cluster states [16] to perform gate operations. Here the state $|\Psi\rangle$ for one-way quantum computing is the Schmidt form of cluster states with respect to a fixed bipartition which splits the total systems into measurement part and readout of quantum gate. The Schmidt rank of the state $|\Psi\rangle$, $d$, then represents the size of computation. For example [18], a four-qubit cluster state can be used to implement quantum circuit composed of two-qubit gates, and its Schmidt rank is $d = 4$ for such a bipartition.
18. P. Walther, K. J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer and A. Zeilinger, Nature (London) 434, 169 (2005); K. Chen, C.-M. Li, Q. Zhang, Y.-A. Chen, A. Goebel, S. Chen, A. Mair, and J-W. Pan, Phys. Rev. Lett. 99, 120503 (2007).