Analytic semi-device-independent entanglement quantification for bipartite quantum states

Zhaohui Wei* and Lijinzhi Lin
Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, China

(Received 22 January 2019; revised 1 February 2020; accepted 17 February 2021; published 17 March 2021)

We define a property called nondegeneracy for Bell inequalities, which describes the situation that in a Bell setting, if a Bell inequality and involved local measurements are fixed, any quantum state with a given dimension and its orthogonal quantum state cannot violate remarkably the inequality simultaneously. By choosing a proper nondegenerate Bell inequality, we prove that for an unknown bipartite quantum state of given dimension, based on the measurement statistics only, we can provide an analytic lower bound for the entanglement of formation or even the distillable entanglement, making the whole process semi device independent. We characterize the mathematical structure of nondegeneracy, and prove that quite a lot of well-known Bell inequalities are nondegenerate. We demonstrate our approach by quantifying entanglement for qutrit-qutrit states based on their violations of the Collins-Gisin-Linden-Masser-Popescu inequality.

DOI: 10.1103/PhysRevA.103.032215

I. INTRODUCTION

It has been well known that entanglement is a major computational resource for quantum information processing tasks, thus certifying entanglement for unknown quantum states reliably in quantum laboratories is a fundamental and important problem. For small quantum systems tomography is a possible solution [1,2], but as the problem size grows, the cost of tomography goes up exponentially, making this approach infeasible. In this situation, one can instead use the idea of an entanglement witness to detect entanglement [3], but one drawback of this approach is that the knowledge on quantum dimension and accurate measurement implementations must be given, which are often unpractical, otherwise the results may not be reliable [4].

To overcome this problem, it turns out that the approach of device independence, a method that was first introduced in the area of quantum key distribution [5–7] and self-testing [8,9], is very helpful. In this approach, all involved quantum devices are regarded as black boxes and quantum tasks like entanglement certification are usually accomplished by checking the existence of a Bell nonlocality, i.e., a violation of some Bell inequality that is satisfied by all separable states [10]. Particularly, this approach has been utilized extensively to certify the existence of genuine multipartite entanglement [11–18]. Since nontrivial and reliable conclusions can be drawn from limited measurement data only, device independence is highly valuable experimentally. Moreover, for the situations that partial reliable information on the target quantum systems is known, measurement-device-independent [19,20] and semi-device-independent scenarios [21,22] were also proposed.

A further step from entanglement certification is the quantification of entanglement in quantum laboratories [23–25]. In order to provide reliable results, device-independent schemes for quantifying entanglement have also been proposed. For example, inspired by the Navascués-Pironio-Acín (NPA) method [26], a device-independent method to lower bound the negativity was provided in Ref. [14]. Using the concept of semiquantum nonlocal games introduced in Ref. [27], a measurement-device-independent approach to quantify negative-partial-transposition entanglement has been reported [28], and very recently, similar approaches that are able to quantify any convex entanglement measures have also been developed [29,30]. Usually, this kind of work faces two inevitable difficulties. First, nonlocality and entanglement are known as two different resources for quantum information processing [31], which profoundly makes quantifying entanglement in a device-independent way challenging, as what we need to do here is characterize unknown entanglement based on quantum nonlocality we observe. Second, the mathematical structures of quantum correlations are very complicated [32–35], for example, accurate Tsirelson bounds are often notoriously hard to find out, which makes it quite hard to study most device-independent quantum tasks in an analytical way. As a consequence, in most cases of device-independent entanglement quantifications one has to perform costly numerical calculations [26], or can only give weak results based on self-tests [36,37]. Therefore, despite these encouraging progresses, in order to gain deeper understanding of the fundamental relations between nonlocality and entanglement measures, especially those standard entanglement measures with clear operational meanings, direct *analytical* approaches for *general* cases of Bell experiments are highly demanded.

In this paper, for a general unknown bipartite quantum state, we provide an analytic method to quantify the entanglement of formation or the distillable entanglement, two of the most well-known entanglement measures, in a semi-device-independent manner, where besides the measurement statistics data, the only assumption we make is quantum dimension. The main idea behind our approach is a new property called nondegeneracy we define for Bell inequalities.

*weizhaohui@gmail.com

Basically, in a Bell setting, we say the involved Bell inequality is nondegenerate if any quantum state $|\psi\rangle$ of given dimension generates a violation of the inequality larger than a, then any quantum state orthogonal to $|\psi\rangle$ cannot achieve a violation larger than b by using the same local measurements, where $a > b$ are two parameters. By looking into the mathematical structure of nondegenerate Bell inequalities, we prove that a lot of well-known Bell inequalities are nondegenerate, including the Clauser-Horne-Shimony-Holt (CHSH) inequality [38], the I_{3322} inequality [39–41], and the Collins-Gisin-Linden-Masser-Popescu (CGLMP) inequalities [42]. By choosing nondegenerate Bell inequalities, we prove that a fundamental relation between Bell inequality violations and the entanglement measures can be built, eventually giving the desired analytic result. Since our approach is based on the observed quantum nonlocality, the number of measurements needed is usually very modest. We demonstrate the applications of our approach by applying the CGLMP inequalities on qutrit-qutrit quantum states, and specific examples show that a nontrivial lower bound for the entanglement measures can be obtained when the violation is sufficient.

II. RESULTS

A. Nondegenerate Bell inequalities

In a two-party Bell experiment, Alice and Bob, located at different places, share a physical system and perform local measurements on their own subsystems without communications. Specifically, Alice (Bob) has a set of measurement apparatus labeled by a finite set X (Y), and the set of possible measurement outcomes are labeled by a finite set A (B). When the experiment begins, they choose random apparatuses to measure the system and repeat the whole process many times. By recording the frequency of outcomes, they calculate the joint probability distribution $p(ab|xy)$, indicating the probability of obtaining outcomes $a \in A$ and $b \in B$ when choosing measurement apparatuses $x \in X$ and $y \in Y$. The collection of all $|A \times B \times X \times Y|$ joint probability distributions can be written as a vector $p := \{p(ab|xy)\}$, called a *correlation*.

The set of correlations depends heavily on the physical laws that the system that Alice and Bob share obeys. If the experiment is purely classical, all the correlations they are able to produce are local correlations, which can be replicated by a local hidden variable (LHV) model, where public randomness is shared before the experiment begins and the distributions of outputs at each party are generated depending only on the public randomness and the input received. On the other hand, if what they share beforehand is a quantum state ρ of dimension $d \times d$, then the correlation can be written as

$$p(ab|xy) = \mathrm{Tr}\big[\rho\big(M_x^a \otimes M_y^b\big)\big], \tag{1}$$

where M_x^a and M_y^b are the measurement operators of the apparatuses x and y.

A major discovery in quantum mechanics is that there exist quantum correlations that cannot be produced with LHV models, which can be explained by the concept of Bell inequalities [10]. A typical Bell inequality can be expressed as

$$I := \sum_{abxy} s_{abxy}\, p(ab|xy) \leqslant C_l, \tag{2}$$

where s_{abxy} are normally real coefficients, and C_l is the maximal value of the Bell expression I that local correlations achieve. It turns out that in some cases the maximal value of I that quantum correlations achieve, called the Tsirelson bound and denoted by C_q, can be strictly larger than C_l, revealing the profound discovery we just mentioned. From now on, when considering correlations produced by quantum states of dimension $d \times d$, we denote the Bell expression by $I(\rho, M_x^a, M_y^b)$, and its maximal value by C_q^d.

In this paper, we define and focus on a special case of Bell inequalities called *nondegenerate*. We will show that for an unknown bipartite quantum state ρ, this property makes it possible to obtain analytic estimations for the entanglement of formation, denoted $E_f(\rho)$, by utilizing the measurement statistics data only, assuming the quantum dimension is known.

Definition 1. A Bell inequality $I \leqslant C_l$ is nondegenerate if there exists two real numbers $0 \leqslant \epsilon_1 < \epsilon_2 \leqslant C_q^d$, such that for any pure state $|\psi\rangle$ acting on $\mathcal{H}^d \otimes \mathcal{H}^d$ and any measurements $\{M_x^a\}$ and $\{M_y^b\}$,

$$I\big(|\psi\rangle\langle\psi|, M_x^a, M_y^b\big) \geqslant C_q^d - \epsilon_1$$

always implies that

$$I\big(|\psi^\perp\rangle\langle\psi^\perp|, M_x^a, M_y^b\big) \leqslant C_q^d - \epsilon_2,$$

where $|\psi^\perp\rangle$ is any pure state orthogonal to $|\psi\rangle$.

Intuitively, the nondegeneracy means that if a quantum state makes a large violation of the Bell inequality, any orthogonal quantum state cannot with the measurements *unchanged*.

A few remarks are in order. First, nondegeneracy is meaningful only when the dimension is given, as any Bell inequality cannot satisfy the definition if extra subsystems can be introduced freely. Second, in some device-independent quantum tasks like self-testing [8,9,43,44], a crucial issue is whether the maximal violation is achieved by multiple pure quantum states, where the involved measurements can be different. For convenience in this case we say the Bell inequality enjoys the uniqueness property. We stress that the nondegeneracy property is different from the uniqueness property. After all, it is possible that two close but essentially different quantum pure states achieve the maximal violation simultaneously, but they are using different measurements, and still satisfy the definition of nondegeneracy. Usually it is notoriously hard to determine whether or not a given Bell inequality has the uniqueness property. However, we will show that the nondegeneracy property has a rich mathematical structure, which allows us to certify the existence of this property relatively easier, potentially resulting in wide applications of this new definition. Actually, later we will see that quite a lot of well-known Bell inequalities are nondegenerate. Third, nondegeneracy can also be defined on Bell inequalities of nonlinear forms.

B. Principal component analysis

Before proving that nondegenerate Bell inequalities exist, let us see that nondegeneracy can provide useful information on the purity of underlying quantum states.

Suppose a quantum correlation $p(ab|xy)$ is produced by measuring a bipartite quantum state ρ of dimension $d\times d$ with measurements $\{M_x^a\}$ and $\{M_y^b\}$. And suppose there exists a nondegenerate Bell inequality $I\leqslant C_l$ with parameters ϵ_1 and ϵ_2 such that the Bell expression given by $p(ab|xy)$ is larger than $C_q^d-\epsilon_1$, that is,

$$I\big(\rho, M_x^a, M_y^b\big)\geqslant C_q^d-\epsilon_1. \tag{3}$$

Let an orthogonal decomposition of ρ be $\rho=\sum_{i=1}^{d^2}a_i|\psi_i\rangle\langle\psi_i|$. Since the Bell expression is linear in the shared quantum state, there must be a $|\psi_i\rangle$ such that $I(|\psi_i\rangle\langle\psi_i|, M_x^a, M_y^b)\geqslant C_q^d-\epsilon_1$. Without loss of generality, we suppose $i=1$. Then it holds that

$$\begin{aligned}I\big(\rho, M_x^a, M_y^b\big)&=\sum_{i=1}^{d^2}a_iI\big(|\psi_i\rangle\langle\psi_i|, M_x^a, M_y^b\big)\\&\leqslant a_1I\big(|\psi_1\rangle\langle\psi_1|, M_x^a, M_y^b\big)\\&\quad+\big(1-a_1\big)\big(C_q^d-\epsilon_2\big)\\&\leqslant a_1C_q^d+\big(1-a_1\big)\big(C_q^d-\epsilon_2\big),\end{aligned}$$

where we have used the definition of nondegeneracy and the fact that $I(|\psi_1\rangle\langle\psi_1|, M_x^a, M_y^b)\leqslant C_q^d$.

Combining the above inequality with Eq. (3), we immediately have that $a_1\geqslant 1-\epsilon_1/\epsilon_2$. Therefore, if $\epsilon_1/\epsilon_2\ll 1$, the nondegeneracy guarantees that violating the Bell inequality almost maximally means that the involved quantum state ρ must be close to pure. And the purity of ρ can be lower bounded by

$$\begin{aligned}\mathrm{Tr}(\rho^2)&=\sum_{i=1}^{d^2}a_i^2\geqslant a_1^2+\frac{1}{d^2-1}\left(\sum_{i=2}^{d^2}a_i\right)^2\\&=a_1^2+\frac{1}{d^2-1}(1-a_1)^2,\end{aligned}$$

where we have utilized the Cauchy-Schwarz inequality and the fact that $\sum_{i=1}^{d^2}a_i=1$. Then note that when $a_1\geqslant 1-\epsilon_1/\epsilon_2\geqslant 1/d^2$ (it is satisfied in our later applications), $a_1^2+\frac{1}{d^2-1}(1-a_1)^2$ is an increasing function of a_1, implying that

$$\mathrm{Tr}(\rho^2)\geqslant\left(1-\frac{\epsilon_1}{\epsilon_2}\right)^2+\frac{(\epsilon_1/\epsilon_2)^2}{d^2-1}.$$

C. The certification of nondegeneracy

We now show that the concept of nondegeneracy is well defined, and a lot of well-known Bell inequalities are nondegenerate.

Consider a Bell scenario over finite setting sets $\mathcal{X}$, $\mathcal{Y}$ and finite outcome sets $\mathcal{A}$, $\mathcal{B}$. The corresponding Bell expression is $I(\rho_{AB}, M_x^a, M_y^b)=\sum_{abxy}s_{abxy}p(ab|xy)$, where $s_{abxy}\in\mathbb{R}$, $a\in\mathcal{A}$, $b\in\mathcal{B}$, $x\in\mathcal{X}$, $y\in\mathcal{Y}$, and $\{M_x^a\}$ and $\{M_y^b\}$ are positive operator-valued measures (POVMs) on d-dimensional quantum subsystems A and B, respectively. In particular, for a pure state $|\psi\rangle_{AB}$, if we let $H(M_x^a, M_y^b)=\sum_{abxy}s_{abxy}M_x^a\otimes M_y^b$, then we have

$$I\big(|\psi\rangle_{AB}\langle\psi|_{AB}, M_x^a, M_y^b\big)=\langle\psi|_{AB}H\big(M_x^a, M_y^b\big)|\psi\rangle_{AB}.$$

Since $H(M_x^a, M_y^b)$ is Hermitian, it has d^2 real eigenvalues, and we now denote them by $\lambda_1(H(M_x^a, M_y^b))\geqslant\cdots\geqslant\lambda_{d^2}(H(M_x^a, M_y^b))$. Furthermore, we define

$$C(I, d, t)=\max_{\{M_x^a, M_y^b\}}\sum_{i=1}^{t}\lambda_i\big(H\big(M_x^a, M_y^b\big)\big).$$

Then it is not hard to see that $C_q^d=C(I, d, 1)$.

We now show that there is a simple relation between $C(I, d, k)$ and nondegeneracy of I, as shown in the following lemma.

Lemma 1. For any bipartite quantum system of dimension $d\times d$, a Bell expression I is nondegenerate if and only if $C(I, d, 2)<2C(I, d, 1)$.

Proof. Suppose I is nondegenerate with $0\leqslant\epsilon_1<\epsilon_2$. Suppose POVMs $\{M_x^a\}$ and $\{M_y^b\}$ maximize $C(I, d, 2)$. And let $|\psi_1\rangle, |\psi_2\rangle$ be the eigenstates corresponding to $\lambda_1(H(M_x^a, M_y^b))$ and $\lambda_2(H(M_x^a, M_y^b))$, respectively. If $C(I, d, 2)=2C(I, d, 1)$, then, by

$$\begin{aligned}C(I, d, 2)&=\lambda_1\big(H\big(M_x^a, M_y^b\big)\big)+\lambda_2\big(H\big(M_x^a, M_y^b\big)\big)\\&=I\big(|\psi_1\rangle\langle\psi_1|, M_x^a, M_y^b\big)+I\big(|\psi_2\rangle\langle\psi_2|, M_x^a, M_y^b\big),\end{aligned}$$

we have

$$I\big(|\psi_1\rangle\langle\psi_1|, M_x^a, M_y^b\big)=I\big(|\psi_2\rangle\langle\psi_2|, M_x^a, M_y^b\big)=C_q^d,$$

which contradicts the definition of nondegeneracy.

Conversely, suppose $C(I, d, 2)<2C(I, d, 1)$. For any pair of orthogonal pure states $|\psi\rangle, |\phi\rangle$ and any POVMs $\{M_x^a\}$ and $\{M_y^b\}$, we have

$$I\big(|\psi\rangle\langle\psi|, M_x^a, M_y^b\big)+I\big(|\phi\rangle\langle\phi|, M_x^a, M_y^b\big)\leqslant C(I, d, 2).$$

Choose a proper ϵ_1 such that $0\leqslant\epsilon_1<C_q^d-\frac{1}{2}C(I, d, 2)$. Then, if $I(|\psi\rangle\langle\psi|, M_x^a, M_y^b)\geqslant C_q^d-\epsilon_1$, it can be verified that

$$\begin{aligned}I\big(|\phi\rangle\langle\phi|, M_x^a, M_y^b\big)&\leqslant C(I, d, 2)-I\big(|\psi\rangle\langle\psi|, M_x^a, M_y^b\big)\\&\leqslant C(I, d, 2)-C_q^d+\epsilon_1\\&=C_q^d-\big[2C_q^d-C(I, d, 2)-\epsilon_1\big].\end{aligned}$$

Therefore, if we let $\epsilon_2=2C_q^d-C(I, d, 2)-\epsilon_1$, then we have that $\epsilon_1<\epsilon_2$ and $I(|\phi\rangle\langle\phi|, M_x^a, M_y^b)\leqslant C_q^d-\epsilon_2$, which implies that I is nondegenerate with parameters ϵ_1 and ϵ_2. ■

We now introduce an approach to determine whether the above condition is satisfied or not by looking at $C(I, d-1, 1)$. For this, we need the following fact.

Lemma 2. Let $|\psi\rangle, |\phi\rangle$ be two bipartite states in a $d\times d$ dimensional system. If both of $|\psi\rangle$ and $|\phi\rangle$ have Schmidt number d, then there is $\alpha, \beta\in\mathbb{C}$ with $\alpha\beta\neq 0$ such that $\alpha|\psi\rangle+\beta|\phi\rangle$ have Schmidt number at most $d-1$.

Proof. For any state $|\varphi\rangle=\sum_{ij}a_{ij}|i\rangle\otimes|j\rangle$, we transform it into a $d\times d$ matrix with (i, j)th entry equal to a_{ij}. We transform $|\psi\rangle$ and $|\phi\rangle$ into A and B in this fashion, respectively. Then both A and B have full rank, that is, rank d.

The linear combination of A and B reads $\alpha A+\beta B=A(\alpha I+\beta A^{-1}B)$. Let $C=A^{-1}B$; then C has full rank as well. By assuming that $\beta\neq 0$, we can write $\alpha A+\beta B=\beta A(\gamma I+C)$, where $\alpha/\beta=\gamma\in\mathbb{C}$ is arbitrary. Since C is a complex matrix, it has a nonzero eigenvalue λ; that is, $C-\lambda I$ is of rank at most $d-1$. By picking $\gamma = -\lambda$, the resulting linear combination $\alpha A + \beta B$ has rank at most $d-1$, so the Schmidt number of $\alpha|\psi\rangle + \beta|\phi\rangle$ is at most $d-1$ as well. ■

Then we have the following characterization of nondegeneracy for Bell inequalities.

Theorem 1. Let I be a Bell expression and $d > 1$. If $C(I, d, 1) > C(I, d-1, 1)$, then I is nondegenerate.

Proof. We now prove that if $C(I, d, 1) > C(I, d-1, 1)$, then $C(I, d, 2) \leqslant C(I, d, 1) + C(I, d-1, 1)$. According to Lemma 1, this implies that I is nondegenerate. Suppose $C(I, d, 2) > C(I, d, 1) + C(I, d-1, 1)$. Let $\{M_x^a\}$ and $\{M_y^b\}$ be the POVMs that achieve $C(I, d, 2)$. Then there exist two corresponding eigenstates $|\psi\rangle, |\phi\rangle$ that satisfy

$$
\begin{aligned}
&I\big(|\psi\rangle\langle\psi|, M_x^a, M_y^b\big) + I\big(|\phi\rangle\langle\phi|, M_x^a, M_y^b\big) \\
&\quad = C(I, d, 2) > C(I, d, 1) + C(I, d-1, 1).
\end{aligned}
$$

By the definition of $C(I, d, 1)$, this means that

$$
\begin{aligned}
I\big(|\psi\rangle\langle\psi|, M_x^a, M_y^b\big) &> C(I, d-1, 1), \\
I\big(|\phi\rangle\langle\phi|, M_x^a, M_y^b\big) &> C(I, d-1, 1),
\end{aligned}
$$

and thus both $|\psi\rangle$ and $|\phi\rangle$ have Schmidt number at least d. For $\alpha, \beta \in \mathbb{C}$ with $|\alpha|^2 + |\beta|^2 = 1$, we have

$$
\begin{aligned}
&I\big((\alpha|\psi\rangle + \beta|\phi\rangle)(\bar{\alpha}\langle\psi| + \bar{\beta}\langle\phi|), M_x^a, M_y^b\big) \\
&\quad = |\alpha|^2 I\big(|\psi\rangle\langle\psi|, M_x^a, M_y^b\big) + |\beta|^2 I\big(|\phi\rangle\langle\phi|, M_x^a, M_y^b\big) \\
&\quad > C(I, d-1, 1).
\end{aligned}
$$

However, by Lemma 2, there is $\alpha, \beta \in \mathbb{C}$ with $\alpha\beta \neq 0$ such that $|\varphi\rangle = \alpha|\psi\rangle + \beta|\phi\rangle$ has Schmidt number at most $d-1$. By normalizing the linear combination, we can fit $|\varphi\rangle$ into a $(d-1) \times (d-1)$ dimensional system. Let M'^a_x, M'^b_y be the compression of M_x^a and M_y^b into the reduced system. Then we have $I(|\varphi\rangle\langle\varphi|, M'^a_x, M'^b_y) > C(I, d-1, 1)$, which contradicts the definition of $C(I, d-1, 1)$. Therefore, $C(I, d, 2) \leqslant C(I, d, 1) + C(I, d-1, 1)$. ■

This theorem implies the following two interesting consequences. First, any Bell inequality that can be violated by a pair of qubits is nondegenerate. Indeed, when $d = 1$, the system is entirely classical, and there will be no violation, hence $C(I, 1, 1) < C(I, 2, 1)$. In particular, the CHSH inequality is nondegenerate, as it is well known that it can be violated by a pair of qubits [38]. Actually, quite a lot of device-independent characterization of qubit-qubit states based on the CHSH inequalities have been reported [45–47].

Second, any Bell expression with the maximal quantum violation C_q^d strictly monotonic with respect to d is nondegenerate. Two well-known Bell inequalities with this property are the I_{3322} inequality and the CGLMP inequality [48,49].

D. A demonstration: Quantifying qutrit-qutrit entanglement with the CGLMP inequality

We now show that after the involved Bell inequality is certified to be nondegenerate, we can quantify analytically the entanglement of an unknown bipartite quantum state in a semi-device-independent manner. For simplicity, we will focus on the CGLMP inequality for a qutrit-qutrit quantum state ρ. We stress that our approach can be applied generally on quantum states of any given dimension, and beforehand assumption on quantum dimension is possible in quantum experiments (see Ref. [50] for an example).

The form of the CGLMP inequality we choose is from Ref. [48], which is

$$
\mathrm{P}(A_2 \geqslant B_2) + \mathrm{P}(B_2 \geqslant A_1) + \mathrm{P}(A_1 \geqslant B_1) + \mathrm{P}(B_1 > A_2) \leqslant 3.
$$

In Ref. [48], it was found that when $d = 3$, $C_q^3 = C(I, 3, 1) = 3.3050$. Through numerical simulations, we find that for qutrit-qutrit quantum states, $C(I, 3, 2) = 6.2071$ (see Appendix A). Note that $C(I, 3, 2) < 2C(I, 3, 1)$, then Lemma 1 indicates that the CGLMP inequality is nondegenerate for $d = 3$. Furthermore, the proof of Lemma 1 provides a systematic way to choose the parameters ϵ_1 and ϵ_2. Therefore, if a target quantum state ρ satisfies that $I(\rho, M_x^a, M_y^b) \geqslant C_q^3 - \epsilon_1$, we can use the principal component analysis introduced before to obtain a lower bound for the purity of ρ, that is,

$$
\mathrm{Tr}(\rho^2) \geqslant \left(1 - \frac{\epsilon_1}{\epsilon_2}\right)^2 + \frac{(\epsilon_1/\epsilon_2)^2}{8} \equiv \gamma_\rho.
$$

Then according to Ref. [51], the von Neumann entropy of ρ, denoted by $S(\rho)$, can be upper bounded as

$$
S(\rho) \leqslant -c_i \sum_{i=1}^{9} \log(c_i),
$$

where $c_1 = \frac{1}{9} + \frac{2}{3}\sqrt{2(\gamma_\rho - \frac{1}{9})}$, and $c_2 = \cdots = c_9 = (1 - c_1)/8$.

On the other hand, according to Refs. [52,53], the purity of $\rho_A = \mathrm{Tr}_B(\rho)$ [or $\rho_B = \mathrm{Tr}_A(\rho)$] can also be upper bounded. Indeed, if we define

$$
f_1(p) = \min_{y_1, y_2} \sum_{b_1, b_2} \min_x \left(\sum_a \sqrt{p(ab_1|xy_1)p(ab_2|xy_2)} \right)^2 \tag{4}
$$

and

$$
f_2(p) = \min_{x_1, x_2} \sum_{a_1, a_2} \min_y \left(\sum_b \sqrt{p(a_1b|x_1y)p(a_2b|x_2y)} \right)^2, \tag{5}
$$

then it holds that [52,53]

$$
\mathrm{Tr}\big(\rho_A^2\big) \leqslant \min\{f_1(p), f_2(p)\} \equiv \gamma_A. \tag{6}
$$

Again, when $\gamma_A < 1/2$, according to Ref. [51] the von Neumann entropy of ρ_A can be lower bounded as

$$
S(\rho_A) \geqslant -f_i \sum_{i=1}^{3} \log(f_i),
$$

where $f_1 = f_2 = \frac{1-\alpha}{2}$, $f_3 = \alpha$, and $\alpha = \frac{1}{3} - \sqrt{\frac{2}{3}(\gamma_A - \frac{1}{3})}$.

We next consider the coherent information of ρ defined as [54,55]

$$
I_C(\rho) = S(\rho_A) - S(\rho).
$$

Clearly, our discussions above provide an analytical lower bound for $I_C(\rho)$.

Importantly, it turns out that, for any bipartite quantum state ρ, we have that [56]

$$
E_f(\rho) \geqslant E_D(\rho) \geqslant I_C(\rho), \tag{7}
$$

where $E_D(\rho)$ is the distillable entanglement of ρ. Therefore, our approach actually lower bounds the entanglement of formation or even the distillable entanglement for ρ. Note that in addition to the measurement statistics $p(ab|xy)$, we do not need any assumption on the internal working of the quantum system or the precision of quantum operations except the dimension d, which means that our quantification for $E_f(\rho)$ or $E_D(\rho)$ is of a semi-device-independent nature.

We test our approach on numerically generated qutrit-qutrit correlations, and the results are illustrated in the figure below (see Appendix A for more details). It can be seen that when the gap between the violation and C_q^3 is smaller than 0.065, our method gives a positive lower bound for the distillable entanglement.

Lastly, we would like to point out that $E_f(\rho)$ can also be lower bounded in the following alternative way. According to Ref. [53], $E_f(|\psi_1\rangle\langle\psi_1|)$ can be lower bounded as the purity of $\mathrm{Tr}_B(|\psi_1\rangle\langle\psi_1|)$ can be upper bounded, where $|\psi_1\rangle$ is the principal component of ρ we have discussed above. Then by the continuous property of the entanglement of formation proved by Refs. [57,58], we can bound the gap between $E_f(\rho)$ and $E_f(|\psi_1\rangle\langle\psi_1|)$. Combining these two results together, we can obtain a lower bound for $E_f(\rho)$. However, specific examples of quantum correlations show that our first approach is much better than the second one (see Appendix B).

E. Multipartite case

In principle the approach above can be generalized to the multipartite case [59], as the concept of nondegeneracy can also be defined naturally on multipartite Bell inequalities. But a major issue raised in the multipartite case is that the structure of multipartite entanglement is much more complicated. For example, in the multipartite case we cannot quantify entanglement based on Schmidt decompositions as in Ref. [53]; thus this part has to be redeveloped carefully. Similarly, bounding coherent information will be also much more challenging in the multipartite case.

III. DISCUSSION

We define a property called nondegeneracy for Bell inequalities, and based on this concept, we propose an approach to quantify the entanglement of formation or the distillable entanglement for the shared quantum state underlying a Bell experiment in a semi-device-independent manner, which is analytic and does not rely on complicated numerical optimizations, unlike most results on device-independent quantum tasks. We also provide a mathematical characterization for nondegenerate Bell inequalities, and prove that quite a lot of well-known Bell inequalities are nondegenerate. We apply our approach on qutrit-qutrit quantum states by choosing the CGLMP inequality, and demonstrate that a positive lower bound for the two entanglement measures can be obtained if the violation is sufficient. Recently, by a different approach, the property of nondegeneracy has also been applied on multipartite quantum systems to characterize unknown entanglement [60]. Therefore, we believe that this concept is of independent interest, and provides insight for studying Bell inequalities.

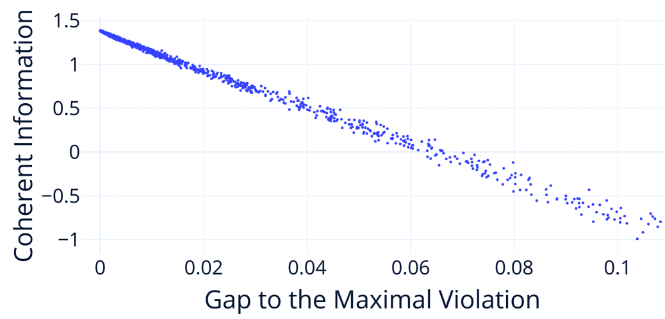

FIG. 1. Our lower bounds for the coherent information (or the distillable entanglement) based on the violations of the CGLMP inequality, where quantum correlations are generated by measuring qutrit-qutrit states. Note that the gap between the classical bound and the Tsirelson bound is 0.3050 [48].

ACKNOWLEDGMENTS

Z.W. thanks Valerio Scarani for helpful discussions. Z.W. and L.L. are supported by the National Key R&D Program of China, Grant No. 2018YFA0306703, the National Natural Science Foundation of China, Grant No. 20181311604, and the startup funds of Tsinghua University, Grant No. 53330100118. This work has been supported in part by the Zhongguancun Haihua Institute for Frontier Information Technology.

APPENDIX A: SPECIFICATIONS OF NUMERICAL SIMULATIONS USED

1. The estimation of $C(I, 3, 2)$ for the CGLMP expression

The computation for $C(I, 3, 2)$ is a maximization problem over the measurements. Note that each party has two measurement settings, and each setting is composed by three measurement operators, so all the measurements can be parametrized by $2 \times 2 \times 2 \times 3 \times 3 \times 3 = 216$ real parameters (they are not independent). We used the Nelder-Mead method [61] and the L-BFGS-B method [62,63] implemented by SCIPY [64] to solve the optimization problem. Two methods consistently yield the result $C(I, 3, 2) = 6.2071$ over many rounds.

2. Sample generation

Denote the state achieving the maximal violation (as in Ref. [48]) as $|\psi\rangle$. Every sample point in Fig. 1 is generated in the following way:

(i) We perturb the amplitudes of the state $|\psi\rangle$; the resulting state is a pure state $|\psi'\rangle$ close to $|\psi\rangle$.

(ii) Then, we measure $|\psi'\rangle$ with the optimal measurement given by Ref. [48] to generate a physical correlation.

(iii) Finally, the Bell value and the coherent information bound are computed from the physical correlation, giving a sample point in Fig. 1.

By varying the strengths of perturbations, we can roughly control the Bell values of the resulting correlations, thereby allowing us to illustrate the performance of our approach.

APPENDIX B: THE CONTINUITY-BASED APPROACH

In Ref. [58], Winter proved the continuity of the entanglement of formation, E_f, in the following form:

$$E_f(\sigma_{AB}) - E_f(\rho_{AB}) \leqslant \delta \log_2 d + (1+\delta) H\left(\frac{\delta}{1+\delta}\right),$$

where $\delta = \sqrt{D(\rho_{AB}, \sigma_{AB})(2 - D(\rho_{AB}, \sigma_{AB}))}$, $D(\rho_{AB}, \sigma_{AB})$ is the trace distance, and $H(x) = -x \log_2 x - (1-x)\log_2(1-x)$ is the Shannon entropy.

According to Ref. [53], it holds that

$$E_f(|\psi_1\rangle\langle\psi_1|) \geqslant -\log_2(\min\{f_1(p), f_2(p)\}) + 2\log_2 a_1,$$

where $f_1(p)$ and $f_2(p)$ are given as Eq. (4) and Eq. (5), respectively.

In addition, the definition of a_1 and $|\psi_1\rangle$ gives $D(\rho, |\psi_1\rangle\langle\psi_1|) = 1 - a_1$; hence we have

$$E_f(\rho) \geqslant -\log_2(\min\{f_1(p), f_2(p)\}) + 2\log_2 a_1 - \delta \log_2 d - (1+\delta) H\left(\frac{\delta}{1+\delta}\right), \quad \text{(B1)}$$

where $\delta = \sqrt{1 - a_1^2}$.

All sample correlations in Fig. 1 can also be utilized by Eq. (B1); thus we can readily compare the performances of these two approaches: while the two approaches give the same estimate for E_f as the Bell value approaches the maximal violation, Eq. (B1) gives a nontrivial estimate only when the gap between the violation and C_q^3 is smaller than 2×10^{-3}, which is a far more stringent condition compared to the 6.5×10^{-2} gap of the approach in the main text.

[1] I. L. Chuang and M. A. Nielsen, Prescription for experimental determination of the dynamics of a quantum black box, J. Mod. Opt. **44**, 2455 (1997).

[2] J. F. Poyatos, J. I. Cirac, and P. Zoller, Complete Characterization of a Quantum Process: The Two-Bit Quantum Gate, Phys. Rev. Lett. **78**, 390 (1997).

[3] O. Gühne and G. Toth, Entanglement detection, Phys. Rep. **474**, 1 (2009).

[4] D. Rosset, R. Ferretti-Schöbitz, J.-D. Bancal, N. Gisin, and Y. C. Liang, Imperfect measurement settings: Implications for quantum state tomography and entanglement witnesses, Phys. Rev. A **86**, 062325 (2012).

[5] A. Ekert, Quantum Cryptography Based on Bell's Theorem, Phys. Rev. Lett. **67**, 661 (1991).

[6] J. Barrett, L. Hardy, and A. Kent, No Signaling and Quantum Key Distribution, Phys. Rev. Lett. **95**, 010503 (2005).

[7] A. Acín, N. Gisin, and L. Masanes, From Bell's Theorem to Secure Quantum Key Distribution, Phys. Rev. Lett. **97**, 120405 (2006).

[8] S. Popescu and D. Rohrlich, Which states violate Bell's inequality maximally? Phys. Lett. A **169**, 411 (1992).

[9] D. Mayers and A. Yao, Quantum cryptography with imperfect apparatus, In *Proceedings of 39th Annual Symposium on Foundations of Computer Science* (IEEE, Piscataway, NJ, 1998), pp. 503–509.

[10] J. S. Bell, On the Einstein-Podolsky-Rosen paradox, Physics **1**, 195 (1964).

[11] D. Collins, N. Gisin, S. Popescu, D. Roberts, and V. Scarani, Bell-Type Inequalities to Detect True *n*-Body Nonseparability, Phys. Rev. Lett. **88**, 170405 (2002).

[12] J. D. Bancal, N. Gisin, Y. C. Liang, and S. Pironio, Device-Independent Witnesses of Genuine Multipartite Entanglement, Phys. Rev. Lett. **106**, 250404 (2011).

[13] K. F. Pál and T. Vértesi, Multisetting Bell-type inequalities for detecting genuine multipartite entanglement, Phys. Rev. A **83**, 062123 (2011).

[14] T. Moroder, J. D. Bancal, Y. C. Liang, M. Hofmann, and O. Gühne, Device-Independent Entanglement Quantification and Related Applications, Phys. Rev. Lett. **111**, 030501 (2013).

[15] G. Murta, R. Ramanathan, N. Móller, and M. T. Cunha, Quantum bounds on multiplayer linear games and device-independent witness of genuine tripartite entanglement, Phys. Rev. A **93**, 022305 (2016).

[16] F. Baccari, D. Cavalcanti, P. Wittek, and A. Acín, Efficient Device-Independent Entanglement Detection for Multipartite Systems, Phys. Rev. X **7**, 021042 (2017).

[17] A. Tavakoli, A. A. Abbott, M. O. Renou, N. Gisin, and N. Brunner, Semi-device-independent characterization of multipartite entanglement of states and measurements, Phys. Rev. A **98**, 052333 (2018).

[18] M. Zwerger, W. Dür, J. D. Bancal, and P. Sekatski, Device-Independent Detection of Genuine Multipartite Entanglement for All Pure States, Phys. Rev. Lett. **122**, 060502 (2019).

[19] H. K. Lo, M. Curty, and B. Qi, Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **108**, 130503 (2012).

[20] S. L. Braunstein and S. Pirandola, Side-Channel-Free Quantum Key Distribution, Phys. Rev. Lett. **108**, 130502 (2012).

[21] T. Moroder and O. Gittsovich, Calibration-robust entanglement detection beyond Bell inequalities, Phys. Rev. A **85**, 032301 (2012).

[22] Y. C. Liang, T. Vértesi, and N. Brunner, Semi-device-independent bounds on entanglement, Phys. Rev. A **83**, 022108 (2011).

[23] R. Islam, R. Ma, P. M. Preiss, M. E. Tai, A. Lukin, M. Rispoli, and M. Greiner, Measuring entanglement entropy in a quantum many-body system, Nature **528**, 77 (2015).

[24] T. Brydges, A. Elben, P. Jurcevic, B. Vermersch, C. Maier, B. P. Lanyon, P. Zoller, R. Blatt, and C. F. Roos, Probing Rényi entanglement entropy via randomized measurements, Science **364**, 260 (2019).

[25] N. M. Linke, S. Johri, C. Figgatt, K. A. Landsman, A. Y. Matsuura, and C. Monroe, Measuring the Rényi entropy of a two-site Fermi-Hubbard model on a trapped ion quantum computer, Phys. Rev. A **98**, 052334 (2018).

[26] M. Navascués, S. Pironio, and A. Acín, Bounding the Set of Quantum Correlations, Phys. Rev. Lett. **98**, 010401 (2007).

[27] F. Buscemi, All Entangled Quantum States are Nonlocal, Phys. Rev. Lett. **108**, 200401 (2012).

[28] F. Shahandeh, M. J. W. Hall, and T. C. Ralph, Measurement-Device-Independent Approach to Entanglement Measures, Phys. Rev. Lett. **118**, 150505 (2017).
[29] D. Rosset, A. Martin, E. Verbanis, C. C. W. Lim, and R. Thew, Practical measurement-device-independent entanglement quantification, Phys. Rev. A **98**, 052332 (2018).
[30] Y. Guo *et al.*, Measurement-device-independent quantification of irreducible high-dimensional entanglement, npj Quantum Inf. **6**, 52 (2020).
[31] A. A. Methot and V. Scarani, An anomaly of non-locality, Quantum Inf. Comput. **7**, 157 (2007).
[32] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Bell nonlocality, Rev. Mod. Phys. **86**, 419 (2014).
[33] K. T. Goh, J. Kaniewski, E. Wolfe, T. Vértesi, X. Wu, Y. Cai, Y. C. Liang, and V. Scarani, Geometry of the set of quantum correlations, Phys. Rev. A **97**, 022104 (2018).
[34] J. M. Donohue and E. Wolfe, Identifying nonconvexity in the sets of limited-dimension quantum correlations, Phys. Rev. A **92**, 062120 (2015).
[35] W. Slofstra, The set of quantum correlations is not closed, *Forum of Mathematics, Pi* (Cambridge University Press, 2019), Vol. 7.
[36] R. Arnon-Friedman and J.-D. Bancal, Device-independent certification of one-shot distillable entanglement, New J. Phys. **21**, 033010 (2019).
[37] R. Arnon-Friedman and H. Yuen, Noise-tolerant testing of high entanglement of formation, in *45th International Colloquium on Automata, Languages, and Programming (ICALP 2018)*, edited by I. Chatzigiannakis, C. Kaklamanis, D. Marx, and D. Sannella, Leibniz International Proceedings in Informatics (Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, Dagstuhl, Germany, 2018), Vol. 107, pp. 11:1–11:12.
[38] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Proposed Experiment to Test Local Hidden Variable Theories, Phys. Rev. Lett. **24**, 549 (1970).
[39] M. Froissart, Constructive generalization of Bell's inequalities, Nuov. Cim. B **64**, 241 (1981).
[40] C. Śliwa, Symmetries of the Bell correlation inequalities, Phys. Lett. A **317**, 165 (2003).
[41] D. Collins and N. Gisin, A relevant two qubit Bell inequality inequivalent to the CHSH inequality, J. Phys. A: Math. Gen. **37**, 1775 (2004).
[42] D. Collins, N. Gisin, N. Linden, S. Massar, and S. Popescu, Bell Inequalities for Arbitrarily High-Dimensional Systems, Phys. Rev. Lett. **88**, 040404 (2002).
[43] S. L. Braunstein, A. Mann, and M. Revzen, Maximal Violation of Bell Inequalities for Mixed States, Phys. Rev. Lett. **68**, 3259 (1992).
[44] A. Coladangelo, K. T. Goh, and V. Scarani, All pure bipartite entangled states can be self-tested, Nat. Commun. **8**, 15485 (2017).
[45] V. Scarani and N. Gisin, Spectral decomposition of Bell's operators for qubits, J. Phys. A: Math. Gen. **34**, 6043 (2001).
[46] C. E. Bardyn, T. C. H. Liew, S. Massar, M. McKague, and V. Scarani, Device-independent state estimation based on Bell's inequalities, Phys. Rev. A **80**, 062327 (2009).
[47] J. Kaniewski, Analytic and Nearly Optimal Self-Testing Bounds for the Clauser-Horne-Shimony-Holt and Mermin Inequalities, Phys. Rev. Lett. **117**, 070402 (2016).
[48] S. Zohren and R. D. Gill, Maximal Violation of the Collins-Gisin-Linden-Massar-Popescu Inequality for Infinite Dimensional States, Phys. Rev. Lett. **100**, 120406 (2008).
[49] K. F. Pál and T. Vértesi, Maximal violation of a bipartite three-setting, two-outcome Bell inequality using infinite-dimensional quantum systems, Phys. Rev. A **82**, 022116 (2010).
[50] A. Bennet, T. Vértesi, D. J. Saunders, N. Brunner, and G. J. Pryde, Experimental Semi-Device-Independent Certification of Entangled Measurements, Phys. Rev. Lett. **113**, 080405 (2014).
[51] G. Smith, J. A. Smolin, X. Yuan, Q. Zhao, D. Girolami, and X. Ma, Quantifying coherence and entanglement via simple measurements, arXiv:1707.09928.
[52] J. Sikora, A. Varvitsiotis, and Z. Wei, Minimum Dimension of a Hilbert Space Needed to Generate a Quantum Correlation, Phys. Rev. Lett. **117**, 060401 (2016).
[53] Z. Wei and J. Sikora, Device-independent characterizations of a shared quantum state independent of any Bell inequalities, Phys. Rev. A **95**, 032103 (2017).
[54] B. Schumacher and M. A. Nielsen, Quantum data processing and error correction, Phys. Rev. A **54**, 2629 (1996).
[55] S. Lloyd, Capacity of the noisy quantum channel, Phys. Rev. A **55**, 1613 (1997).
[56] M. F. Cornelio, M. C. de Oliveira, and F. F. Fanchini, Entanglement Irreversibility from Quantum Discord and Quantum Deficit, Phys. Rev. Lett. **107**, 020502 (2011).
[57] M. A. Nielsen, Continuity bounds for entanglement, Phys. Rev. A **61**, 064301 (2000).
[58] A. Winter, Tight uniform continuity bounds for quantum entropies: Conditional entropy, relative entropy distance and energy constraints, Commun. Math. Phys. **347**, 291 (2016).
[59] Z. Wei and J. Sikora, Device-independent dimension test in a multiparty Bell experiment, New J. Phys. **21**, 043021 (2019).
[60] L. Lin and Z. Wei, Quantifying multipartite quantum entanglement in a semi-device-independent manner, arXiv:2008.12064.
[61] J. A. Nelder and R. Mead, A simplex method for function minimization, Comput. J. **7**, 308 (1965).
[62] R. H. Byrd, P. Lu, J. Nocedal, and C. Zhu, A limited memory algorithm for bound constrained optimization, SIAM J. Sci. Comput. **16**, 1190 (1995).
[63] C. Zhu, R. H. Byrd, P. Lu, and J. Nocedal, Algorithm 778: L-BFGS-B: Fortran subroutines for large-scale bound-constrained optimization, ACM Trans. Math. Software **23**, 550 (1997).
[64] P. Virtanen *et al.*, SciPy 1.0: Fundamental algorithms for scientific computing in Python, Nat. Methods **17**, 261 (2020).