Measurement-Device-Independent Approach to Entanglement Measures

Farid Shahandeh,[1,*] Michael J. W. Hall,[2] and Timothy C. Ralph[1]
[1]Centre for Quantum Computation and Communication Technology, School of Mathematics and Physics, University of Queensland, Brisbane, Queensland 4072, Australia
[2]Centre for Quantum Computation and Communication Technology, Centre for Quantum Dynamics, Griffith University, Brisbane, Queensland 4111, Australia
(Received 4 September 2016; published 13 April 2017)

Within the context of semiquantum nonlocal games, the trust can be removed from the measurement devices in an entanglement-detection procedure. Here, we show that a similar approach can be taken to quantify the amount of entanglement. To be specific, first, we show that in this context, a small subset of semiquantum nonlocal games is necessary and sufficient for entanglement detection in the local operations and classical communication paradigm. Second, we prove that the maximum payoff for these games is a universal measure of entanglement which is convex and continuous. Third, we show that for the quantification of negative-partial-transpose entanglement, this subset can be further reduced down to a single arbitrary element. Importantly, our measure is measurement device independent by construction and operationally accessible. Finally, our approach straightforwardly extends to quantify the entanglement within any partitioning of multipartite quantum states.

DOI: 10.1103/PhysRevLett.118.150505

Introduction.—Entanglement is a valuable resource for practical as well as fundamental applications of quantum theory, ranging from quantum computation and communication to metrology [1–3]. There are two major challenges in understanding entanglement that stimulates this research. First, it is extremely difficult to specify all the nonentangled bipartite or multipartite quantum states. In fact, the problem is known to be NP-hard [4,5]. Second, not surprisingly, the characterization of entangled states, i.e., the quantification of entanglement within quantum states, is an equally difficult task. The answer to the second challenge is practically very important because it tells us how well our protocols will perform using a given state [6–9].

Focusing on the second challenge above, a first level of hardness is that the quantification of entanglement using almost any entanglement measure, e.g., entanglement of formation [10], negativity [11,12], or random robustness [13], requires estimating a large number of density matrix elements, a task which is difficult to perform on bipartite and multipartite quantum states. While this difficulty can be partially circumvented by making use of entanglement witnesses (EWs) when lower bounds on the entanglement are desired [14–19], errors and misalignments of the measurement devices can still lead to incorrect estimations of the quantities and thus, erroneous conclusions. A measurement-device-independent approach is therefore desirable.

Recent work by Buscemi [20] has introduced a new way to think about entanglement detection [21–24]. The idea is to map the problem onto a modified class of nonlocal games, called semiquantum nonlocal games (SQNLGs). In any such game, two players (Alice and Bob) share a possibly entangled state. A referee (Charlie) starts by asking them quantum questions by sending quantum states and receiving classical answers—the outcomes of some local measurements (see Fig 1). He then evaluates a *reward* function from the responses and pays the players accordingly. Confined to not communicate during the game, known as the local operations and shared randomness (LOSR) paradigm, all separable states deliver an equal *payoff* (maximum average reward) in any specific SQNLG. Importantly, for every entangled quantum state, one can always find a SQNLG which can deliver a larger payoff than any separable state. This mapping allows one to merely rely on the coincidence statistics of measurement outcomes, without any assumptions that specific quantum operators are measured, to violate an entanglement witnessing inequality [21], a property called *measurement device independence* that was once believed to be true only in Bell nonlocality tests.

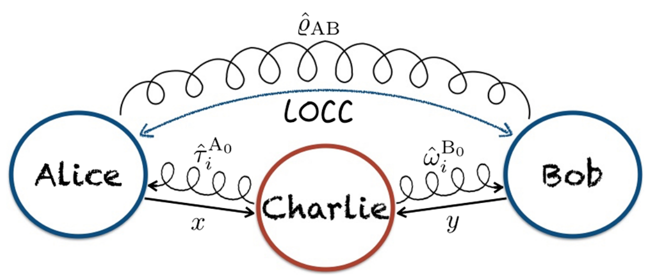

FIG. 1. The scheme of a semiquantum nonlocal game. Charlie asks the players quantum questions while the players return classical answers. The shared state between the players helps them to obtain a maximum payoff in the game. Here, we allow LOCC operations to be applied to the shared state and quantum questions and introduce a device-independent measure of entanglement.

Consequently, researchers interpreted Buscemi's results as a clever way to remove the trust from measurement devices in an entanglement witnessing procedure since any linear EW can be recast as a SQNLG [21,25].

In this Letter, inspired by Buscemi's approach, we consider SQNLGs in the paradigm of local operations and classical communication (LOCC). We show that a small subset of games, which we call extremal semiquantum witnessing games (ESQWGs), are both necessary and sufficient for the full characterization of entangled states. We then focus on the entanglement of negative-partial-transpose (NPT) states as the necessary ingredient for distillability [26]. We present a practical measurement-device-independent (MDI) NPT-entanglement measure by proving that NPT entanglement can be quantified by a referee in *a single arbitrary* ESQWG. The main result of the present Letter is thus to introduce a MDI measure of entanglement which is convex and operationally accessible. Furthermore, we extend our measure to quantify the entanglement in all possible partitionings of multipartite quantum states.

From SQNLGs to SQWGs.—Let us start by describing SQNLGs more rigorously. A SQNLG is a collaborative game, denoted here by $\mathsf{G}_{\rm sq}$, in which Alice and Bob share a quantum state $\hat{\varrho}_{AB}$. Charlie prepares two sets of quantum states $\{\hat{\tau}_i^{A_0}\}$ and $\{\hat{\omega}_i^{B_0}\}$ as (quantum) questions with probability $\{p_i\}$ and sends them to Alice and Bob, respectively. Here, A (B) and A_0 (B_0) label Alice's (Bob's) input Hilbert spaces for shared state and quantum questions, respectively. The joint Hilbert space of Alice thus can be labeled by $\tilde{A} \equiv AA_0$ and similarly for Bob, $\tilde{B} \equiv B_0 B$. Alice responds to each question classically from the set of labels $\{x\}$ and similarly, Bob from the set $\{y\}$. Before the game starts, given the LOSR paradigm, they can agree on a best strategy to win the game; however, during the game; they are no longer allowed to communicate. For each question i, Charlie evaluates a reward corresponding to the answers x and y according to the function $\wp(x,y|i)$. The average reward of the game is then given by

$$\bar{\wp}(\hat{\varrho}_{AB};\hat{P}^{\tilde{A}};\hat{Q}^{\tilde{B}};\mathsf{G}_{\rm sq}) = \sum_{i,x,y} p_i \wp(x,y|i)\mu(\hat{P}_x^{\tilde{A}},\hat{Q}_y^{\tilde{B}}|i,\hat{\varrho}_{AB}), \tag{1}$$

in which the joint probability distribution $\mu(\hat{P}_x^{\tilde{A}},\hat{Q}_y^{\tilde{B}}|i,\hat{\varrho}_{AB})$ is given by

$$\mathrm{Tr}(\hat{P}_x^{\tilde{A}} \otimes \hat{Q}_y^{\tilde{B}})(\hat{\tau}_i^{A_0} \otimes \hat{\varrho}_{AB} \otimes \hat{\omega}_i^{B_0}), \tag{2}$$

where $\hat{P}_x^{\tilde{A}} \in \mathcal{M}_{\tilde{A}}$ and $\hat{Q}_y^{\tilde{B}} \in \mathcal{M}_{\tilde{B}}$ are local effects (positive operator-valued measure (POVM) elements) of the players. They win or lose some value if the average reward is positive or negative, respectively.

The players' goal is, of course, to maximize the average amount they can obtain in a game. Let us call the maximum average reward the *payoff* value [27] and denote it by

$$\wp^\star(\hat{\varrho}_{AB};\mathsf{G}_{\rm sq}) = \max_{\hat{P}^{\tilde{A}},\hat{Q}^{\tilde{B}}} \bar{\wp}(\hat{\varrho}_{AB};\hat{P}^{\tilde{A}};\hat{Q}^{\tilde{B}};\mathsf{G}_{\rm sq}). \tag{3}$$

The main result of Buscemi [20], relevant for entanglement detection, can be recast as follows. Given the set of all SQNLGs $\mathcal{G}_{\rm sq}$ and the set of all separable states $\mathcal{S}_{\rm sep}$ for any game $\mathsf{G}_{\rm sq} \in \mathcal{G}_{\rm sq}$ and for any two states $\hat{\varrho}_{AB}, \hat{\sigma}_{AB} \in \mathcal{S}_{\rm sep}$, one has

$$\wp^\star(\hat{\varrho}_{AB};\mathsf{G}_{\rm sq}) = \wp^\star(\hat{\sigma}_{AB};\mathsf{G}_{\rm sq}) \coloneqq \wp^\star(\mathcal{S}_{\rm sep};\mathsf{G}_{\rm sq}). \tag{4}$$

This simply reads as all separable quantum states, at best, are equal in a SQNLG.

Criterion 1. (Buscemi).—A quantum state $\hat{\varrho}_{AB}$ is entangled if and only if there exists a SQNLG for which $\wp^\star(\hat{\varrho}_{AB};\mathsf{G}_{\rm sq}) > \wp^\star(\mathcal{S}_{\rm sep};\mathsf{G}_{\rm sq})$.

It is relevant to ask whether one should search within the whole set $\mathcal{G}_{\rm sq}$ for a game violating Eq. (4). The short answer is negative [21]. Without a loss of generality, we assume that the Hilbert spaces are finite dimensional since entanglement can always be verified in finite dimensional subspaces [28]. It is well known that, by the Hahn-Banach theorem, for any entangled state $\hat{\varrho}_{AB} \notin \mathcal{S}_{\rm sep}$, there exists an EW $\hat{W}$ such that

$$\mathrm{Tr}\hat{W}\hat{\varrho}_{AB} > 0, \quad \text{and} \quad \forall \hat{\sigma}_{AB} \in \mathcal{S}_{\rm sep}, \quad \mathrm{Tr}\hat{W}\hat{\sigma}_{AB} \le 0. \tag{5}$$

Note that, here, for the sake of consistency, we have changed the sign of the usual convention. Moreover, we set $\mathrm{Tr}\hat{W} = -D$, with $D = \min\{d_A, d_B\}$ being the minimum dimensionality of Alice and Bob's subsystems, to compare different EWs, where such a normalization is always possible [29]. Now, every EW can be transformed into a SQNLG as follows. Charlie decomposes the witness in terms of product states as $\hat{W} = \sum_i \beta_i \hat{\tau}_i^{A_0\mathsf{T}} \otimes \hat{\omega}_i^{B_0\mathsf{T}}$, with T denoting the transposition operation and $\beta_i \in \mathbb{R}$, and defines a SQNLG via

$$\hat{W} \leftrightarrow \mathsf{W}_{\rm sq} \Leftrightarrow \wp(x,y|i) = \left(\frac{\beta_i}{p_i}\right)\delta_{1,x}\delta_{1,y}.$$

We can then rewrite Eq. (3) as

$$\wp^\star(\hat{\varrho}_{AB};\mathsf{W}_{\rm sq}) = \max_{\hat{P}^{\tilde{A}},\hat{Q}^{\tilde{B}}} \mathrm{Tr}(\hat{P}_1^{\tilde{A}} \otimes \hat{Q}_1^{\tilde{B}})(\hat{W} \otimes \hat{\varrho}_{AB}). \tag{6}$$

We call any such a game a semiquantum witnessing game (SQWG) and denote the set of all such games by $\mathcal{W}_{\rm sq}$. Branciard *et al.* [21] showed that the set $\mathcal{W}_{\rm sq}$ is indeed necessary and sufficient for verifying the entanglement of a state $\hat{\varrho}_{AB}$ shared by the players. That is, $\wp^\star(\mathcal{S}_{\rm sep};\mathsf{W}_{\rm sq}) \le 0$, and for any entangled state $\hat{\varrho}_{AB} \notin \mathcal{S}_{\rm sep}$, there exists a SQWG such that $\wp^\star(\hat{\varrho}_{AB};\mathsf{W}_{\rm sq}) > 0$.

SQWGs with LOCC.—In general, every EW is (with our sign convention) a member of the compact convex set of normalized block-negative operators (defined as operators with negative expectation values in all pure product states). An extremal EW (EEW) $\hat{W}^e$ is one that cannot be written as a convex combination of any two other block-negative operators, and hence, there exists a pure product state $|a,b\rangle \in \mathcal{S}_{\rm sep}$ such that $\langle a,b|\hat{W}^e|a,b\rangle = 0$ [30,31]. We now introduce the set of *extremal semiquantum witnessing games* (ESQWGs), $\mathcal{W}_{\rm sq}^e \subset \mathcal{W}_{\rm sq}$, which correspond to EEWs. This class of games is necessary and sufficient for entanglement detection, since for every entangled state there exists an EEW which detects it [30,31]. A very important corollary thus follows. For any $\mathsf{W}_{\rm sq}^e \in \mathcal{W}_{\rm sq}^e$, we have that [32]

$$\wp^\star(\mathcal{S}_{\rm sep}; \mathsf{W}_{\rm sq}^e) = 0. \tag{7}$$

We extend this statement by first allowing the local effects to be *relabeled* [37]. This is the procedure of shuffling the labels of the measurement effects and possibly assigning the same label to multiple outcomes with the help of classical communication. This leads to LOCC effects on the shared state and input quantum questions of the form $\hat{Z}_{xy}^{\tilde{A}\tilde{B}} = \sum_{f(u,v)=(x,y)} \hat{P}_{uv}^{\tilde{A}} \otimes \hat{Q}_{uv}^{\tilde{B}} \in \mathcal{M}_{\rm LOCC}$ [38]. Here, x and y are labels to be sent to Charlie, u and v characterize the local outcomes obtained by Alice and Bob, and $f: \mathbb{N}\times\mathbb{N} \to \mathbb{N}\times\mathbb{N}$ is a LOCC strategy relating the output labels to the local measurement outcomes. Note that any LOCC POVM is necessarily separable, but the converse is not true [39]. Next, by substituting this into Eqs. (1) and (2) and restricting the games to extremal ones, we define

$$\wp^{\rm MDI}(\hat{\varrho}_{AB}) = \max_{\mathsf{W}_{\rm sq}^e} \max_{\hat{Z}^{\tilde{A}\tilde{B}}} \bar{\wp}(\hat{\varrho}_{AB}; \hat{Z}_{11}^{\tilde{A}\tilde{B}}; \mathsf{W}_{\rm sq}^e). \tag{8}$$

Consequently, we have the following entanglement criterion.

Criterion 1'.—A quantum state $\hat{\varrho}_{AB}$ is entangled if and only if $\wp^{\rm MDI}(\hat{\varrho}_{AB}) > 0$.

The proof is given in the Supplemental Material [32]. The importance of Criterion 1' is that it reduces the entanglement detection down to a much smaller set of games while simultaneously relaxing to general LOCC measurements.

MDI quantification of entanglement.—Criterion 1' also provides an equivalent way to define the set of separable states as the set of all quantum states providing a maximum payoff of zero: $\mathcal{S}_{\rm sep} = \{\hat{\varrho}|\wp^{\rm MDI}(\hat{\varrho}) = 0\}$. This also induces the idea that there exists the following continuous hierarchy of sets.

Definition 1.—For any $\lambda \geq 0$, define $\mathcal{S}_\lambda = \{\hat{\varrho}_{AB}|\wp^{\rm MDI}(\hat{\varrho}_{AB}) \leq \lambda\}$.

Importantly, the set $\mathcal{S}_\lambda$ is convex as shown in the Supplemental Material [32]. In addition, for any $\lambda > 0$, $\mathcal{S}_{\rm sep} \subset \mathcal{S}_\lambda$, with $\mathcal{S}_{\rm sep} = \mathcal{S}_0$. For any $\hat{\varrho}_{AB} \notin \mathcal{S}_\lambda$, there exists an ESQWG $\mathsf{W}_{\rm sq}^e \in \mathcal{W}_{\rm sq}^e$ and an effect $\hat{Z}_{11}^{\tilde{A}\tilde{B}} \in \mathcal{M}_{\rm LOCC}$ for Alice and Bob such that they can obtain a payoff value $\wp^{\rm MDI}(\hat{\varrho}_{AB}) > \lambda$. To show this, we note that by the Hahn-Banach theorem, there exists a (nonextremal) witness $\hat{W}$ for the convex set $\mathcal{S}_\lambda$ which detects $\hat{\varrho}_{AB}$, and that it can be optimized (i.e., made tangent) to $\mathcal{S}_\lambda$ [29,40]. The resulting optimal witness can be written as a convex combination of extremal points for which at least one of them detects $\hat{\varrho}_{AB}$.

Definition 1, along with the above considerations, suggests that ESQWGs are also necessary and sufficient for characterizing the continuum of the convex sets $\mathcal{S}_\lambda$ via $\wp^{\rm MDI}$. Moreover, we see that the average reward function provides a lower bound on the amount of entanglement shared by Alice and Bob. If, for a given quantum state $\hat{\varrho}_{AB}$, the reward value that Alice and Bob obtain in an ESQWG is $\bar{\wp}(\hat{\varrho}_{AB}; \hat{Z}_{11}^{\tilde{A}\tilde{B}}; \mathsf{W}_{\rm sq}^e) = \lambda_0$, then $\hat{\varrho}_{AB} \notin \mathcal{S}_\lambda$ for any $\lambda < \lambda_0$. We formalize the above observations in the theorem below and point the interested reader to the Supplemental Material for the detailed proof [32].

Theorem 1.—The payoff $\wp^{\rm MDI}$ measures entanglement without relying on the quantum description of the measurement devices.

Importantly, not only is $\wp^{\rm MDI}$ a measure of entanglement for the shared state, but allowing the players to access infinite rounds of LOCC on input questions will not improve their best achievement. Consequently, we can relax the LOSR restriction in ESQWGs to LOCC [41,42]. Nevertheless, it is clear that this task of measuring $\wp^{\rm MDI}$ is practically challenging in high dimensions. Shortly, we will provide a particularly interesting scenario where the referee is only interested in the amount of NPT entanglement which, in turn, eliminates the need for the maximization over all EEWs. This removes the aforementioned difficulty while preserving measurement-device independence.

MDI quantification of NPT entanglement.—It is a well known fact that there are two types of entangled states, namely, positive- and negative-partial-transpose (P- and NPT) entangled states, which possess legitimate or unphysical density operators upon partial transposition, respectively. It is also known that NPT entanglement is necessary for distillability [26], and this is the only type of entanglement for systems with dimensions up to 6 [43], e.g., two-qubit systems.

Similarly, EEWs are divided into indecomposable and decomposable classes, where the latter only detects NPT entangled states [29,44]. Denoting the corresponding games as $\mathcal{W}_{\rm sq}^{\rm ie}$ and $\mathcal{W}_{\rm sq}^{\rm de}$, respectively, we have $\mathcal{W}_{\rm sq}^e = \mathcal{W}_{\rm sq}^{\rm ie} \cup \mathcal{W}_{\rm sq}^{\rm de}$. We now state and prove the most important result of the present Letter, which enables a referee to characterize NPT entanglement between two *untrusted* agents.

Theorem 2.—For every Schmidt-rank-D decomposable ESQWG $\mathsf{W}_{\rm sq}^{\rm de}$, the payoff,

$$\wp_{\rm NPT}^{\rm MDI}(\hat{\varrho}_{AB}; \mathsf{W}_{\rm sq}^{\rm de}) = \max_{\hat{Z}^{\tilde{A}\tilde{B}}} \bar{\wp}(\hat{\varrho}_{AB}; \hat{Z}_{11}^{\tilde{A}\tilde{B}}; \mathsf{W}_{\rm sq}^{\rm de}), \tag{9}$$

measures NPT entanglement without relying on the quantum description of the measurement devices.

An immediate consequence is the following.

Corollary.—$\wp_{\mathrm{NPT}}^{\mathrm{MDI}}$ is necessary and sufficient for full MDI characterization of entanglement of the systems with dimensions up to 6.

To outline the proof of the above theorem, we first notice that decomposable EEWs are sufficient for detection of NPT entangled states and possess a very simple structure [30]; they are of the form $\hat{W}^{\mathrm{de}} = -D|\psi\rangle\langle\psi|^{\mathsf{T}_B}$, where $|\psi\rangle$ is a normalized entangled vector, and T_B denotes the partial transposition operation with respect to the second party. Second, in a $d_A \times d_B$ dimensional Hilbert space, we may further restrict the vectors $|\psi\rangle$ to have a Schmidt rank of $D = \min\{d_A, d_B\}$. The main point here is that, for any Schmidt-rank-D pure entangled state $|\psi\rangle$, there exists a stochastic LOCC (SLOCC) procedure that converts $|\psi\rangle$ into an arbitrary pure entangled state $|\phi\rangle$ with the same Schmidt rank [1,34,35]. The class SLOCC is a subset of separable operations, implying that the partial transpose of a SLOCC map is also SLOCC. Therefore, $\hat{W}^{\mathrm{de}}$ can be transformed into any other decomposable EEW $\hat{V}^{\mathrm{de}} = -D|\phi\rangle\langle\phi|^{\mathsf{T}_B}$, with a nonzero probability $0 < q \leq 1$ via SLOCC. This simple fact enables Alice and Bob to win a positive payoff in an arbitrary Schmidt-rank-D decomposable ESQWG chosen by Charlie if and only if they share a NPT entangled state, via appropriately altering the questions using SLOCC. As a result, the maximization on ESQWGs in Eq. (8) becomes unnecessary for Charlie if we restrict the games to Schmidt-rank-D decomposable extremal ones. We refer the interested reader to the Supplemental Material [32] for a detailed proof of Theorem 2.

Clearly, $\wp_{\mathrm{NPT}}^{\mathrm{MDI}}(\hat{\varrho}_{AB}; \mathsf{W}_{\mathrm{sq}}^{\mathrm{de}}) \leq \wp^{\mathrm{MDI}}(\hat{\varrho}_{AB})$ and $\wp_{\mathrm{NPT}}^{\mathrm{MDI}}(\hat{\varrho}_{AB}; \mathsf{W}_{\mathrm{sq}}^{\mathrm{de}}) = 0$ if and only if $\hat{\varrho}_{AB} \in \mathcal{S}_{\mathrm{PPT}}$. We also note that universality follows from the fact that all completely positive local operations (in particular, invertible ones) preserve PPT and NPT entanglement. Furthermore, changing the game to a different Schmidt-rank-D decomposable ESQWG provides a different universal measure of NPT entanglement. We emphasize that the whole procedure described here is MDI and thus, it is not possible for the players to cheat and convince the referee that they have more NPT entanglement than that contained in their state.

At this point, it is important to mention that the maximization in the expression for $\wp_{\mathrm{NPT}}^{\mathrm{MDI}}$ is, in principle, performed by the players. Note that this is of least importance for the referee because $\bar{\wp} \leq \wp_{\mathrm{NPT}}^{\mathrm{MDI}}$ guarantees that the average reward always gives a lower bound on the amount of NPT entanglement of $\hat{\varrho}_{AB}$. To Charlie, the average reward $\bar{\wp}$ can be considered as the *effective entanglement* shared by Alice and Bob. This is the amount of NPT entanglement contained within their shared state $\hat{\varrho}_{AB}$ extracted by their LOCC effect. We also note that Charlie's payment is based on the quantum questions he prepares himself and the coincidence statistics of the responses from Alice and Bob. Thus, he does not need to make any assumptions about Alice and Bob's measurements in any form, as long as they are spatially separated. However, he should hide the indices of the questions by ensuring that his questions cannot be unambiguously discriminated and that there are no side channels from his lab to Alice and Bob [41]. The players can increase $\bar{\wp}$ by either sharing a more entangled state or using a better LOCC strategy. We also emphasize that there is no need for the referee to trust the players; if the players do not perform their optimization appropriately, they will incur losses.

Connection to other measures.—Consider the measure $\wp_{\mathrm{NPT}}^{\mathrm{MDI}}(\hat{\varrho}_{AB}; \mathsf{W}_{\mathrm{sq}}^{\mathrm{de}})$ obtained in a decomposable ESQWG, where the optimal POVM element is determined to be $\hat{X}_{11}^{\tilde{A}\tilde{B}}$, i.e., $\wp_{\mathrm{NPT}}^{\mathrm{MDI}}(\hat{\varrho}_{AB}; \mathsf{W}_{\mathrm{sq}}^{\mathrm{de}}) = \max_{\hat{Z}^{\tilde{A}\tilde{B}}} \mathrm{Tr}\hat{Z}_{11}^{\tilde{A}\tilde{B}}(\hat{W}^{\mathrm{de}} \otimes \hat{\varrho}_{AB}) = \mathrm{Tr}\hat{X}_{11}^{\tilde{A}\tilde{B}}(\hat{W}^{\mathrm{de}} \otimes \hat{\varrho}_{AB})$. Following the discussion given in the previous section, defining the partial trace of the POVM element and the state as the *effective entangled state*, $\hat{\varsigma}_{A_0B_0} = \mathrm{Tr}_{AB}\hat{X}_{11}^{\tilde{A}\tilde{B}}\hat{\varrho}_{AB}$, we arrive at the following form of the measure:

$$\wp_{\mathrm{NPT}}^{\mathrm{MDI}}(\hat{\varrho}_{AB}; \mathsf{W}_{\mathrm{sq}}^{\mathrm{de}}) = \max_{\hat{V}^{\mathrm{de}} \in \mathcal{V}^{\mathrm{de}}} \mathrm{Tr}_{A_0B_0}\hat{V}^{\mathrm{de}}\hat{\varsigma}_{A_0B_0}, \tag{10}$$

where $\mathcal{V}^{\mathrm{de}}$ is the set of all decomposable EEWs with a trace equal to $-D$. The equality can be easily deduced by noting that any transformation from $\hat{W}^{\mathrm{de}}$ to some better witness can be done using SLOCC operations, the effect of which can be mimicked via the conjugate SLOCC operation on the state $\hat{\varsigma}_{A_0B_0}$. By assumption, this leads to no increase in the payoff and thus, $\hat{W}^{\mathrm{de}}$ is the witness with highest payoff for $\hat{\varsigma}_{A_0B_0}$.

The second equality in Eq. (10) has exactly the form of the witness-based measures introduced by Brandão [14] for the class of decomposable witnesses with a trace equal to $-D$ [45]. Consequently, we argue that $\wp_{\mathrm{NPT}}^{\mathrm{MDI}}$ is computable using convex optimization algorithms in almost all cases of interest. Following Brandão [14] and Eisert *et al.* [15], in this particular case, our measure provides a MDI lower bound on the amount of random robustness, $R(\hat{\varsigma}_{A_0B_0}) \geq \wp_{\mathrm{NPT}}^{\mathrm{MDI}}(\hat{\varrho}_{AB}; \mathsf{W}_{\mathrm{sq}}^{\mathrm{de}})$, [13] that is the minimum amount of white noise to be added to the effective entangled state $\hat{\varsigma}_{A_0B_0}$ so that all the entanglement is removed [46].

Example.—Consider the Schmidt-rank-2 decomposable EEW $\hat{W}^{\mathrm{de}} = -2|\Psi^-\rangle\langle\Psi^-|^{\mathsf{T}_B}$, where $|\Psi^-\rangle = (1/\sqrt{2})(|01\rangle - |10\rangle)$ is a Bell state. In a standard witnessing procedure, the Bell state $|\Phi^+\rangle_{AB} = (1/\sqrt{2})(|00\rangle_{AB} + |11\rangle_{AB})$ is detected by maximally violating the witnessing inequality of Eq. (5), $\mathrm{Tr}\hat{W}^{\mathrm{de}}|\Phi^+\rangle_{AB}\langle\Phi^+| = 1$, while the other Bell states cannot be detected using $\hat{W}^{\mathrm{de}}$ and require different witnesses. In an ESQWG corresponding to $\hat{W}^{\mathrm{de}}$, on the other hand, by sharing $|\Phi^+\rangle_{AB}$, Alice and Bob will win the payoff $\wp^{\mathrm{MDI}}_{\mathrm{NPT}}(|\Phi^+\rangle_{AB}) = 1$ if they perform the projection onto $\hat{Z}^{\tilde{A}\tilde{B}}_{11} = |\Phi^+\rangle_{\tilde{A}}\langle\Phi^+| \otimes |\Phi^+\rangle_{\tilde{B}}\langle\Phi^+| + |\Phi^-\rangle_{\tilde{A}}\langle\Phi^-| \otimes |\Phi^-\rangle_{\tilde{B}}\langle\Phi^-| + |\Psi^+\rangle_{\tilde{A}}\langle\Psi^+| \otimes |\Psi^+\rangle_{\tilde{B}}\langle\Psi^+| + |\Psi^-\rangle_{\tilde{A}}\langle\Psi^-| \otimes |\Psi^-\rangle_{\tilde{B}}\langle\Psi^-|$. Now, one would naively expect that the players could not gain a positive reward in the same game if they share instead, for instance, the state $|\Phi^-\rangle_{AB}$, just as the witness $\hat{W}^{\mathrm{de}}$ could not detect their state in the standard witnessing procedure. Theorem 2, however, states the contrary because the shared state is indeed NPT entangled. It can be easily checked that if Alice and Bob project onto $\hat{Z}^{\tilde{A}\tilde{B}}_{11} = |\Phi^-\rangle_{\tilde{A}}\langle\Phi^-| \otimes |\Phi^+\rangle_{\tilde{B}}\langle\Phi^+| + |\Phi^+\rangle_{\tilde{A}}\langle\Phi^+| \otimes |\Phi^-\rangle_{\tilde{B}}\langle\Phi^-| + |\Psi^-\rangle_{\tilde{A}}\langle\Psi^-| \otimes |\Psi^+\rangle_{\tilde{B}}\langle\Psi^+| + |\Psi^+\rangle_{\tilde{A}}\langle\Psi^+| \otimes |\Psi^-\rangle_{\tilde{B}}\langle\Psi^-|$, they will obtain the payoff $\wp^{\mathrm{MDI}}_{\mathrm{NPT}}(|\Phi^-\rangle_{AB}) = 1$. As a result, in accordance with Theorem 2, both $|\Phi^+\rangle_{AB}$ and $|\Phi^-\rangle_{AB}$ are maximally NPT entangled as measured by $\wp^{\mathrm{MDI}}_{\mathrm{NPT}}$.

Multipartite extension.—It is straightforward to extend our approach to quantify the entanglement within any partitioning of a multipartite quantum state. In such scenarios, there are K players denoted by the index set $\mathbf{I} = \{1, 2, \ldots, K\}$, where a k partition of them is uniquely specified by the set $\mathbf{P}_k = \{\mathbf{I}_1, \ldots, \mathbf{I}_k\}$ such that $\cup_{j=1}^{k}\mathbf{I}_j = \mathbf{I}$ and that the players within the same party $\mathbf{I}_j$ $(j = 1, \ldots, k)$ can perform joint (global) measurements on their respective questions, while the group of players in different parties are confined to LOCC.

According to Refs. [19,47], in general, multipartite entanglement has a highly complex structure. However, the subset of witnesses extremal to the set of $\mathbf{P}_k$-separable quantum states is necessary and sufficient for detecting entanglement within $\mathbf{P}_k$. Depending on the partitioning, Charlie thus performs the optimization over all such games denoted as $\mathcal{W}^{\mathbf{P}_k}_{\mathrm{sq}}$.

Theorem 3.—The payoff,

$$\wp^{\mathrm{MDI}}(\hat{\varrho}_{\mathbf{P}_k}) = \max_{\mathsf{W}^{\mathbf{P}_k}_{\mathrm{sq}} \in \mathcal{W}^{\mathbf{P}_k}_{\mathrm{sq}}} \max_{\hat{Z}^{\mathbf{P}_k} \in \mathcal{M}^{\mathbf{P}_k}_{\mathrm{LOCC}}} \bar{\wp}(\hat{\varrho}_{AB}; \hat{Z}^{\mathbf{P}_k}_{11}; \mathsf{W}^{\mathbf{P}_k}_{\mathrm{sq}}), \tag{11}$$

measures entanglement with respect to the partitioning $\mathbf{P}_k$ in a MDI way, and it is universal and faithful.

The proof follows from the same line of proof of Theorem 1.

Conclusions.—We showed that entanglement can be quantified operationally in a measurement-device-independent way within the context of extremal semi-quantum witnessing games, a subclass of semiquantum nonlocal games, and in the LOCC paradigm. Thus, we reduced the whole set of games down to a much smaller subset of games. We proved that the LOCC does not help the players to increase their maximum reward for a fixed amount of effective shared entanglement. In this way, the average reward provides a lower bound on the amount of entanglement within the shared state, while the payoff value provides a universal convex measure of entanglement. We also showed that an arbitrary decomposable member of this class of games is necessary and sufficient for both detection and quantification of NPT entanglement, and thus, we reduced the whole set of games down to a single arbitrary game in such scenarios. We also extended our approach to the multipartite scenario where quantification of entanglement within an arbitrary partitioning of a multipartite quantum state is desired.

The authors acknowledge useful discussions with Maciej Lewenstein and Fabio Costa. This project was supported by the Australian Research Council Centre of Excellence for Quantum Computation and Communication Technology (CE110001027).

*f.shahandeh@uq.edu.au

[1] M. A. Nielsen and I. L. Chunang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
[2] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009).
[3] (The LIGO Scientific Collaboration), Nat. Phys. **7**, 962 (2011).
[4] L. Gurvits, in *Proceedings of the Thirty-fifth Annual ACM Symposium on Theory of Computing, 2003* (ACM, New York, 2003), p. 10.
[5] S. Gharibian, Quantum Inf. Comput. **10**, 343 (2010).
[6] A. Furusawa, J. L. Sørensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik, Science **282**, 706 (1998).
[7] S. Parker, S. Bose, and M. B. Plenio, Phys. Rev. A **61**, 032305 (2000).
[8] D. Gross, S. T. Flammia, and J. Eisert, Phys. Rev. Lett. **102**, 190501 (2009).
[9] C. Gross, T. Zibold, E. Nicklas, J. Estve, and M. K. Oberthaler, Nature (London) **464**, 1165 (2010).
[10] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 1996.
[11] K. Zyczkowski, P. Horodecki, A. Sanpera, and M. Lewenstein, Phys. Rev. A **58**, 883 (1998).
[12] G. Vidal and R. F. Werner, Phys. Rev. A **65**, 032314 (2002).
[13] G. Vidal and R. Tarrach, Phys. Rev. A **59**, 141 (1999).
[14] F. G. S. L. Brandão, Phys. Rev. A **72**, 022310 (2005).
[15] J. Eisert, F. G. S. L. Brandão, and K. M. R. Audenaert, New J. Phys. **9**, 46 (2007).
[16] J. Sperling and W. Vogel, Phys. Rev. A **83**, 042315 (2011).
[17] S.-S. B. Lee and H.-S. Sim, Phys. Rev. A **85**, 022325 (2012).
[18] F. Shahandeh, J. Sperling, and W. Vogel, Phys. Rev. A **88**, 062323 (2013).
[19] F. Shahandeh, J. Sperling, and W. Vogel, Phys. Rev. Lett. **113**, 260502 (2014).
[20] F. Buscemi, Phys. Rev. Lett. **108**, 200401 (2012).
[21] C. Branciard, D. Rosset, Y-C. Liang, and N. Gisin, Phys. Rev. Lett. **110**, 060405 (2013).
[22] P. Xu, X. Yuan, L.-K. Chen, H. Lu, X.-C. Yao, X. Ma, Y.-A. Chen, and J.-W. Pan, Phys. Rev. Lett. **112**, 140506 (2014).

[23] M. Nawareg, S. Muhammad, E. Amselem, and M. Bourennane, Sci. Rep. **5**, 8048 (2015).

[24] E. Verbanis, A. Martin, D. Rosset, C. C. W. Lim, R. T. Thew, and H. Zbinden, Phys. Rev. Lett. **116**, 190501 (2016).

[25] E. G. Cavalcanti, M. J. W. Hall, and H. M. Wiseman, Phys. Rev. A **87**, 032306 (2013).

[26] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998).

[27] Note that our terminology here is slightly different from that of Buscemi. As we will see shortly, the payoff made by Charlie is always considered by him to be the best Alice and Bob could do.

[28] J. Sperling and W. Vogel, Phys. Rev. A **79**, 052313 (2009).

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

[30] D. Chruściński and G. Sarbicki, J. Phys. A **47**, 483001 (2014).

[31] F. Shultz, J. Math. Phys. (N.Y.) **57**, 015218 (2016).

[32] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.118.150505, which includes Refs. [1,33–36], for detailed proofs of Eq. (7), Criterion 1', the convexity of the sets $\mathcal{S}_\lambda$, and Theorems 1 and 2.

[33] J. Sperling and W. Vogel, Phys. Scr. **83**, 045002 (2011).

[34] M. A. Nielsen, Phys. Rev. Lett. **83**, 436 (1999).

[35] G. Vidal, Phys. Rev. Lett. **83**, 1046 (1999).

[36] M. Nielsen and G. Vidal, Quantum Inf. Comput. **1**, 76 (2001).

[37] E. Haapasalo, T. Heinosaari, and J-P. Pellonpää, Quantum Inf. Process. **11**, 1751 (2012).

[38] V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight, Phys. Rev. Lett. **78**, 2275 (1997).

[39] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **59**, 1070 (1999).

[40] J. Sperling and W. Vogel, Phys. Rev. A **79**, 042337 (2009).

[41] D. Rosset, C. Branciard, N. Gisin, and Y-C. Liang, New J. Phys. **15**, 053025 (2013).

[42] The authors of Ref. [41] have shown that the correlations from entangled states in a SQWG cannot be simulated classically even if the two spatially separated parties have access to LOCC. Here, however, we have shown in Theorem 1 that relaxing the LOSR to LOCC within the context of ESQWGs allows the payoff function to induce a faithful measure of entanglement.

[43] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).

[44] S. L. Woronowicz, Rep. Math. Phys. **10**, 165 (1976).

[45] Note that, as shown by Brandão [14], many entanglement measures can be recast as witness-based measures, depending on the choice of the subset of all entanglement witnesses on which the optimization is performed.

[46] I. Šupić, P. Skrzypczyk, and D. Cavalcanti, arXiv:1702.04752.

[47] J. Sperling and W. Vogel, Phys. Rev. Lett. **111**, 110503 (2013).