Correlations in Entanglement-Assisted Prepare-and-Measure Scenarios

Armin Tavakoli⬤,[1,2,3,†] Jef Pauwels⬤,[4,*,†] Erik Woodhead,[4] and Stefano Pironio[4]

[1]*Institute for Quantum Optics and Quantum Information—IQOQI Vienna, Austrian Academy of Sciences, Boltzmanngasse 3, Vienna 1090, Austria*

[2]*Département de Physique Appliquée, Université de Genève, Genève CH-1211, Switzerland*

[3]*Institute for Atomic and Subatomic Physics, Vienna University of Technology, 1020 Vienna, Austria*

[4]*Laboratoire d'Information Quantique, Université libre de Bruxelles (ULB), B-1050 Brussels, Belgium*

We investigate the correlations that can arise between Alice and Bob in prepare-and-measure communication scenarios where the source (Alice) and the measurement device (Bob) can share prior entanglement. The paradigmatic example of such a scenario is the quantum dense-coding protocol, where the communication capacity of a qudit can be doubled if a two-qudit entangled state is shared between Alice and Bob. We provide examples of correlations that actually require more general protocols based on higher-dimensional entangled states. This motivates us to investigate the set of correlations that can be obtained from communicating either a classical or a quantum d-dimensional system in the presence of an unlimited amount of entanglement. We show how such correlations can be characterized by a hierarchy of semidefinite programming relaxations by reducing the problem to a noncommutative polynomial optimization problem. We also introduce an alternative relaxation hierarchy based on the notion of informationally restricted quantum correlations, which, though it represents a strict (nonconverging) relaxation scheme, is less computationally demanding. As an application, we introduce device-independent tests of the dimension of classical and quantum systems that, in contrast to previous results, do not make the implicit assumption that Alice and Bob share no entanglement. We also establish several relations between communication with and without entanglement as resources for creating correlations.

I. INTRODUCTION

The archetype communication scenario, which is ubiquitous in classical and quantum information theory, is the prepare-and-measure scenario illustrated in Fig. 1(a). Alice prepares a physical system, depending on some input $x \in \{1, \ldots, n_X\}$, and sends it to Bob. Bob then performs on the incoming system a measurement, according to some choice of input $y \in \{1, \ldots, n_Y\}$, and obtains an output $b \in \{1, \ldots, n_B\}$. From an operational perspective, this prepare-and-measure scenario is completely characterized by the conditional probabilities $p(b|x, y)$, which describe the correlations that are established between Alice and Bob. These correlations are limited by the amount of communication carried by the physical systems from Alice to Bob.

Communication may naturally be, and is commonly, quantified in terms of the dimension d of the exchanged messages, i.e., the alphabet size for classical messages and the dimension of the Hilbert space for quantum messages. Consequently, much research has been directed at studying the correlations $p(b|x, y)$ that arise from the communication of a classical or quantum d-dimensional system. This covers a wide range of topics, including foundations of quantum theory [1,2], dimension witnessing [3–6], random access coding [7–9], quantum random-number generation [10,11], quantum key distribution [12,13], self-testing [14–16], and various protocols for characterizing and certifying quantum devices [17–19]. It has also motivated a considerable number of experiments (see, e.g., Refs. [20–26]).

Typically, quantum communication models, e.g., as in the above references, consider Alice and Bob as initially independent or allow them to share a classical random variable [as in Fig. 1(a)]. However, quantum theory naturally enables a more general communication scenario in which Alice and Bob share prior entanglement [as in Fig. 1(b)].

---

*jef.pauwels@ulb.be

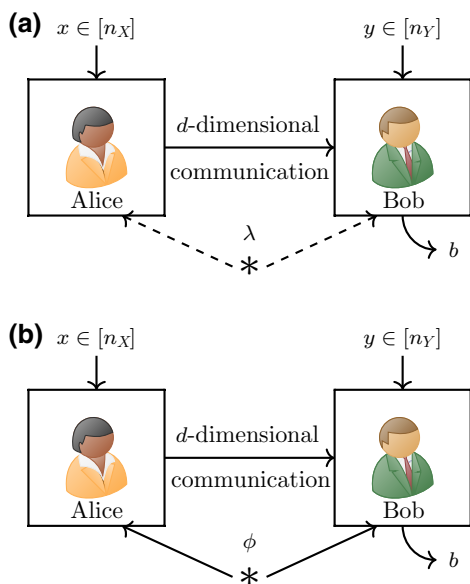†These authors share the first authorship.

FIG. 1. The prepare-and-measure scenario. Alice encodes an input x into a physical system communicated to Bob. Bob measures the incoming system depending on an input y and obtains an output b. We are interested in characterizing the possible conditional probabilities $p(b|x,y)$ if the communication is limited to d-dimensional messages. Much of past research has considered the case (a) where Alice and Bob are initially independent or share classical randomness. We consider the situation (b) where they share quantum entanglement.

The introduction of entanglement to assist classical and quantum communication should enlarge the set of possible correlations between Alice and Bob. Indeed, while entanglement itself cannot be used for communication, it is well known to amplify the capacity of quantum channels [27], most famously via the quantum dense-coding protocol [28]. In fact, even if Alice only communicates classical messages to Bob, prior entanglement provides an advantage for different tasks, such as communication complexity [29–31] and random access codes [32].

An understanding of how the presence of entanglement impacts the set of possible correlations between Alice and Bob is also important for analyzing the security of semi-device-independent prepare-and-measure protocols such as random-number generation and quantum key distribution. Commonly, such protocols are based on unentangled devices. Nevertheless, even if Alice's and Bob's devices are initially uncorrelated, quantum messages in the early communication rounds could be used to build up shared entanglement that could then be exploited in later rounds in order to corrupt the protocol.

In spite of the conceptual and practical interest, much less is known about prepare-and-measure scenarios with entanglement than scenarios without entanglement. It is particularly noteworthy that, in contrast to the setting

without entanglement [33,34], no general technique is known for bounding (from the exterior) the set of correlations $p(b|x,y)$ that can be generated by d-dimensional messages assisted by a, potentially unbounded amount of, entanglement. In this work, we address this central question and initiate a systematic study of prepare-and-measure scenarios with entanglement.

In Sec. II, we define formally the entanglement-assisted (EA) communication scenario that we consider. The quantum dense-coding protocol, which is the paradigmatic example by which entanglement can enhance quantum communication, exploits an entangled pair of the same local dimension as the quantum communication (i.e., an entangled qubit pair in the case that a qubit is transmitted). In Sec. III, we show that certain correlations that can be achieved by sending an EA qubit require higher-dimensional entanglement. The classical analog of this result is established in Ref. [35]. Motivated by these observations, we proceed in Sec. IV by addressing the general question of characterizing the set of correlations achievable with d-dimensional classical and quantum communication when the communicating parties may share any amount of entanglement. We connect this problem to noncommutative polynomial optimization [36] and to the recently developed concept of informationally restricted correlations [37,38]. This allows us to bound the correlations using a hierarchy of semidefinite programming (SDP) relaxations. In Sec. V, we apply our methods to different device-independent tests of classical and quantum dimension. In all considered examples, our method produces either verifiably optimal bounds or (at worst) nearly optimal bounds. Our more general setting leads us to reexamine the conclusions that one can draw from such dimension tests in light of shared entanglement. Finally, in Sec. VI, we apply our methods to investigate the relationship between entanglement and quantum communication as resources for creating correlations. We show that there exist situations where either resource can outperform the other. While such questions have been the topic also of previous research efforts [26,32,39–42], our analysis requires no additional assumptions and is tolerant to noise.

II. CORRELATIONS FROM ENTANGLEMENT-ASSISTED d-DIMENSIONAL COMMUNICATION

Consider an experiment featuring two parties, Alice and Bob, who share an arbitrary, and without loss of generality, pure entangled state $|\phi_{AB}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ [43]. Alice receives an input x from the set $[n_X] \equiv \{1, \ldots, n_X\}$ and encodes her input, possibly using her share of the entangled state $|\phi\rangle$, into a system C of dimension no greater than d that is sent to Bob. Bob receives an input $y \in [n_Y] \equiv \{1, \ldots, n_Y\}$ and performs a measurement, depending on y, on the incoming system C and his share of the entangled state. The
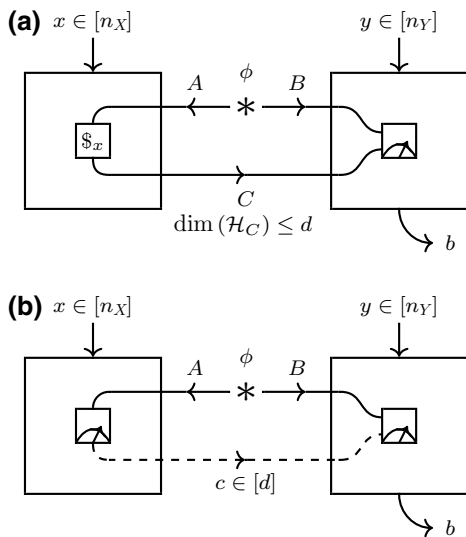
FIG. 2. (a) The general channel. When Alice and Bob share an entangled state ϕ, Alice encodes her classical input x into a d-dimensional message c by applying a quantum channel $\$_x$. Depending on his classical input y, Bob performs a joint measurement $\{M_{b|y}\}_b$ on Alice's message and his share of the entanglement and produces an outcome b. (b) The quantum-to-classical channel. When the communication is classical, Alice performs a POVM $\{M_{c|x}\}_c$ and relays the outcome c to Bob. Bob's operation can be viewed as a POVM $\{M_{b|y,c}\}_{y,c}$ conditioned on his classical input y and Alice's message c.

outcome of this measurement is denoted by $b \in [n_B] \equiv \{1, \ldots, n_B\}$. This scenario is characterized by the conditional probability distributions $p(b|x,y)$, which we refer to as the correlations.

The most general way that Alice can exploit her share of the entangled state when encoding her classical input x into the d-dimensional system C is through the application of a completely positive trace-preserving (CPTP) map $\$_x : L(\mathcal{H}_A) \to L(\mathcal{H}_C)$ from the space $L(\mathcal{H}_A)$ of linear operators on $\mathcal{H}_A$ to the space $L(\mathcal{H}_C)$ of linear operators on $\mathcal{H}_C \simeq \mathbb{C}^d$. The total state available to Bob, composed of the communicated d-dimensional quantum system C from Alice and of his share of $|\phi\rangle$, is then $\tau_{CB}^x \equiv (\$_x \otimes \mathbb{1}_B)[|\phi_{AB}\rangle\langle\phi_{AB}|]$. The most general measurement he can perform on this state when selecting input y is then given by a measurement (a positive operator-valued measure, or POVM) with elements $\{M_{b|y}\}_b$. This is illustrated in Fig. 2(a) and leads to the following definition.

Definition 1. *We say that the correlations $p(b|x,y)$ can be reproduced by an EA d-dimensional quantum communication protocol if there exists*

(a) *A bipartite pure entangled state $|\phi_{AB}\rangle$ in $\mathcal{H}_A \otimes \mathcal{H}_B$, where A and B are physical systems with finite or separable [44] Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$*

(b) *A CPTP map $\$_x : L(\mathcal{H}_A) \to L(\mathcal{H}_C)$ from system A to a system C with a d-dimensional Hilbert space $\mathcal{H}_C \simeq \mathbb{C}^d$ for each input x*

(c) *An n_B-outcome POVM $\{M_{b|y}\}_b$ on the joint systems C and B for each input y*

such that

$$p(b|x,y) = \mathrm{Tr}\left(\tau_{CB}^x M_{b|y}\right), \tag{1}$$

where

$$\tau_{CB}^x \equiv (\$_x \otimes \mathbb{1}_B)\left[|\phi_{AB}\rangle\langle\phi_{AB}|\right]. \tag{2}$$

The above definition is fully general and assumes that the communication from Alice to Bob is quantum. However, we can also restrict the communication to be classical. This can be represented in the Hilbert-space formalism of quantum theory by imposing that the CPTP maps $\$_x$ output diagonal classical states: $\$_x[\rho] = \sum_{c=1}^d p(c|x,\rho)|c\rangle\langle c|$ for all $\rho \in L(\mathcal{H}_A)$. The Riesz representation theorem asserts that, for every x, linear maps of the form $p(c|x,\rho)$ can be written in terms of the Born rule. Therefore, any CPTP map of this form represents the outcome of a POVM $\{M_{c|x}\}_c$ performed on the input state ρ: $\$_x[\rho] = \sum_{c=1}^d \mathrm{Tr}\left(\rho M_{c|x}\right)|c\rangle\langle c|$. The states available to Bob are then the classical-quantum (CQ) states $\tau_{CB}^x = (\$_x \otimes \mathbb{1}_B)\left[|\phi_{AB}\rangle\langle\phi_{AB}|\right] = \sum_{c=1}^d |c\rangle\langle c| \otimes \tau_B^{c,x}$, where $\tau_B^{c,x} = \mathrm{Tr}_A\left(|\phi_{AB}\rangle\langle\phi_{AB}|M_{c|x} \otimes \mathbb{1}_B\right)$ is the (subnormalized) reduced state of Bob when Alice performs the POVM $\{M_{c|x}\}$ on her share of $|\phi_{AB}\rangle$ and obtains outcome c. Any measurement by Bob on such a CQ state can be viewed as Bob first reading the classical system C and then performing a measurement on the quantum system B depending on the value c he obtained. This is illustrated in Fig. 2(b). The correlations that Alice and Bob generate are then $p(b|x,y) = \sum_c \mathrm{Tr}\left(\tau_B^{c,x} M_{b|y,c}\right) = \sum_c \mathrm{Tr}\left(|\phi_{AB}\rangle\langle\phi_{AB}| M_{c|x} \otimes M_{b|y,c}\right)$. We thus have the following definition in the classical case.

Definition 2. *We say that the correlations $p(b|x,y)$ can be reproduced by an EA d-dimensional classical communication protocol if there exists*

(a) *A bipartite pure entangled state $|\phi_{AB}\rangle$ in $\mathcal{H}_A \otimes \mathcal{H}_B$, where A and B are physical systems with finite or separable Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$*

(b) *A d-outcome POVM $\{M_{c|x}\}_c$ on A for each input x*

(c) *An n_B-outcome POVM $\{M_{b|y,c}\}_b$ on B for each input y and $c \in [d]$*

such that

$$p(b|x,y) = \sum_{c=1}^d \mathrm{Tr}\left(|\phi_{AB}\rangle\langle\phi_{AB}| M_{c|x} \otimes M_{b|y,c}\right). \tag{3}$$

Note that Eq. (3) simply represents Bob's marginal correlations in a kind of bipartite Bell experiment where the measurement performed on Bob's side depends not only on his input y but also on the communicated output c of Alice's measurement.

III. BEYOND DENSE CODING: QUBIT COMMUNICATION ENHANCED BY FOUR-DIMENSIONAL ENTANGLEMENT

The simplest form of quantum communication has Alice sending qubits ($d = 2$) to Bob. While a single qubit can only carry only 1 bit of information [45], it is well known that if Alice and Bob share the maximally entangled two-qubit state

$$|\phi_{\max}\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big), \qquad (4)$$

Alice can use a single qubit of communication to send 2 bits of information to Bob; this is the quantum dense-coding protocol [28]. Specifically, in this celebrated protocol, Alice has four possible inputs $x = (x_1, x_2) \in \{0, 1\}^2$ and, given x, applies the Pauli unitary $X^{x_2}Z^{x_1}$ to her share of $|\phi_{\max}\rangle$ before sending it to Bob. Bob's total state $|\tau_{CB}^x\rangle = (X^{x_2}Z^{x_1} \otimes \mathbb{1}_B)|\phi_{\max}\rangle$ then corresponds to one the four Bell states $\{(|00\rangle \pm |11\rangle)/\sqrt{2}, (|01\rangle \pm |10\rangle)/\sqrt{2}\}$, depending on Alice's input x. Since these states form a basis, Bob can deterministically learn the value of x by measuring in this basis, thus allowing Alice to send 2 bits to Bob. More generally, this protocol enables Bob to generate any correlations $p(b|x, y)$ in a protocol with $n_X = 4$, since knowing Alice's input x and his input y, Bob can sample b according to the desired distribution $p(b|x, y)$.

Note that from the perspective of the general definition introduced in the previous section, the dense-coding protocol is particular in that the shared entangled state is of the same local dimension as the communicated quantum system and the CPTP maps applied by Alice are unitaries. We now provide a qubit communication example, based on a modified random access coding task, where entanglement of local dimension *four* processed by nonunitary CPTP maps outperforms any strategy based on two-dimensional entanglement.

A. Random access code with flagged input

The starting point for the task that we introduce is the usual $2 \to 1$ quantum random access code (RAC) [7], where Alice must encode 2 bits $x = (x_1, x_2) \in \{00, 01, 10, 11\}$ in a single qubit such that Bob is able to guess as best as possible either the first bit, if $y = 1$, or the second bit, if $y = 2$. Denoting Bob's guess by $b \in \{0, 1\}$ and assuming that Alice's and Bob's inputs are chosen uniformly, the success probability of Bob is given by $\frac{1}{8} \sum_{x_1, x_2 = 0}^{1} \sum_{y=1}^{2} p(b = x_y | (x_1, x_2), y)$.

For convenience, we introduce the change of notation $x \in \{00, 01, 10, 11\} \to \{1, 2, 3, 4\}$ and $b \in \{0, 1\} \to b \in \{1, -1\}$. We can then write the success probability as $1/2 + W_{\text{RAC}}/16$, where W_{RAC} is the RAC correlation function

$$W_{\text{RAC}} = \sum_{x=1}^{4} \sum_{y=1}^{2} c_{xy} E_{xy}, \qquad (5)$$

$E_{xy} = p(1|x, y) - p(-1|x, y)$ denotes the expectation value of b, and the 4×2 coefficients c_{xy} are given by

$$c = \begin{pmatrix} 1 & 1 \\ 1 & -1 \\ -1 & 1 \\ -1 & -1 \end{pmatrix}. \qquad (6)$$

Obviously, if shared entanglement is present, then a value of $W_{\text{RAC}} = 8$ (corresponding to a success probability of 1) is possible, as Alice can perfectly encode her four possible inputs into a single qubit using the dense-coding protocol. To make the task nontrivial, we add the following modification. We assume that Alice has a fifth possible choice of input $x = 5$ and Bob has a third input $y = 3$. This additional input of Alice can be thought of as a special flagged input (e.g., one that communicates a very important or urgent matter) that must be unambiguously identified by Bob whenever he decides on $y = 3$. This can be represented by adding the following constraints to our task:

$$E_{13} = E_{23} = E_{33} = E_{43} = -E_{53} = 1, \qquad (7)$$

i.e., when Bob uses input $y = 3$, he must necessarily obtain output $b = 1$ if $x = 1, 2, 3, 4$ and $b = -1$ if $x = 5$, allowing him to identify perfectly whether or not $x = 5$ has been sent.

In summary, our scenario corresponds to $n_X = 5$, $n_Y = 3$, $n_B = 2$ and we are interested in the maximal value of Eq. (5) subject to the constraints Eq. (7) when Alice communicates a quantum system to Bob of dimension $d = 2$.

Clearly, we cannot achieve $W_{\text{RAC}} = 8$ while respecting the constraint given in Eq. (7), as this would imply that Bob can perfectly guess the five inputs of Alice, i.e., that Alice can communicate to Bob $\log_2(5)$ bits, while we recall that an EA qubit only can carry at most 2 bits of information.

A strategy directly based on the dense-coding protocol can achieve a value $W_{\text{RAC}} = 6$. Indeed, it amounts to a strategy where two classical bits are sent from Alice to Bob. But since the input $x = 5$ must be perfectly discriminated from the inputs $x = 1, \ldots, 4$, this means that effectively Alice encodes the four inputs $x = 1, \ldots, 4$ using a classical trit. The best value of the $2 \to 1$ RAC function given in Eq. (5) when communicating a trit is known to

be 6 [46]. We show in the next subsection that there are strategies using a two-qubit entangled state that are more effective than the dense-coding protocol and in the following one that strategies based on two-ququart entanglement are even better.

B. Strategies based on two-dimensional entanglement

Consider the following simple strategy for evaluating W_{RAC} under the constraint given in Eq. (7) when the entanglement is restricted to a two-qubit state. The intuition stems directly from the quantum dense-coding protocol. Let Alice and Bob share the maximally entangled state given in Eq. (4) and let Alice, on her share of the state, apply the unitaries $[(\mathbb{1} - i\sigma_x)/\sqrt{2}, \mathbb{1}, \sigma_x, \sigma_y, \sigma_z]$ for inputs $x = 1, 2, 3, 4, 5$, respectively. She then communicates the transformed qubit to Bob. It is immediate that the states τ_{CB}^x for $x = 1, \ldots, 4$ live in the subspace $\{(|00\rangle + |11\rangle)/\sqrt{2}, (|01\rangle \pm |10\rangle)/\sqrt{2}\}$, while $|\tau_{CB}^5\rangle = (|00\rangle - |11\rangle)/\sqrt{2}$ is in the orthogonal complement. Thus the input $x = 5$ can be completely discriminated from the other inputs using an appropriate measurement for $y = 3$ and the constraint given in Eq. (7) is satisfied. Replacing $E_{xy} = \text{Tr}\left(\tau_{CB}^x M_y\right)$ in Eq. (5), where $M_y = M_{1|y} - M_{-1|y}$ is the observable associated with Bob's input y, we have

$$W_{\text{RAC}} = \text{Tr}\big[(\tau_{CB}^1 + \tau_{CB}^2 - \tau_{CB}^3 - \tau_{CB}^4)M_1\big]$$
$$+ \text{Tr}\big[(\tau_{CB}^1 - \tau_{CB}^2 + \tau_{CB}^3 - \tau_{CB}^4)M_2\big], \quad (8)$$

which is maximized when the ± 1 eigenspace of M_y is the ± 1 eigenspace of the combination of states appearing in the traces. This leads to

$$W_{\text{RAC}} = \text{Tr}\big(|\tau_{CB}^1 + \tau_{CB}^2 - \tau_{CB}^3 - \tau_{CB}^4|\big)$$
$$+ \text{Tr}\big(|\tau_{CB}^1 - \tau_{CB}^2 + \tau_{CB}^3 - \tau_{CB}^4|\big)$$
$$= 2(1 + \sqrt{5})$$
$$\approx 6.47 \quad (9)$$

for the specific states chosen above. This strategy thus makes a better use of the shared entanglement than one directly based on the dense-coding protocol.

It turns out that no larger value of W_{RAC} is possible by means of qubit communication assisted by two-qubit entanglement. To prove this, note that the states τ_{CB}^x in Bob's possession are four dimensional, since $\mathcal{H}_C \simeq \mathbb{C}^2$ (Alice communicates a qubit) and $\mathcal{H}_B \simeq \mathbb{C}^2$ (we assume that the shared entanglement is of local dimension two). These states actually occupy a subset of the total four-dimensional Hilbert space, since they must satisfy the condition given in Eq. (7). Let us relax this condition and consider the more generous situation where the states τ_{CB}^x live in an unconstrained four-dimensional space. This does

not decrease the largest possible value of W_{RAC} and it simplifies the analysis of the problem. The constraint given in Eq. (7) implies that Alice's first four states must be confined to a three-dimensional Hilbert space orthogonal to her fifth state. This reduces the problem to one of evaluating the largest value of the RAC function W_{RAC} when the four relevant states ($x \in \{1, \ldots, 4\}$) are encoded in a qutrit. This problem has been addressed in previous literature [14,47], where it has been shown that the optimal quantum implementation achieves the value given in Eq. (9). Actually, the strategy that we describe above is a straightforward reformulation of this optimal qutrit strategy to our EA qubit scenario.

C. Strategy based on four-dimensional entanglement

We now show that qubit communication assisted by higher-dimensional entanglement can further improve the value of W_{RAC}. Specifically, we show that a value of W_{RAC} larger than that in Eq. (9) is possible if Alice and Bob share two copies of the maximally entangled two-qubit state: $|\phi\rangle_{AB} = |\phi_{\max}\rangle_{A_1 B_1} \otimes |\phi_{\max}\rangle_{A_2 B_2}$. Consequently, the states held by Bob after Alice's communication are of dimension eight, corresponding to a qubit system (the communication) and the ququart system (Bob's share of $|\phi\rangle_{AB}$).

Alice's strategy consists in applying a two-qubit unitary U_x on her systems $A_1 A_2$, binning the first qubit A_1, and sending the second qubit A_2 to Bob. The channel that she implements is thus given by

$$(10)$$
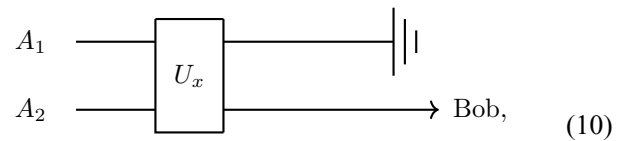
where the unitary operations are given by

$$U_1 = \mathbb{1} \otimes \mathbb{1}, \quad (11)$$
$$U_2 = \text{CNOT}_1 \, \text{CNOT}_2, \quad (12)$$
$$U_3 = \mathbb{1} \otimes \sigma_x \, \text{CNOT}_1 \, \text{CNOT}_2, \quad (13)$$
$$U_4 = \mathbb{1} \otimes \sigma_z, \quad (14)$$
$$U_5 = \mathbb{1} \otimes \sigma_z \sigma_x \, \text{CNOT}_2, \quad (15)$$

where CNOT_i is the controlled-NOT gate with the control on the ith qubit.

It can be checked that the total states τ_{CB}^x Bob measures in his laboratory are then rank-two states of the form

$$\tau_{CB}^x = \frac{1}{2}\big(|\psi_x\rangle\langle\psi_x| + |\varphi_x\rangle\langle\varphi_x|\big), \quad (16)$$

where the states $|\psi_x\rangle$ and $|\phi_x\rangle$ are readily computed from the unitaries given above. In particular, one finds that $|\psi_5\rangle$

and $|\phi_5\rangle$ are orthogonal to all other states and thus that the constraint given in Eq. (7) is satisfied through a proper choice of measurement for $y = 3$. The optimization of Bob's measurements for $y = 1, 2$ can be performed as in the previous subsection and, replacing the specific states obtained from the unitaries Eqs. (11)–(14) in Eq. (9), we obtain

$$W = 2(2 + \sqrt{2}) \approx 6.83, \qquad (17)$$

which exceeds the bound $W_{\text{RAC}} \leq 6.47$ for qubit communication assisted by two-qubit entanglement.

In summary, we show in this section that in EA d-dimensional quantum communication protocols, we cannot restrict the entanglement to be of local dimension d. We establish a similar result for the case of EA classical communication in Ref. [35]. Whether some finite upper bound on the entanglement dimension can generally be assumed is an interesting question not resolved here. The analogy with the usual Bell scenario would suggest a negative answer [48].

IV. SEMIDEFINITE PROGRAMS FOR CORRELATIONS IN ENTANGLEMENT-ASSISTED d-DIMENSIONAL COMMUNICATION

We now describe how to characterize, through sequences of SDP approximations, the set of correlations achievable from d-dimensional quantum or classical communication. We consider both inner and outer characterizations that approximate the quantum set from the inside and the outside.

A. Inner characterization through seesaw iterations

In Definition 1, the correlations $p(b|x, y)$ are expressed as the result of a measurement performed by Bob on a state τ_{CB}^x resulting from Alice's application of a CPTP map on her part of an entangled state shared with Bob. This representation can be simplified using state-channel duality [49,50]. Specifically, by exploiting the isomorphism between CPTP maps and quantum states, we may represent the total state τ_{CB}^x as a (generally mixed) bipartite state in $L(\mathcal{H}_C \otimes \mathcal{H}_B)$ with the property that the marginal state on system B is independent of Alice's input x (no signaling): $\text{Tr}_C(\tau_{CB}^x) = \tau_B$ for all x. We thus have the following definition, which is equivalent to Definition 1.

Definition 1'. *We say that the correlations $p(b|x, y)$ can be reproduced by an EA d-dimensional quantum communication protocol if there exists*

(a) *A bipartite entangled state $\tau_{CB}^x \in L(\mathcal{H}_C \otimes \mathcal{H}_B)$, where C is a physical system with d-dimensional Hilbert space $\mathcal{H}_C \simeq \mathbb{C}^d$ and B is a physical system with finite or separable Hilbert space $\mathcal{H}_B$, for*

each input x, where the states τ_{CB}^x all have the same marginal state τ_B:

$$\text{Tr}_C(\tau_{CB}^x) = \tau_B \quad \text{for all } x \qquad (18)$$

(b) *An n_B-outcome POVM $\{M_{b|y}\}_b$ on the joint systems C and B for each input y*

such that

$$p(b|x, y) = \text{Tr}(\tau_{CB}^x M_{b|y}). \qquad (19)$$

In the case of classical communication, it is easily seen that we can similarly use state-channel duality, and more specifically the Gisin-Hughston-Jozsa-Wootters theorem [51,52], to provide the following alternative to Definition 2.

Definition 2'. *We say that the correlations $p(b|x, y)$ can be reproduced by an EA d-dimensional classical communication protocol if there exists*

(a) *d subnormalized states $\{\tau_B^{c,x}\}_c$ in $L(\mathcal{H}_B)$, where B is a physical system with finite or separable Hilbert space $\mathcal{H}_B$, for each input x, where the total normalized state $\sum_{c=1}^d \tau_B^{c,x} = \tau_B$ is independent of x*

(b) *An n_B-outcome POVM $\{M_{b|y,c}\}_b$ on B for each input y and $c \in [d]$*

such that

$$p(b|x, y) = \sum_{c=1}^d \text{Tr}(\tau_B^{c,x} M_{b|y,c}). \qquad (20)$$

If we fix the dimension of $\mathcal{H}_B$ to some finite value $\dim(\mathcal{H}_B) = D$, it is straightforward from Definitions 1' and 2' that optimizing over the set of correlations $p(b|x, y)$ for fixed measurements is an SDP, as it amounts to optimizing over quantum states satisfying certain linear properties. Similarly, if we fix the states, the search for optimal measurements is also an SDP. Approximations to the set of correlations $p(b|x, y)$ can thus be obtained through a seesaw algorithm that repeatedly optimizes over the states for fixed measurements and then over the measurements for fixed states until some degree of convergence is achieved. This seesaw scheme represents an inner relaxation of the set of correlations for two reasons. First, though every solution that is obtained is a valid strategy, it is not necessarily the optimal one. Second, some finite value D on the dimension of $\mathcal{H}_B$ must be chosen. However, better solutions can, in principle, be obtained by increasing the dimension of D. If some general upper bounds on the dimension of the shared entanglement were to hold and be known, this could evidently be used to limit the size of the SDP.

More interestingly, we now provide SDP methods for obtaining outer relaxations that are valid irrespective of the amount of shared entanglement, i.e., without assumptions on dim $(\mathcal{H}_A)$ and dim $(\mathcal{H}_B)$.

B. Outer approximations through noncommutative polynomial optimization

To introduce our outer relaxation scheme, let us again consider Definition 1. Since we do not assume any bound on the dimension of $\mathcal{H}_A$ or $\mathcal{H}_B$, the CPTP maps $\$_x\colon L(\mathcal{H}_A) \to L(\mathcal{H}_C)$ appearing in Definition 1 can be seen as arising from unitary transformations on $\mathcal{H}_A \otimes \mathcal{H}_C$ and the POVMs $\{M_{b|y}\}_b$ can be assumed to be projective. That is, for some initial state $|\varphi\rangle_C$ in $\mathcal{H}_C$, we can reexpress the correlations as

$$p(b|x,y) = \langle \Psi | U_x^\dagger M_{b|y} U_x | \Psi \rangle, \qquad (21)$$

where $|\Psi\rangle = |\phi\rangle_{AB}|\varphi\rangle_C$, the $U_x = U_{AC}^x \otimes \mathbb{1}_B$ are unitaries that act nontrivially only on $\mathcal{H}_A \otimes \mathcal{H}_C$, and $M_{b|y} = \mathbb{1}_A \otimes M_{BC}^{b|y}$ are projectors that act nontrivially only on $\mathcal{H}_B \otimes \mathcal{H}_C$.

Let us now introduce the following (Kraus) operators, which induce a parametrization on the system C:

$$U_A^{x;j} = (\mathbb{1}_A \otimes \langle j |_C) U_x (\mathbb{1}_A \otimes |\varphi\rangle_C), \qquad (22)$$

$$M_B^{b|y;jk} = (\mathbb{1}_B \otimes \langle k|_C) M_{b|y} (\mathbb{1}_B \otimes |j\rangle_C). \qquad (23)$$

Inserting two resolutions of the identity on $\mathcal{H}_C$ into Eq. (21), we find that

$$p(b|x,y) = \sum_{j,k=0}^{d-1} \langle \Psi | U_x^\dagger |j\rangle \langle j | M_{b|y} |k\rangle \langle k | U_x | \Psi \rangle \qquad (24)$$

$$= \sum_{j,k=0}^{d-1} \langle \phi | U_{x;j}^\dagger U_{x;k} \otimes M_{b|y;jk} | \phi \rangle, \qquad (25)$$

which now involves only subsystems A and B, i.e., the shared state $|\phi\rangle$, the (Kraus) operators $U_{x;j}$ acting in $\mathcal{H}_A$, and the operators $M_{b|y;jk}$ acting in $\mathcal{H}_B$ (to simplify the notation, we drop the subsystem superscripts from the states and operators).

One can verify that the unitary conditions $U_x^\dagger U_x = \mathbb{1}_{AC}$ translate to the operator constraints

$$\sum_{k=0}^{d-1} U_{x;k}^\dagger U_{x;k} = \mathbb{1}_A, \qquad (26)$$

while the mathematical properties $\sum_b M_{b|y} = \mathbb{1}_{BC}$ and $M_{b|y}^\dagger = M_{b|y}$, $M_{b|y} M_{b'|y} = \delta_{b,b'} M_{b|y}$ of the projectors are

equivalent to

$$\sum_b M_{b|y;jk} = \delta_{jk} \mathbb{1},$$

$$M_{b|y;kj}^\dagger = M_{b|y;jk}, \qquad (27)$$

$$\sum_{k=0}^{d-1} M_{b|y;jk} M_{b'|y;kl} = \delta_{bb'} M_{b|y;jl}.$$

The problem of determining whether given correlations $p(b|x,y)$ can be reproduced through EA d-dimensional quantum communication, or finding the maximal value of a linear functional of the correlations $p(b|x,y)$, thus amounts to optimizing over a state $|\phi\rangle$ and (non-Hermitian) operators $U_{x,j}$, $U_{x,j}^\dagger$, $M_{b|y;jk}$, satisfying the constraints given in Eqs. (26) and (27) such that Eq. (25) holds. Without the subsystem restriction and the tensor product appearing in Eq. (25), that would be a typical instance of noncommutative polynomial optimization [36], to which the Navascués-Pironio-Acín (NPA) hierarchy of SDP relaxations [53,54] could be directly applied. As usual, one can relax the subsystem structure and the tensor product using commutation relations instead. That is, one can assume that all the operators $U_{x,j}$, $U_{x,j}^\dagger$, $M_{b|y;jk}$, act on the same Hilbert space, but satisfy

$$[U_{x;j}, M_{b|y;jk}] = 0, \qquad [U_{x;j}^\dagger, M_{b|y;jk}] = 0. \qquad (28)$$

Physically, this amounts to considering a *field-theoretic* variant of our prepare-and-measure scenario. The NPA hierarchy can now be applied directly. It provides an SDP relaxation hierarchy that represents an outer relaxation of the original tensor-product variant of our problem, that converges asymptotically to the field-theoretic variant, and that returns the original tensor-product variant when rank optimality conditions are satisfied [36,54].

Note that the scheme that we introduce here can be seen as a hybrid scheme, where the dimension-free subsystems A and B are accounted for *à la* NPA, while the subsystem C, the dimension of which is fixed, is explicitly parametrized. In particular, if we impose the additional constraints that all the operators on subsystems A and B commute between themselves (corresponding to a situation where the devices do not share any prior entanglement but possibly only classical correlations), we recover a Lasserre-type SDP hierarchy [55] applied to an explicit parametrization of Alice's preparations of and Bob's measurement on system C.

Finally, the case of EA classical communication can be seen as a subcase of the general quantum communication by imposing additional constraints on Alice's operations forcing the output system C to be in a diagonal state $\sum_{j=0}^{d-1} p(j|x)|j\rangle\langle j|_C$ irrespective of the input state $|\phi\rangle_{AB}|\varphi\rangle_C$. Alternatively and equivalently, one can directly

start from Definition 2. As we mentioned below that definition, the correlations in that scenario can be seen as the marginal correlations (obtained by summing over c) in a relaxed Bell scenario where the measurement performed on Bob's side depends not only on his input y but also on the communicated output c of Alice's measurement. Such relaxations of the usual Bell scenarios have been considered in Refs. [56–58]. Similarly to the observation made in Ref. [58] for the slightly different Instrumental scenario, one can then directly use the NPA hierarchy for Bell nonlocal correlations [53,54] in order to bound the correlations in our case. Indeed, it is immediate from Eq. (3) that the correlations $p(b|x,y)$ are a linear combination of standard Bell correlations where Bob has $n_Y \times d$ measurements labeled by inputs $y' = (y,c)$ and thus they can be viewed as linear combinations of entries of the moment matrices of the Bell-NPA hierarchy.

C. Outer approximations through information-restricted correlations

The NPA relaxations that we introduce above involve $2n_X d + n_B n_Y d^2$ operators in the case of quantum communication and $n_X d + n_B n_Y d$ [59] operators in the case of classical communication. The size of the corresponding SDP is determined by the number of such operators and grows rapidly as one increases the order, with the number of such operators. In practice, these SDPs cannot be used to characterize EA communication scenarios with more than a few inputs or outputs without excessive computational resources.

For this reason, we propose an entirely different approach that applies equally well to both classical and quantum communication. It is based on two relaxations of the problem. First, we relax the (postcommunication) state space of Bob to a state space characterized by its information content [37]. Second, we use semidefinite relaxations of the set of informationally restricted correlations [38] to efficiently bound the correlations from EA communication. We now proceed to outline this approach.

Recently, a framework has been developed for studying the correlations $p(b|x,y) = \mathrm{Tr}\left(\rho_x M_{b|y}\right)$ in prepare-and-measure experiments when the only assumption is that the *information* relayed about x through the states ρ_x is restricted [37,38]. This information restriction is quantified through a bound on the guessing probability

$$P_g = \max_{\{N_z\}} \sum_x p_x \, \mathrm{Tr}\left(\rho_x N_x\right),\qquad(29)$$

which expresses how well the input x can be guessed on average when performing an ideal measurement $\{N_z\}_z$ on the states ρ_x if they are given with prior probabilities p_x. This restriction can equivalently be expressed in terms of

the information quantity

$$\mathcal{I} \equiv -\log_2\left(\max_x p_x\right) + \log_2 P_g,\qquad(30)$$

which quantifies in entropic terms the information that is gained when given the ensemble $\{p_x, \rho_x\}$ as compared to when the ensemble is not given (in which case the best guess of x is its most likely value and this guess is thus correct with probability $\max_x p_x$). We refer the reader to Ref. [38] for further details on informationally restricted correlations.

An important feature is that no assumption is made in Ref. [38] on how the states ρ_x that Bob eventually receives and measures are physically prepared: they may leverage shared randomness, entanglement, high-dimensional systems, etc. The only thing that matters is the bound on the information quantity Eq. (30). Thus if we can find a bound on the information conveyed by the states $\rho_x = \tau_{CB}^x$ in Eq. (2), we can apply the methods of Ref. [38] to our setting.

In the case of classical communication, since the dimension of the message is d, we expect the bound $\mathcal{I} \leq \log d$ bits to be valid since, by no signaling, shared entanglement should not help Alice communicate the value of x to Bob. In the case of quantum dimension, we would instead expect a bound of $\mathcal{I} \leq 2 \log d$ bits, since shared entanglement can double the capacity of quantum communication through dense coding. Indeed, we now prove that this intuition is correct.

More generally, we express a bound on $\mathcal{I}$ that depends on how well the entanglement shared between Alice and Bob is preserved by Alice's actions $\$_x$. For this, let k_x be the Schmidt number of the bipartite state τ_{CB}^x (i.e., the minimum Schmidt rank of the pure states in optimal ensemble realizing the density operator τ_{CB}^x) and let $k = \max_x k_x$ be the largest Schmidt number. The parameter k can be viewed as a measure of the entanglement content in the set of states τ_{CB}^x. It satisfies the bounds $1 \leq k \leq d$, where the lower limit corresponds to the case of classical communication, since the state τ_{CB}^x is a CQ state with no entanglement between system C and system B and the upper limit corresponds to the general case of quantum communication, where the bounds come from the fact that the local dimension of system C is at most d.

Proposition 1'. *Consider an EA communication protocol where the total states τ_{CB}^x of Bob after Alice's communication are characterized by a maximal Schmidt number $k = \max_x k_x$. Then,*

$$\mathcal{I} \leq \log k + \log d,\qquad(31)$$

where $\mathcal{I}$ is the quantity defined in Eqs. (30) and (29), and the above inequality is valid for any choice of the

prior probabilities p_x. In particular, we obtain the bound $\mathcal{I} \leq \log d$ in the case of classical communication and the bound $\mathcal{I} \leq 2 \log d$ in the case of general quantum communication.

We note that a related, somewhat more restricted, result appears in the independent work of Ref. [60]. We refer the reader to Appendix A for the proof.

Having introduced the connection to informationally restricted correlations and their SDP relaxation hierarchy, several remarks are in order. First, though the relaxation to information-restricted correlations sometimes gives tight bounds (see examples in the next section), it represents in general a strict relaxation of the EA communication correlation set. Indeed, there exist correlations that can be obtained by Alice sending to Bob (high-dimensional) states that carry no more than $\mathcal{I} \leq 1$ bit of information but that cannot be attained by the EA communication of a single bit (see example in the next section) [61]. The approach based on the NPA hierarchy inherits, in contrast, its nice converging properties and we thus expect that it will in general give better bounds at a sufficiently high order. However, in practice, when taking into account limited computer memory and time, the information-based SDP relaxation may sometimes be superior. The reason is that, as we pointed out earlier, the size of these SDP relaxations grows rapidly with the number of basic operators involved, which depend on a factor of order d^2 in the case of quantum communication and d in the case of classical communication. In contrast, the information-based SDP relaxation have a much smaller size, which is moreover independent of d. This provides an advantage for the later relaxation both for fixed dimension d when one increases the relaxation order and at fixed relaxation order when one increases the dimension d.

Finally, note that in a situation where no entanglement is preshared between Alice and Bob, the Schmidt number k satisfies $k = 1$ even in the case of quantum communication. Thus the bound $\mathcal{I} \leq \log d$ valid for EA d-dimensional classical communication is also valid for non-EA d-dimensional quantum communication. Thus the SDP relaxation hierarchy based on informationally restricted correlations does not distinguish these two sets of correlations. We come back to the relationship between these two sets in Sec. VI and see that in general they are distinct overlapping sets (in particular, the set of EA classical d-dimensional correlations is not contained in the set of non-EA quantum d-dimensional correlations and vice versa). Similarly, the bound $\mathcal{I} \leq 2 \log d$ valid for EA d-dimensional quantum communication is also valid for non-EA d^2-dimensional quantum communication and thus the SDP relaxation hierarchy based on informationally restricted correlations does not distinguish these two sets. Again, we discuss the relationship between these two sets in more detail in Sec. VI.

V. APPLICATION: REVISED CLASSICAL AND QUANTUM TESTS OF DIMENSION

We now apply the methods introduced in Sec. IV toward the task of device independently testing the dimension of a physical system (classical or quantum). Specifically, we consider two different tests of dimension that have been previously investigated, in both theory and experiment, and reexamine their analysis to account for the most general picture in which parties may share unlimited entanglement. Notably, in all cases that we consider, we obtain either optimal or close to optimal dimension witnesses.

A. The random access code

Let us begin with the dimension witness experimentally realized in Ref. [46]. It is based on the regular random access code [7] introduced at the beginning of Sec. III A, in which Alice has a choice among four possible inputs $x \in [4]$, while Bob has a binary input $y \in [2]$ and generates binary outcomes $b \in [2]$. We are interested in the success probability of this RAC, which can be expressed through the RAC correlation function W_{RAC} defined in Eqs. (5) and (6). When no entanglement is present, the following bounds on W_{RAC} for classical and quantum systems of dimension two, three, and four are known [46]:

$$W_{\mathrm{RAC}} \overset{C2}{\leq} 4 \overset{Q2}{\leq} 4\sqrt{2} \overset{C3}{\leq} 6 \overset{Q3}{\leq} 2\left(1 + \sqrt{5}\right) \overset{C4,\,Q4}{\leq} 8. \tag{32}$$

Note that for four-dimensional classical and quantum systems, Alice may simply send her input to Bob and thus one reaches the algebraically maximal value of $W_{\mathrm{RAC}} = 8$. Depending on which inequalities in the chain given in Eq. (32) are experimentally violated, one can certify that systems of certain minimal classical and quantum dimensions are produced.

Let us reexamine the problem in a fully device-independent setting in which Alice's and Bob's devices may share prior entanglement. First, it is clear that quantum dense coding allows Alice to send her entire input to Bob and thus reach the algebraically maximal value of $W_{\mathrm{RAC}} = 8$ using only EA qubit communication, i.e., the following bound is tight:

$$W_{\mathrm{RAC}} \overset{\mathrm{Ent\text{-}Q2}}{\leq} 8. \tag{33}$$

Therefore, when entanglement is allowed, it is no longer possible to certify three- and four-dimensional quantum communication using the RAC dimension witness W_{RAC}.

In the classical case, the reexamination is less trivial. In order to bound W_{RAC} for EA classical communication of dimensions two and three, we evaluate semidefinite relaxations based on both the NPA hierarchy [62] and the information-based SDP hierarchy [63] for both messages

of dimension $d = 2$ and $d = 3$. We obtain the same bounds with both approaches, namely

$$W_{\mathrm{RAC}} \overset{\mathrm{Ent\text{-}C2}}{\leq} 5.657 \overset{\mathrm{Ent\text{-}C3}}{\leq} 6.828. \qquad (34)$$

The first bound is tight (up to solver precision), since it is known that it can be saturated if Alice and Bob use the shared entanglement to maximally violate the Clauser-Horne-Shimony-Holt Bell inequality before communicating a two-dimensional classical system [29]. Moreover, we also find that the second bound is tight. To show this, we use the SDP seesaw routine described in Sec. IV to efficiently search for optimal EA classical communication strategies. This leads us to find an explicit strategy, involving a shared entangled state of local dimension $D = 4$, achieving $W_{\mathrm{RAC}} = 6.828$. These results show that in order to test classical dimension in the presence of entanglement, one must significantly revise the bounds in Eq. (32), which are valid only when entanglement is assumed to not be present in the experiment.

In order to also consider a nontrivial setting for EA quantum communication, let us return to the modified RAC considered in Sec. III A, where Alice and Bob are each supplied with one more input and asked to maximize Eq. (5) under the constraint Eq. (7). Rather than requiring these constraints to be exactly satisfied, we can instead incorporate them in a modified witness

$$W_{\mathrm{fRAC}} = \sum_{x=1}^{5} \sum_{y=1}^{3} c_{xy} E_{xy}, \qquad (35)$$

where the 5×3 coefficients c_{xy} are given by

$$c = \begin{pmatrix} 1 & 1 & \beta \\ 1 & -1 & \beta \\ -1 & 1 & \beta \\ -1 & -1 & \beta \\ 0 & 0 & -4\beta \end{pmatrix}, \qquad (36)$$

depending on some positive parameter β, which favors (when β is sufficiently large) strategies where the constraints given in Eq. (7) are satisfied. For concreteness, we use $\beta = 4$. The explicit qubit strategy using entanglement of local dimension four that we introduce in Sec. III C achieves a value $W_{\mathrm{fRAC}} = 6.828 + 8\beta = 38.8284$.

We evaluate the information-based SDP relaxation [64] for EA qubit communication and obtain

$$W_{\mathrm{fRAC}} \overset{\mathrm{Ent\text{-}Q2}}{\leq} 38.8284. \qquad (37)$$

This result is (up to solver precision) identical to that obtained using the explicit strategy of Sec. III C, showing that it is optimal. On the other hand, an EA qutrit

(allowing us to communicate two classical trits using dense coding) can reach the algebraic maximum $W_{\mathrm{fRAC}} = 8 + 8\beta = 40$. The modified witness Eq. (35) thus constitutes a proper qutrit witness, even in the presence of arbitrary entanglement.

B. The witness of Gallego *et al.*

Let us now consider another dimension witness, introduced in Ref. [4], different variants of which have been experimentally realized in Refs. [21,22,24].

In this scenario, Alice receives one of five possible inputs $x \in [5]$, while Bob receives one of four possible inputs $y \in [4]$ and produces binary outcomes $b \in [2]$. The witness, labeled W_5, is written in the correlation format of Eq. (5) with coefficients

$$c = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 0 \\ 1 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}. \qquad (38)$$

In a scenario without shared entanglement, the tight bounds on the witness for classical systems have been obtained in Ref. [4]:

$$W_5 \overset{\mathrm{C2}}{\leq} 8 \overset{\mathrm{C3}}{\leq} 10 \overset{\mathrm{C4}}{\leq} 12 \overset{\mathrm{C5}}{\leq} 14. \qquad (39)$$

In addition, using symmetrized semidefinite relaxations [34], we compute upper bounds on W_5 for dimensionally restricted quantum systems without shared entanglement. These bounds are tight, since we could saturate them numerically with explicit quantum strategies:

$$W_5 \overset{\mathrm{Q2}}{\leq} 8.828 \overset{\mathrm{Q3}}{\leq} 11.527 \overset{\mathrm{Q4}}{\leq} 13.036 \overset{\mathrm{Q5}}{\leq} 14. \qquad (40)$$

Hence, the witness W_5 enables the certification of systems of classical and quantum dimension of two, three, four, or five in scenarios without shared entanglement.

Let us reconsider this analysis for the situation in which entanglement may be shared between Alice and Bob. We first note that in the quantum case, the maximal algebraic value $W_5 = 14$ can be attained with EA qutrit communication, since a dense-coding protocol can be used to relay x to Bob; i.e., the following tight bound holds:

$$W_5 \overset{\mathrm{Ent\text{-}Q3}}{\leq} 14. \qquad (41)$$

For classical communication of dimension two, three, and four as well as for quantum communication of dimension two, we reanalyze the classical bounds given in Eq. (39) and the qubit bound given in Eq. (40) in the presence of shared entanglement.

We start by considering explicit classical and quantum communication strategies based on sharing two copies of the maximally entangled two-qubit state. Using the seesaw routine of Sec. IV, we find explicit strategies achieving $W_5 = 9.034$ (Ent-C2), $W_5 = 11.515$ (Ent-C3), and $W_5 = 13.036$ (both Ent-C4 and Ent-Q2), violating the non-entanglement-assisted bounds for all considered resources.

Next, we compute upper bounds on W_5 for these entanglement-assisted resources using our new SPD methods. In the classical case, we again consider both the NPA hierarchy and the information-based SDP hierarchy. This time, however, the two methods return different results. The best bounds we obtained are the following:

$$W_5 \overset{\text{Ent-C2}}{\leq} 9.034^{\text{npa}} \overset{\text{Ent-C3}}{\leq} 11.563^{\text{info}} \overset{\text{Ent-C4}}{\leq} 13.095^{\text{info}},$$
(42)

where npa indicates that the result is obtained with the NPA SDP relaxation [65] and info indicates that the result is obtained with the information-based SDP relaxation [66]. Thus the lower and upper bounds nearly match: their ratios are $> 99.9\%$, 99.5%, 99.5%, and 99.5%, respectively. Thus, we find the NPA SDP relaxation performs better for the smaller problem ($d = 2$) but that the information-based SDP relaxation becomes advantageous for the somewhat larger problem ($d = 3, 4$). Furthermore, the bound for $d = 2$ allows us to prove that the information relaxation of EA classical communication is, generally, not tight. Indeed, by numerical search, we find explicit strategies from quantum states carrying at most $\mathcal{I} = 1$ bit of information, which achieves $W_5 = 9.054$. Thus the information-based SDP relaxation, even if implemented at an arbitrary high order, cannot return an upper bound smaller than $W_5 = 9.054$. But this exceeds the upper bound Eq. (42) on EA classical communication for $d = 2$ found using NPA.

For the case of EA qubit communication, the relevant information-based SDP relaxation is identical to that considered for EA quart communication. Therefore, the following quantum dimension witness is immediately obtained:

$$W_5 \overset{\text{Ent-Q2}}{\leq} 13.095.$$
(43)

A quantum system of minimal dimension three can be certified by violating this inequality. For comparison, solving the NPA relaxation for EA quantum communication for the same problem at level 2 of the hierarchy, we recover only the trivial algebraic bound $W_5 \lesssim 14$ after more than 40 h of computing time.

To summarize, we emphasize that the bounds given in Eqs. (39) and (40) are completely revised, both in the classical and quantum case, in a fully device-independent setting where entanglement is permitted in the experiment.

VI. QUANTUM COMMUNICATION VERSUS EA CLASSICAL COMMUNICATION

A (non-EA) qubit and a EA bit represent two different ways of employing quantum resources to generate correlations in a prepare-and-measure setting, which in both cases cannot be used to communicate more than one bit of information on Alice's input (in particular, the use of the information-based SDP hierarchy leads to the same relaxations of both sets). It is natural to ask how these resources compare and, in particular, if one is more powerful than the other.

A. EA bits can outperform qubits

The comparison of qubits and EA classical bits has already received substantial research attention. It has been proven in Ref. [39] that when Bob has binary outcomes, all correlations obtained by communicating a qubit can be simulated by communicating an EA bit [67].

By combining the results of Refs. [8,32], it follows that this resource inequality is strict. Reference [32] shows that EA classical bits achieve a winning probability of $p_{\text{win}} = 3/4$ four-bit RAC with binary communication, while Ref. [8] shows that non-EA qubits must satisfy $p_{\text{win}} < 3/4$. However, the noise tolerance of this advantage is presently restricted only to numerical evidence [8].

Our results from Sec. V B in fact prove a noise-robust gap between the correlations obtained from non-EA qubits and EA classical bits. Specifically, in the former case, we find that the witness obeys $W_5 \leq 8.828$, while in the latter case, it can achieve $W_5 = 9.034$. This enables experimental certification of the advantage of EA classical communication, which tolerates a substantial amount of noise.

B. Qudits can outperform EA classical dits

A more interesting situation is encountered when one goes beyond binary outcomes for Bob. Several different works [26,40–42] hint that the above situation can be reversed, i.e., that non-EA qudit communication can outperform EA classical dit communication. However, all these works consider a certain subclass of EA classical dit strategies, which may not always do justice to the full power of EA classical communication [68]. We now proceed to employ the general tools developed in Sec. IV to prove that non-EA qudit communication can outperform completely general EA classical dit communication.

We consider the scenario of Ref. [40], which is a higher-dimensional version of the previously considered RAC. In this task, Alice has nine possible inputs $x \in [9]$, represented by two trits $x_1, x_2 \in \{0, 1, 2\}$. Bob has an input $y \in [2]$ and aims to guess Alice's yth input trit in his output $b \in [3]$. With uniformly distributed inputs, the average

success probability is

$$W = \frac{1}{18} \sum_{x_1,x_2=0}^{2} \sum_{y=1}^{2} p(b = x_y | x_1, x_2, y). \qquad (44)$$

It is shown in Ref. [9] that non-EA qutrit communication can achieve $W = \frac{1}{2}\left(1 + \frac{1}{\sqrt{3}}\right) \approx 0.788$ and in Ref. [40] that certain classes of EA trit communication protocols based on a natural Bell-inequality violation satisfy the bound $W \leq \frac{7}{9} \approx 0.778$.

We now employ our general methods to reexamine the analysis of EA trit communication without the additional assumption of restricting to a particular Bell-inequality test. First, we use the seesaw routine described in Sec. IV. Considering entanglement of local dimension $D = 3$, we recover the value $W = \frac{7}{9}$. However, by considering entanglement of local dimension $D = 9$, we are able to find an improved protocol that achieves $W = 0.784$. This shows that the EA classical communication protocol considered in Ref. [40] is not general enough.

This leads to the question of whether non-EA qutrits do actually outperform the most general EA trit protocols. We answer this in the positive by employing our information-based SDP relaxations to bound W for the latter case. To enable this computation on a standard desktop computer, we exploit the symmetries of the function given in Eq. (44) to reduce the number of variables in the final SDP matrix [69]. We find the bound

$$W \overset{\text{EA-C3}}{\leq} 0.787. \qquad (45)$$

This upper bound is likely to be only nearly optimal but even so it is strictly smaller than the qutrit protocol achieving $W = 0.788$. Thus, it proves that non-EA quantum communication can outperform fully general EA classical communication.

VII. CONCLUSIONS

In this work, we investigate the correlations that can be generated in prepare-and-measure experiments in which parties share entanglement and communicate either classical or quantum systems of a given dimension. We show that the strongest forms of quantum correlations require protocols that go beyond the paradigmatic quantum dense-coding protocol and we develop general methods for bounding the correlations that can be obtained in such experiments when an unlimited amount of entanglement is allowed. We apply this to introduce device-independent tests of the dimension of classical and quantum systems that make no assumption on the presence of entanglement between the involved devices and show how this warrants a reexamination of standard tests of dimension in which entanglement is assumed not be present in experiments.

We also apply the methods to investigate the relation between entanglement-assisted communication protocols and non-entanglement-assisted communication protocols.

Our work introduces the main conceptual and technical tools necessary to pave the way for a systematic investigation of entanglement-assisted communication in prepare-and-measure scenarios. It leaves open several natural questions and continuations. First, while the method for bounding correlations based on a relaxation to informationally restricted quantum correlations is relatively efficient computationally and, as we have seen, often leads to strong bounds, one cannot in general expect the bounds to be optimal. How can one overcome this limitation in both a conceptual and practical manner? Second, we show that the strongest correlations possible from EA qubit communication in general require high-dimensional entanglement [70]. How high does this dimension need to be? Do there exist correlations that can only be generated with qubit communication and infinite-dimensional entanglement? Third, our work motivates a comparison of different types of quantum resources in prepare-and-measure scenarios. We explore some of these in Sec. VI but there remain many other open questions. For instance, our results in Sec. III imply that there exist scenarios where EA qubit communication can outperform non-EA quaquart communication [compare Eqs. (17) with Eq. (9)] [71]. Is this a strict resource inequality or do there exist scenarios in which non-EA ququart communication can outperform EA qubit communication? Fourth, it is interesting to explore tests of classical and quantum dimension when entanglement is involved. Can one construct simple families of dimension witnesses, favorably based on binary measurements, that are valid for any dimension? Fifth, tests of physical dimension are primarily practically motivated tasks. This has led to several experiments (see, e.g., Refs. [21,22,24,46]) testing dimension in standard prepare-and-measure experiments (assuming no shared entanglement). However, as we show, the conclusions of such experiments are generally not valid when entanglement is introduced. It is interesting and relevant to consider experimental implementations of device-independent tests of both classical and quantum dimensions when no assumptions are made on the entanglement that can be shared between preparation and measurement devices. Finally, it would also be interesting to use our method to design and analyze the security of semi-device-independent quantum random-number generation and quantum key distribution protocols that do not make the assumption that the devices do not share prior entanglement.

The code that is used in the numerical analysis of this paper can be found on GitHub [72]. The repository contains scripts for the information hierarchy as well as the NPA hierarchy for entanglement-assisted classical communication. It also contains scripts for the heuristic search algorithms that we use to find lower bounds for

quantum communication, information-restricted communication, and entanglement-assisted classical communication, in addition to the optimal strategies achieving the lower bounds quoted in this paper.

APPENDIX A: PROOF OF PROPOSITION 1

To prove Proposition 1, we need the following lemma.

Lemma 1'. *Let ρ, σ be two positive semidefinite operators on a joint finite Hilbert space $\mathcal{H}_C \otimes \mathcal{H}_B$. Then,*

$$\mathrm{Tr}[\rho\sigma] \leq k\,\mathrm{Tr}[\rho_B \sigma_B], \tag{A1}$$

where k is the Schmidt number of ρ and $X_B = \mathrm{Tr}_C[X]$ denotes the partial trace.

Proof. Let us start by assuming that $\rho = |\phi\rangle\langle\phi|$ and $\sigma = |\psi\rangle\langle\psi|$ are rank one. We can then introduce Schmidt decompositions

$$|\phi\rangle = \sum_{i=1}^{k} \sqrt{p_i}|\alpha_i\rangle|\beta_i\rangle, \tag{A2}$$

$$|\psi\rangle = \sum_{j} \sqrt{q_j}|\alpha_j'\rangle|\beta_j'\rangle, \tag{A3}$$

where the sum over i runs at most over k values by assumption.

We have that $\mathrm{Tr}[\phi\psi] = |\langle\phi|\psi\rangle|^2$. Writing the inner product explicitly gives

$$|\langle\phi|\psi\rangle| = \left|\sum_{ij} \sqrt{p_i}\sqrt{q_j}\langle\alpha_i|\alpha_j'\rangle\langle\beta_i|\beta_j'\rangle\right|$$

$$\leq \sqrt{\sum_{ij} |\langle\alpha_i|\alpha_j'\rangle|^2}\sqrt{\sum_{ij} p_i q_j |\langle\beta_i|\beta_j'\rangle|^2}$$

$$\leq \sqrt{k}\sqrt{\mathrm{Tr}[\phi_B \psi_B]}. \tag{A4}$$

The second line follows from applying the Cauchy-Schwarz inequality $|\mathbf{a} \cdot \mathbf{b}| \leq \|\mathbf{a}\|\|\mathbf{b}\|$ to vectors of components

$$\mathbf{a} = \left(\langle\alpha_i|\alpha_j'\rangle^*\right), \tag{A5}$$

$$\mathbf{b} = \left(\sqrt{p_i}\sqrt{q_j}\langle\beta_i|\beta_j'\rangle\right). \tag{A6}$$

The third line follows by noting that $\sum_{ij} |\langle\alpha_i|\alpha_j'\rangle|^2 \leq k$, since the $|\alpha_j'\rangle$ form an orthonomal basis and the sum over i runs over at most k values. Equally is thus obtained when i runs over precisely k values. Hence,

$$\mathrm{Tr}[\phi\psi] \leq k\,\mathrm{Tr}[\phi_B \psi_B]. \tag{A7}$$

If ρ and σ are not rank one, we can decompose them as $\rho = \sum_i \phi_i$ and $\sigma = \sum_j \psi_j$, where the ϕ_i and ψ_j are rank one and, furthermore, the Schmidt rank of ϕ_i is at most k by assumption. Then, using that the relation Eq. (A7) is linear, we obtain

$$\mathrm{Tr}[\rho\sigma] = \sum_{ij} \mathrm{Tr}[\phi_i \psi_j]$$

$$\leq k \sum_{ij} \mathrm{Tr}[\phi_{iB} \psi_{jB}]$$

$$= k\,\mathrm{Tr}[\rho_B \sigma_B]. \tag{A8}$$

∎

Equipped with this, we can now prove a general bound on the guessing probability given in Eq. (29) for the specific states $\rho_x = \tau_{CB}^x$ in our EA scenario:

$$P_g = \max_{\{N_z\}} \sum_x p_x \mathrm{Tr}\left(\tau_{CB}^x N_x\right)$$

$$\leq k \max_{\{N_z\}} \sum_x p_x \mathrm{Tr}\left(\tau_B \tilde{N}^x\right)$$

$$\leq k\left(\max_x p_x\right)\max_{\{N_z\}} \mathrm{Tr}\left(\tau_B \sum_x \tilde{N}_x\right)$$

$$= k\left(\max_x p_x\right)\max_{\{N_z\}} \mathrm{Tr}\left[\tau_B\,\mathrm{Tr}_C\left(\mathbb{1}_C \otimes \mathbb{1}_B\right)\right]$$

$$= kd\left(\max_x p_x\right). \tag{A9}$$

In the second line, we use the inequality Eq. (A1), together with the fact that $\tau_B^x = \tau_B$ is independent of x, and introduce the notation $\tilde{N}_x = \mathrm{Tr}_C(N_x)$. In the fourth line, we use the completeness of the measurement $\{N_z\}$ and in the fifth line the fact that $\mathrm{Tr}_C \mathbb{1}_C = d$, since $\dim(\mathcal{H}_C) = d$. Inserting this bound into Eq. (30), we obtain Eq. (31).

We thus relax the problem of deciding whether $p(b|x,y)$ can be achieved by EA communication of a classical or quantum d-dimensional system to a problem of deciding whether the same correlations can be achieved by states carrying at most, respectively, $\log d$ or $2\log d$ bits of information. The latter problem is known to admit a hierarchy of increasingly precise semidefinite relaxations [38], which can thus also be applied to our original problem. We discuss the main features of this hierarchy in Appendix B.

The information bound given in Eq. (31) is valid for any choice of the prior probabilities $\{p_x\}$ and any such

choice defines a relaxation of the set of correlations achievable through EA d-dimensional communication. However, the choice of uniform priors, i.e., $p_x = 1/n_X$, is the optimal choice that results in the most constraining relaxation. Indeed, any bound of the form $\mathcal{I} \leq \alpha$ for arbitrary priors is necessarily implied by the bound $\mathcal{I}_{\text{uni}} \leq \alpha$ for uniform priors $p_x = 1/n_X$. To see this, simply note that

$$
\begin{aligned}
P_g^{\text{bias}} &= \max_{\{N_z\}} \sum_{x=1}^{n_X} p_x \, \text{Tr} \left(\rho_x N_x \right) \\
&\leq \left(\max_x p_x \right) \max_{\{N_z\}} \sum_{x=1}^{n_X} \text{Tr} \left(\rho_x N_x \right) \\
&= \left(\max_x p_x \right) n_X P_g^{\text{uni}}.
\end{aligned} \tag{A10}
$$

Consequently,

$$
\begin{aligned}
\mathcal{I} &\leq -\log \left(\max_x p_x \right) + \log \left[\left(\max_x p_x \right) n_X P_g^{\text{uni}} \right] \\
&= \log n_X + \log \left(P_g^{\text{uni}} \right) = \mathcal{I}_{\text{uni}} \leq \alpha.
\end{aligned} \tag{A11}
$$

APPENDIX B: SKETCH OF THE INFORMATION-BASED SDP HIERARCHY

Here, we sketch the hierarchy of semidefinite programs for bounding the set of informationally restricted quantum correlations, which we employ to efficiently (but, in general, not tightly) bound the set of correlations obtainable from classical or quantum communication in entanglement-assisted prepare-and-measure scenarios. This hierarchy has originally been introduced in Ref. [38] to investigate the concept of informationally restricted correlations. Notably, due to a connection between this concept and quantum contextuality, a modification of this hierarchy has also recently been proposed to bound the set of quantum correlations in contextuality experiments [73].

Given that Alice's input is sampled from a probability distribution p_x, the information carried by her communicated quantum ensemble is given by Eq. (30). This quantity is one to one with the so-called guessing probability P_g, defined in Eq. (29) as the performance of the best possible quantum protocol for minimal-error state discrimination of Alice's ensemble. Consider now that we are given a probability distribution $p(b|x,y)$ in a prepare-and-measure scenario and asked to decide whether $p(b|x,y)$ is compatible with some quantum model based on an information transmission corresponding to a fixed value of P_g (for given p_x). A hierarchy of increasingly precise necessary conditions for the existence of such a quantum model has been presented in Ref. [38]. Each condition takes the form of a semidefinite program. We now proceed to sketch the construction of these semidefinite relaxations.

Define a list of operators containing all the preparations and measurements in the relevant scenario:

$$
S = \{ \mathbb{1}, \sigma, \rho_1, \ldots, \rho_{n_X}, M_{1|1}, \ldots, M_{n_B|1}, \ldots, M_{n_B|n_Y} \}. \tag{B1}
$$

The measurements can, without loss of generality, be chosen as projective ($M_{b|y} M_{b'|y} = \delta_{b,b'} M_{b|y}$). Moreover, the list also includes the identity (of unknown dimension) and an auxiliary operator σ. By considering products of the elements of S (monomials), we can build a list, which we name $\mathcal{S}$. This list should, at the very least, contain all elements of S (products of length one). The addition of more monomials to this list corresponds to a more precise necessary condition for a quantum model. From the monomial list $\mathcal{S}$, we can now build a $|\mathcal{S}| \times |\mathcal{S}|$ matrix of moments, defined as

$$
\Gamma_{ij} = \text{Tr} \left(\mathcal{S}_i \mathcal{S}_j^\dagger \right). \tag{B2}
$$

Note that the quantum probabilities $p(b|x,y) = \text{Tr} \left(\rho_x M_{b|y} \right)$ appear as explicit entries in the moment matrix. By associating $\text{Tr} \left(\rho_x M_{b|y} \right)$ to the corresponding entry (i,j) in Γ, we may label the relevant entries as Γ_{bxy}. A quantum model is compatible with the positivity condition $\Gamma \geq 0$.

So far, no physically relevant constraint is placed on Γ. *A priori*, it may appear difficult to impose the constraint on the guessing probability, since in itself it corresponds to a semidefinite program. The key observation for resolving the apparent difficulty is that one may exploit the program dual to that corresponding to the guessing probability. Specifically, define $\sigma \geq p_x \rho_x \; \forall x$. Then,

$$
P_g = \max_{\{N_z\}} \sum_x p_x \, \text{Tr} \left(\rho_x N_x \right) \leq \max_{\{N_z\}} \sum_x \text{Tr} \left(\sigma N_x \right) = \text{Tr} \left(\sigma \right). \tag{B3}
$$

This is the reason why we include σ in the operator list S. In order to constrain the guessing probability, we can impose a bound on $\text{Tr} \left(\sigma \right)$, which appears as an explicit entry in Γ. We label that single entry as Γ_σ. However, in order to nontrivially impose this constraint, we must also account for the semidefinite conditions $\sigma \geq p_x \rho_x$ on the level of the semidefinite relaxation. To this end, we introduce a set of localizing matrices, defined as

$$
\tilde{\Gamma}_{ij}^{(x)} = \text{Tr} \left(\mathcal{R}_i \left(\sigma - p_x \rho_x \right) \mathcal{R}_j^\dagger \right), \tag{B4}
$$

where $\mathcal{R}$ is (in analogy with $\mathcal{S}$) a list of monomials built from products taken from the elements of S. Notably, one does not need to choose $\mathcal{R} = \mathcal{S}$ but it is favorable to choose $\mathcal{R}$ such that all entries in $\tilde{\Gamma}^{(x)}$ appear in Γ. Imposition of the positivity constraint $\tilde{\Gamma}^{(x)} \geq 0$ for all x nontrivially enforces the desired constraints.

Finally, it is known that the analysis of informationally restricted correlations cannot be restricted to pure quantum states without loss of generality [38]. This means that we do not wish to enforce $\rho_x^2 = \rho_x$ but, instead, the constraint $\rho_x \geq 0$ on the level of the semidefinite relaxation. To this end, we introduce another set of localizing matrices, defined as

$$\bar{\Gamma}_{ij}^{(x)} = \text{Tr}\left(\mathcal{T}_i \rho_x \mathcal{T}_j^\dagger\right), \tag{B5}$$

where $\mathcal{T}$ is (in analogy with $\mathcal{S}$ and $\mathcal{R}$) a list of monomials built from products taken from the elements of S. The positivity of the state is nontrivially imposed by the condition $\bar{\Gamma}^{(x)} \geq 0$.

Putting the above together, a necessary condition for the existence of a quantum model with guessing probability P_g (for given prior p_x) takes the form of the following semidefinite program:

Find $\{\Gamma, \tilde{\Gamma}^{(x)}, \bar{\Gamma}^{(x)}\}$ such that

$$\Gamma \geq 0, \quad \forall x: \tilde{\Gamma}^{(x)} \geq 0, \quad \forall x: \bar{\Gamma}^{(x)} \geq 0, \tag{B6}$$
$$\text{Tr}(\rho_x) = 1, \quad \Gamma_\sigma \leq P_g, \quad \Gamma_{bxy} = p(b|x,y).$$

For any given choice of monomial lists $\{\mathcal{S}, \mathcal{R}, \mathcal{T}\}$, the failure of this program implies the impossibility of a quantum model. Note that for the purposes of entanglement-assisted communication scenarios, we always choose $p_x = 1/n_X$ and $P_g = d/n_X$ (where d is the dimension of communication) when communication is classical. When communication is quantum, we choose $P_g = d^2/n_X$.

APPENDIX C: EA BITS ARE STRICTLY MORE POWERFUL THAN HYPERBITS

In Ref. [39], an equivalence is claimed between EA bit and hyperbit strategies. While it is true that any hyperbit strategy can be simulated by EA bits, the converse claim is incorrect, as we illustrate with an explicit counterexample.

We consider the dimension witness of Gallego *et al.* from Sec. V B. As discussed there, we find an explicit EA bit strategy achieving $W_5 \approx 9.034$, which we prove to be optimal. The correlations in a hyperbit model are given by the scalar products between unit vectors. Hence, finding the optimal value of a linear function of the correlations for a hyperbit strategy amounts to a search over Gram matrices, which can be cast as a single SDP [74]. Taking into account the possibility that Bob may use more complex strategies (e.g., where he probabilistically decides to discard Alice's message and he outputs a predetermined output), we find, following the methods of Ref. [74],

$$W_5 \overset{\text{hyperbit}}{\leq} 9, \tag{C1}$$

which is strictly smaller than the EA bit value.

The hyperbit construction given in Appendix A of Ref. [39] fails, because the probabilities for Bob to flip his bit, under [Eq. (A9) [39]], are not guaranteed to be positive. Taking our optimal EA bit strategy achieving $W_5 \approx 9.034$, we can verify that this is indeed the issue by attempting to transform it into a hyperbit strategy following the construction of Ref. [39]. As expected, the flipping probabilities are negative for most of Bob's inputs and Alice's messages. The explicit calculation can be found in two MATLAB files as ancillary files on the arXiv page of the present paper [72].

[1] M. Pawłowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Żukowski, Information causality as a physical principle, Nature **461**, 1101 (2009).

[2] G. Brassard, H. Buhrman, N. Linden, A. A. Méthot, A. Tapp, and F. Unger, Limit on Nonlocality in Any World in Which Communication Complexity is Not Trivial, Phys. Rev. Lett. **96**, 250401 (2006).

[3] S. Wehner, M. Christandl, and A. C. Doherty, A lower bound on the dimension of a quantum system given measured data, Phys. Rev. A **78**, 062112 (2008).

[4] R. Gallego, N. Brunner, C. Hadley, and A. Acín, Device-Independent Tests of Classical and Quantum Dimensions, Phys. Rev. Lett. **105**, 230501 (2010).

[5] N. Brunner, M. Navascués, and T. Vértesi, Dimension Witnesses and Quantum State Discrimination, Phys. Rev. Lett. **110**, 150501 (2013).

[6] J. I. de Vicente, Shared randomness and device-independent dimension witnessing, Phys. Rev. A **95**, 012340 (2017).

[7] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani, in *Proceedings of the 31st Annual ACM Symposium on Theory of Computing (STOC'99)* (ACM Press, New York, 1999), p. 376.

[8] A. Ambainis, D. Leung, L. Mancinska, and M. Ozols, Quantum random access codes with shared randomness, ArXiv:0810.2937.

[9] A. Tavakoli, A. Hameedi, B. Marques, and M. Bourennane, Quantum Random Access Codes Using Single d-Level Systems, Phys. Rev. Lett. **114**, 170502 (2015).

[10] H-W. Li, Z.-Q. Yin, Y.-C. Wu, X.-B. Zou, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Semi-device-independent random-number expansion without entanglement, Phys. Rev. A **84**, 034301 (2011).

[11] H-W. Li, M. Pawłowski, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, Semi-device-independent randomness certification using $n \to 1$ quantum random access codes, Phys. Rev. A **85**, 052308 (2012).

[12] M. Pawłowski, and N. Brunner, Semi-device-independent security of one-way quantum key distribution, Phys. Rev. A **84**, 010302(R) (2011).

[13] E. Woodhead, and S. Pironio, Secrecy in prepare-and-measure CHSH tests with a qubit bound, Phys. Rev. Lett. **115**, 150501 (2015).

[14] A. Tavakoli, J. Kaniewski, T. Vértesi, D. Rosset, and N. Brunner, Self-testing quantum states and measurements in

the prepare-and-measure scenario, Phys. Rev. A **98**, 062307 (2018).

[15] M. Farkas, and J. Kaniewski, Self-testing mutually unbiased bases in the prepare-and-measure scenario, Phys. Rev. A **99**, 032316 (2019).

[16] A. Tavakoli, M. Smania, T. Vértesi, N. Brunner, and M. Bourennane, Self-testing nonprojective quantum measurements in prepare-and-measure experiments, Science Advances **6**, 16 (2020).

[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] P. Mironowicz, and M. Pawłowski, Experimentally feasible semi-device-independent certification of four-outcome positive-operator-valued measurements, Phys. Rev. A **100**, 030301(R) (2019).

[19] A. Tavakoli, Semi-device-independent certification of independent quantum state and measurement devices, Phys. Rev. Lett. **125**, 150503 (2020).

[20] P. Trojek, C. Schmid, M. Bourennane, C. Brukner, M. Żukowski, and H. Weinfurter, Experimental quantum communication complexity, Phys. Rev. A **72**, 050305(R) (2005).

[21] J. Ahrens, P. Badziag, A. Cabello, and M. Bourennane, Experimental device-independent tests of classical and quantum dimensions, Nature Phys **8**, 592 (2012).

[22] M. Hendrych, R. Gallego, M. Mičuda, N. Brunner, A. Acín, and J. P. Torres, Experimental estimation of the dimension of classical and quantum systems, Nat. Phys. **8**, 588 (2012).

[23] S. Muhammad, A. Tavakoli, M. Kurant, M. Pawłowski, M. Żukowski, and M. Bourennane, Quantum Bidding in Bridge, Phys. Rev. X **4**, 021047 (2014).

[24] V. D'Ambrosio, F. Bisesto, F. Sciarrino, J. F. Barra, G. Lima, and A. Cabello, Device-Independent Certification of High-Dimensional Quantum Systems, Phys. Rev. Lett. **112**, 140503 (2014).

[25] M. Smania, A. M. Elhassan, A. Tavakoli, and M. Bourennane, Experimental quantum multiparty communication protocols, npj Quantum Inf. **2**, 16010 (2016).

[26] D. Martínez, A. Tavakoli, M. Casanova, G. Cañas, B. Marques, and G. Lima, High-Dimensional Quantum Communication Complexity beyond Strategies Based on Bell's Theorem, Phys. Rev. Lett. **121**, 150504 (2018).

[27] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem, IEEE Trans. Inf. Theory **48**, 2637 (2002).

[28] C. H. Bennett, and S. J. Wiesner, Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states, Phys. Rev. Lett. **69**, 2881 (1992).

[29] H. Buhrman, R. Cleve, and W. van Dam, Quantum entanglement and communication complexity, SIAM J. Comput. **30**, 1829 (2001).

[30] C. Brukner, T. Paterek, and M. Żukowski, Quantum communication complexity protocols based on higher-dimensional entangled systems, Int J of Quant Inf. **1**, 4 (2003).

[31] A. Tavakoli, and M. Żukowski, Higher-dimensional communication complexity problems: Classical protocols versus quantum ones based on Bell's theorem or

prepare-transmit-measure schemes, Phys. Rev. A **95**, 042305 (2017).

[32] M. Pawłowski, and M. Żukowski, Entanglement-assisted random access codes, Phys. Rev. A **81**, 042326 (2010).

[33] M. Navascués, and T. Vértesi, Bounding the Set of Finite Dimensional Quantum Correlations, Phys. Rev. Lett. **115**, 020501 (2015).

[34] A. Tavakoli, D. Rosset, and M.-O. Renou, Enabling Computation of Correlation Bounds for Finite-Dimensional Quantum Systems via Symmetrization, Phys. Rev. Lett. **122**, 070501 (2019).

[35] J. Pauwels, A. Tavakoli, E. Woodhead, and S. Pironio, Entanglement in prepare-and-measure scenarios: Many questions, a few answers (to be published).

[36] S. Pironio, M. Navascués, and A. Acín, Convergent Relaxations of Polynomial Optimization Problems with Noncommuting Variables, SIAM J. Optim. **20**, 2157 (2010).

[37] A. Tavakoli, E. Z. Cruzeiro, J. B. Brask, N. Gisin, and N. Brunner, Informationally restricted quantum correlations, Quantum **4**, 332 (2020).

[38] A. Tavakoli, E. Zambrini Cruzeiro, E. Woodhead, and S. Pironio, Informationally restricted correlation: A general framework for classical and quantum systems, ArXiv:2007.16145 (2020).

[39] M. Pawłowski, and A. Winter, "Hyperbits": The information quasiparticles, Phys. Rev. A **85**, 022331 (2012).

[40] A. Tavakoli, B. Marques, M. Pawłowski, and M. Bourennane, Spatial versus sequential correlations for random access coding, Phys. Rev. A **93**, 032336 (2016).

[41] A. Hameedi, D. Saha, P. Mironowicz, M. Pawłowski, and M. Bourennane, Complementarity between entanglement-assisted and quantum distributed random access code, Phys. Rev. A **95**, 052345 (2017).

[42] A. Tavakoli, M. Pawłowski, M. Żukowski, and M. Bourennane, Dimensional discontinuity in quantum communication complexity at dimension seven, Phys. Rev. A **95**, 020302(R) (2017).

[43] The requirement that the shared state be pure is not restrictive because we do not limit the dimension of the Hilbert space $\mathcal{H}_B$. This means that, even if the physical state is mixed, it can always be purified, i.e., we can understand every mixed state $\rho \in \mathcal{H}_A \otimes \mathcal{H}_{B_0}$ as the partial trace by Bob of a pure state $|\phi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_{B_0 B_1}$.

[44] A Hilbert space is separable if and only if it admits a countable orthonormal basis.

[45] A. S. Holevo, Bounds for the quantity of information transmitted by a quantum communication channel, Probl. Peredachi Inf. **9**, 3 (1973).

[46] J. Ahrens, P. Badziag, M. Pawłowski, M. Żukowski, and M. Bourennane, Experimental Tests of Classical and Quantum Dimensions, Phys. Rev. Lett. **112**, 140401 (2014).

[47] M. Navascués, A. Feix, M. Araújo, and T. Vértesi, Characterizing finite-dimensional quantum behavior, Phys. Rev. A **92**, 042117 (2015).

[48] A. Coladangelo, and J. Stark, An inherently infinite-dimensional quantum correlation, Nat. Commun. **11**, 3335 (2020).

[49] M. M. Wilde, *Quantum Information Theory* (Cambridge University Press, Cambridge, 2013).

[50] This simplification has also recently been noted in Ref. [60].

[51] N. Gisin, Stochastic quantum dynamics and relativity, Helv. Phys. Acta **62**, 363 (1989).

[52] L. P. Hughston, R. Jozsa, and W. K. Wootters, A complete classification of quantum ensembles having a given density matrix, Phys. Lett. A **183**, 14 (1993).

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

[54] M. Navascués, S. Pironio, and A. Acín, A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations, New J. Phys. **10**, 073013 (2008).

[55] J. B. Lasserre, Global optimization with polynomials and the problem of moments, SIAM J. Optim. **11**, 796 (2001).

[56] R. Chaves, R. Kueng, J. B. Brask, and D. Gross, Unifying Framework for Relaxations of the Causal Assumptions in Bell's Theorem, Phys. Rev. Lett. **114**, 140403 (2015).

[57] J. B. Brask, and R. Chaves, Bell scenarios with communication, J. Phys. A: Math. Theor. **50**, 094001 (2017).

[58] T. Van Himbeeck, J. B. Brask, S. Pironio, R. Ramanathan, A. B. Sainz, and E. Wolfe, Quantum violations in the instrumental scenario and their relations to the Bell scenario, Quantum **3**, 186 (2019).

[59] This can be seen either directly from Eq. (3) or by taking the classical limit of the quantum SDP introduced above (Sec. IV B), where the assumption of classicality is encoded in the fact that Bob's POVMs $M_{b|y}$ are diagonal in a basis for $\mathcal{H}_C$.

[60] G. Moreno, R. Nery, C. de Gois, R. Rabelo, and R. Chaves, Semi-device-independent certification of entanglement in superdense coding, Phys. Rev. A **103**, 022426 (2021).

[61] Similarly, we see no reason to expect that the relaxation to information would be tight in the case of EA *quantum* communication. It is, however, much harder to find an explicit example, because of the high computational requirements of the NPA-type hierarchy for EA quantum communication.

[62] For $d = 2$, we use level 1 and for $d = 3$, we use level $1 + AB + AA$.

[63] For $d = 2$, the moment matrix is size 39 and the localizing matrix is size 8. For $d = 3$, the sizes are 87 and 20, respectively.

[64] Moment matrix size 866. Localizing moment matrix size 127.

[65] With NPA, we obtain 9.034, 11.568, and 13.225, respectively. For $d = 2, 3$, we use the second level. For $d = 4$, we restrict to level $1 + AB$ due to the increasingly demanding computation.

[66] With information relaxations, we obtain 9.081, 11.563, and 13.095, respectively, using moment matrices and localizing matrices of size 498 and 91, respectively.

[67] It is further claimed in Ref. [39] that EA bit strategies are equivalent to *hyperbit* strategies. However, while it is true that EA bit strategies can simulate any hyperbit strategy, the converse is wrong. Using the techniques introduced in the present paper, we find explicit EA bit correlations that cannot be simulated by hyperbit strategies. See Appendix C for details.

[68] A. Tavakoli, M. Żukowski, and Č. Brukner, Does violation of a Bell inequality always imply quantum advantage in a communication complexity problem?, Quantum **4**, 316 (2020).

[69] The moment matrix is size 1585 and originally features over 5×10^5 variables. The use of symmetries reduces it to only about 5×10^3 variables.

[70] This is true even if shared randomness is considered a free resource, as we prove this result using a linear dimension witness for which extremal strategies are always optimal.

[71] This is in contrast to the case of classical communication, where it has been shown that non-EA quarts (with shared randomness) can always be used to simulate bits assisted by any shared maximally entangled state [75].

[72] https://github.com/jefpauwels/arXiv-2103.10748-Supplementary-MATLAB-codes.

[73] A. Tavakoli, E. Zambrini Cruzeiro, R. Uola, and A. A. Abbott, Bounding and simulating contextual correlations in quantum theory, PRX Quantum **2**, 020334 (2021).

[74] J. X. Lin, J. A. Formaggio, A. W. Harrow, and A. V. Natarajan, Quantum blackjack: Advantages offered by quantum strategies in communication-limited games, Phys. Rev. A **102**, 012425 (2020).

[75] P. E. Frankel and M. Weiner, On entanglement assistance to a noiseless classical channel, ArXiv:2103.08567 (2021).