Preparation contextuality as an essential feature underlying quantum communication advantage

Debashis Saha[1,2] and Anubhav Chaturvedi[1]
[1]*Institute of Theoretical Physics and Astrophysics, National Quantum Information Centre, Faculty of Mathematics, Physics and Informatics, University of Gdańsk, 80-952 Gdańsk, Poland*
[2]*Center for Theoretical Physics, Polish Academy of Sciences, Al. Lotników 32/46, 02-668 Warsaw, Poland*

(Received 7 August 2018; published 7 August 2019)

The study of ontology (hidden variables) provides for a vital ground on which significant nonclassical features of quantum theory are revealed. One such nonclassical ontic feature is preparation contextuality (PC) and advantage in oblivious communication tasks is one of its operational signatures. This article primarily pursues the ontic feature underlying quantum advantage in communication complexity (CC). We construct oblivious communication tasks tailored to given CC problems. We upper bound the classical success probability of these oblivious communication tasks, obtaining preparation noncontextual inequalities. We use the very states and measurements responsible for advantage in CC problems along with the orthogonal mixtures of these states to orchestrate an advantageous protocol for the associated oblivious communication tasks and the violation of the associated inequalities, thereby unveiling PC. To showcase the vitality of our results, we find a criterion for unbounded violation of these inequalities and demonstrate the same for two widely studied CC problems.

DOI: 10.1103/PhysRevA.100.022108

I. INTRODUCTION

Quantum resources coupled with ingenious quantum protocols have outshone their classical counterparts in a wide range of computation, communication, and information processing tasks. But, there is little insight into what makes quantum theory stand out. The theory-specific features such as superposition do not make insightful answers for they are cyclic in the sense that they refer back to the operational quantum formalism which was *a priori* responsible for the advantageous predictions. Therefore, any comprehensive approach to this question must arguably invoke a ground common to both classical and quantum theories, on which nonclassical features of the latter are unveiled. The study of hidden variables (ontology) provides for such a ground. Any ontological model that seeks to explain the predictions of operational quantum formalism must have certain nonclassical features [1,2]. Introduced in [3], the ontic feature of preparation contextuality (PC) discards any preparation noncontextual (PNC) models as viable ontological descriptions of an operational theory. An ontological model is said to be PNC if it assigns identical ontic distributions to operationally indistinguishable preparations [3]. Quantum theory manifests preparation contextuality (PC), i.e., it postulates certain operationally indistinguishable preparations which must have nonidentical underlying ontic distributions. Quantum protocols siphon this ontological distinguishability to an advantage in oblivious communication (OC) tasks, i.e., *any* advantage in OC tasks witnesses PC [4–7].

One of the predominant manifestations of quantum communication advantage is captured in communication complexity (CC). The notion of CC, introduced in the seminal paper [8], is an important aspect of complexity theory, which quantifies the amount of communication required for distributed computation. Apart from mainstream applications in algorithmic mechanism design, game theory, and cryptography, lower bounds in CC can be used to prove lower bounds in decision tree complexity, data structures, space-time tradeoffs for Turing machines, and more [9]. Quantum resources and strategies have demonstrated supremacy in a multitude of CC problems [10–15]. In this article, we substantiate a fundamental link between quantum CC advantage and PC. Specifically, we establish that quantum advantage in CC manifests PC. We begin by constructing an OC task tailored to a given instance of the generic CC problem. We orchestrate advantageous quantum strategies for the constructed OC tasks based on advantageous (i) one-way prepare and measure quantum CC protocols, (ii) two-way multiround quantum CC protocols, and (iii) entanglement assisted classical communication CC protocols. These OC strategies utilize the same quantum setup responsible for advantage in the CC task. Specifically, we provide a family of PNC inequalities tailored to CC tasks and show that quantum CC advantage implies a violation of these inequalities, subject to certain conditions. Additionally, we obtain a criterion for unbounded violation of these PNC inequalities and demonstrate it for two widely studied CC problems with exponential quantum advantage. We present an alternative construction of the OC task and discuss the potential extension of our results to general probabilistic theories. Next, we use the machinery thus developed to provide a complete proof of the fact (originally stated in [6]) that violation of (spatial or temporal) Bell inequalities [16–18] implies an advantage in an associated OC task. Finally, we conclude with a discussion of the implications of this work.

II. PRIMITIVES

In this section, we lay down the framework we employ in our investigation. Specifically, we introduce the generic

formulations of CC problems and OC tasks, which form the key subjects of this article.

A. Communication complexity problem

We begin with briefly introducing the generic formulation of CC problem. A typical CC problem entails two parties Alice and Bob, with inputs $x \in [n_x]$, $y \in [n_y]$ (where $[n] = \{0, 1, \ldots, n-1\}$), respectively, distributed according to a prior probability distribution $p(x, y)$. Their task is to compute the value of a binary output bivariate function $f(x, y) : [n_x] \times [n_y] \to \{0, 1\}$ by exchanging messages. Without loss of generality, we assume that Bob guesses the value of $f(x, y)$ and his guess is stored in an output bit $z \in \{0, 1\}$. They achieve success with probability

$$p = \sum_{x,y} p(x, y)p(z = f(x, y)|x, y). \tag{1}$$

There are two interconvertible metrics to gauge their performance: (i) maximal achievable success probability ($p_{\mathcal{C}_d}$ for classical resources and $p_{\mathcal{Q}_d}$ for quantum resources) given a bounded amount of communication (bounded dimension d of the communicated system), and (ii) amount of communication [usually quantified in bits, denoted by $\mathcal{C}(f, p_S)$ or qubits, denoted by $\mathcal{Q}(f, p_S)$] required to achieve a specified probability of success (denoted by p_S). Quantum CC advantage implies $p_{\mathcal{Q}_d} > p_{\mathcal{C}_d}$ or alternatively $\mathcal{Q}(f, p_S) < \mathcal{C}(f, p_S)$.

B. Oblivious communication task

For this article, we need only invoke a subclass of general OC tasks (introduced in [5]) wherein Alice's (sender) input comprises of a pair $a = (a_1, a_2)$ with $a_1 \in [n_{a_1}]$, $a_2 \in [n_{a_2}]$. Bob (receiver) gets an input $b \in [n_b]$ and yields an output $c \in [n_c]$. The inputs are distributed according to a prior probability distribution $p(a, b)$ with an additional condition $p(a_2|a_1, b) = p(a_2|a_1)$. Their task is to guess the value of a function $g(a, b) : [n_a] \times [n_b] \to [n_c]$. In contrast to CC problems, there is no restriction on the amount of communication. The communication is constrained to be completely oblivious to the value of a_1. They achieve success with probability defined as $p = \sum_{a,b} p(a, b)p(c = g(a, b)|a, b)$.

In a classical OC protocol Alice prepares the message m employing an encoding scheme $\mathcal{E}$ which comprises of conditional probability distributions of the form $p_{\mathcal{E}}(m|a)$. Bob outputs c based on his input b and the message m using a decoding scheme $\mathcal{D}$ entailing conditional probability distributions $p_{\mathcal{D}}(c|b, m)$. The oblivious constraint for classical encoding schemes $\mathcal{E}$ reads as

$$\forall\, m, \forall\, a_1, a_1' \in [n_{a_1}],\ p_{\mathcal{E}}(m) = p_{\mathcal{E}}(m|a_1) = p_{\mathcal{E}}(m|a_1'), \tag{2}$$

where $p_{\mathcal{E}}(m|a_1) = \sum_{a_2} p(a_2|a_1)p_{\mathcal{E}}(m|a_1, a_2)$. This condition ensures that the same classical mixture is prepared for all values of a_1. The expression for maximal classical success probability is

$$p_{\text{NC}} = \max_{\{\mathcal{E}\}\{\mathcal{D}\}} \left\{ \sum_m \sum_b p(b) \times \left(\sum_a p(a|b)p_{\mathcal{E}}(m|a)p_{\mathcal{D}}(g(a, b)|b, m) \right) \right\}, \tag{3}$$

where the message m can take arbitrary number of distinct values. We use the subscript NC to reflect the fact that for OC tasks the maximal classical success probability is the same as the maximal PNC success probability [5,6].

On the other hand, quantum strategy for a OC task involves Alice transmitting states of arbitrary dimension, ρ_a for input a, such that the same mixed state ρ is prepared for all values of a_1, i.e., $\forall\, a_1$, $\sum_{a_2} p(a_2|a_1)\rho_{a_1,a_2} = \rho$. This ensures adherence to the oblivious condition. Upon receiving input b, Bob performs measurement $\{M_c^b\}$ (where $\sum_c M_c^b = \mathbb{I}$) on the transmitted system. The average success probability is given by the expression $p_{\mathcal{Q}} = \sum_{a,b} p(a, b)\text{Tr}(\rho_a M^b_{c=g(a,b)})$.

III. ADVANTAGE IN CC IMPLIES ADVANTAGE IN OC

In this section we present our main results. First, we make a couple of essential observations concerning the maximal classical success probability of OC tasks. Next, we construct an OC task tailored to a given instance of generic CC problem described in the previous section. We then formulate a PNC inequality by obtaining an upper bound on the classical success probability of the OC task. We utilize the very resources responsible for quantum advantage in the given CC problem [pertaining to without prior entanglement (i) one-way prepare and measure protocols, (ii) two-way multiround protocols, and (iii) entanglement assisted classical communication protocols] to orchestrate an advantageous quantum protocol for the associated OC task, thereby demonstrating the violation of the PNC inequality. Further, we present two instances of unbounded violations of PNC inequalities based on CC problems with exponential quantum advantage. Finally, we provide an alternative construction of OC task tailored to given CC problems and discuss the persistence of our results in general probabilistic theories.

A. Bounding classical success in OC tasks

In general, finding maximal classical success probability for OC tasks is an arduous task as (i) the dimension of the message is unbounded and (ii) the encoding scheme may be probabilistic. In lieu of these issues we employ the following lemmas (based on the observation in [5]) to facilitate an upper bound on classical success probability of the OC task.

Lemma 1: For an instance of the subclass of OC tasks defined in *Sec.* II B, the classical success probability p_{NC} is upper bounded in the following way:

$$p_{\text{NC}} \leqslant \max_{\{q_{a_1,a_2}\}} \left\{ \sum_b p(b) \max_c \left\{ \sum_{a_1,a_2} p(a_1|b) q_{a_1,a_2} \delta_{c,g(a,b)} \right\} \right\}, \tag{4}$$

where the outer maximization is over a set of variables $\{q_{a_1,a_2}\}$ satisfying the conditions

$$q_{a_1,a_2} \geqslant 0,\ \sum_{a_2} q_{a_1,a_2} = 1. \tag{5}$$

Lemma 2: The set of valid assignments of $\{q_{a_1,a_2}\}$ satisfying the linear constraints (5) form a convex polytope. The extremal points of this polytope resemble deterministic probability distributions, i.e., any extremal point $\{q^{\text{ext}}_{a_1,a_2}\}$ is of

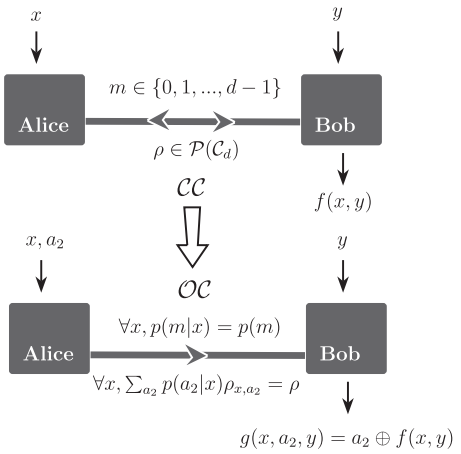

FIG. 1. Construction of OC task based on a given CC task. Notice while the amount of communication in the CC task by the dimension d of the physical system, there is no such constraint on communication in the OC. Instead, the communication is restricted so as not to reveal any information about the oblivious variable x.

the following form: for each a_1, $q^{\text{ext}}_{a_1,a_2} = 0$ for all values of a_2 except a specific $\tilde{a}_2$ for which $q^{\text{ext}}_{a_1,\tilde{a}_2} = 1$.

The proofs have been deferred to the Appendix. It follows from Lemma 2 that the outer maximization in (4) can be performed by evaluating the contained expression at each extremal point of convex polytope formed by the valid assignments of $\{q_{a_1,a_2}\}$. Let the extremal point yielding the maximal value be $\{q^{\text{ext,max}}_{a_1,a_2}\}$. This extremal point without loss of generality entails for each a_1, an $\tilde{a}_2$ where $q^{\text{ext,max}}_{a_1,\tilde{a}_2} = 1$. Let for each a_1, $\tilde{a}_2 = e_{a_1}$, then we have $q^{\text{ext,max}}_{a_1,a_2} = \delta_{a_2,e_{a_1}}$. Similarly, for the inner maximization suppose that for this extremal point, for each b the maximal value of $\sum_{a_1,a_2} p(a_1|b) q_{a_1,a_2} \delta_{c,g(a,b)}$ is obtained for $c = c_b$. Consequently, we arrive at the following distilled reexpression of (4):

$$p_{\text{NC}} \leqslant \sum_b p(b) \sum_{a_1,a_2} p(a_1|b)\ \delta_{e_{a_1},a_2}\ \delta_{c_b,g(a,b)}. \tag{6}$$

B. Tailoring OC tasks to given CC problems and PNC inequality

We now present the key ingredient of our modus operandi, an OC task tailored to a given CC problem. Given an instance of the generic CC problem described above, we construct the following OC task (see Fig. 1):

$$\begin{aligned} &a = (a_1 = x, a_2),\ b = y,\ c = z, \\ &p(a, b) = p(x, a_2, y) = p(y)p(x|y)p(a_2|x), \\ &\text{where } a_2 \in \{0, 1\},\ p(a_2|x) = \begin{cases} \frac{1}{d}, & \text{if } a_2 = 0 \\ \frac{d-1}{d}, & \text{if } a_2 = 1 \end{cases} \\ &\text{and } g(x, a_2, y) = f(x, y) \oplus a_2. \end{aligned} \tag{7}$$

Recall, that in the OC task the oblivious condition constrains the communicated system to not carry any retrievable information about x.

Next, by the means of the following proposition which upper bounds the classical success probability for the constructed OC task, we present a family of PNC inequalities tailored to CC problems.

Proposition 1: The PNC success probability of the OC task described in (7) is upper bounded by the maximal classical success probability of the CC problem wherein Alice is restricted to communicate a two-leveled system, i.e.,

$$p_{\text{NC}} \leqslant p_{\mathcal{C}_2}. \tag{8}$$

Proof. The proof involves obtaining an upper bound for the classical success probability of the OC task (constructed above) with the help of Lemmas 1 and 2. We then show that this upper bound forms a viable (not necessarily optimal) classical success probability for the original CC problem whilst the dimension of the message is restricted to two. Note that when the communication is restricted to be at most two-dimensional, two-way multiround CC protocols are equivalent to one-way CC protocols wherein only Alice is allowed to communicate a two-level message $m \in \{0, 1\}$ to Bob, deeming this inequality to be independent of the choice of protocol.

The expression for maximal classical success probability of the CC task when Alice is restricted to transmit a bit of communication $p_{\mathcal{C}_2}$ reads as

$$\begin{aligned} p_{\mathcal{C}_2} = \max_{\{E\}\{D\}} \Bigg\{ &\sum_y p(y) \\ &\times \Bigg(\sum_{m=0}^{1} \sum_x p(x|y) p_E(m|x) p_D(z = f(x, y)|y, m) \Bigg) \Bigg\}, \end{aligned} \tag{9}$$

where Alice's encoding scheme E entails conditional probability distributions of the form $p_E(m|x)$ and Bob's decoding scheme D entails conditional probability distributions of the form $p_D(z|y, m)$. On the other hand, it follows from (6) that the classical success probability of the OC task is upper bounded as follows:

$$\begin{aligned} p_{\text{NC}} &\leqslant \sum_y p(y) \sum_{x,a_2} p(x|y) \delta_{e_x,a_2}\ \delta_{c_y,a_2 \oplus f(x,y)} \\ &= \sum_y p(y) \sum_{x,a_2} p(x|y) \delta_{e_x,a_2}\ \delta_{a_2,c_y \oplus f(x,y)} \\ &= \sum_{x,y} p(x, y) \delta_{e_x,c_y \oplus f(x,y)}. \end{aligned} \tag{10}$$

To complete the proof, we demonstrate that this upper bound [right-hand side of (10)] is achievable in the CC task employing a two-leveled message $m \in \{0, 1\}$. To this end, we present the following classical $\mathcal{CC}$ protocol:

$$p_E(m|x) = \delta_{m,e_x}\ ,\ p_D(z|y, m) = \delta_{z,c_y \oplus m}. \tag{11}$$

Inserting this strategy in (9), one obtains

$$\begin{aligned} p_{\mathcal{C}_2} &\geqslant \sum_y p(y) \sum_{x,m} p(x|y) \delta_{m,e_x}\ \delta_{f(x,y),c_y \oplus m} \\ &= \sum_{x,y} p(x, y) \delta_{e_x,c_y \oplus f(x,y)}\ , \end{aligned} \tag{12}$$

which together with (10) yields the desired thesis (9). ■

C. Violation of PNC inequality from advantageous quantum CC protocols

Notice that up until this point our results are independent of the specifics of the CC protocol including the restriction on the amount of communication, but depend only on the problem itself. Now, we take three distinct classes of the advantageous quantum CC protocols and, based on these, we construct quantum strategies for the OC task to demonstrate the violation of the associated PNC inequalities.

1. One-way prepare and measure quantum CC protocols

One-way quantum CC protocols without prior entanglement are commonly referred to as *prepare and measure protocols*. In such protocols, Alice's state (a qudit ρ_x for input x) preparation and transmission is followed by a binary outcome measurement ($\{M_z^y\}$ upon receiving input y) at Bob's end. The quantum success probability is expressed as

$$p_{\mathcal{Q}_d} = \sum_{x,y} p(x,y)\mathrm{Tr}\left(\rho_x M^y_{z=f(x,y)}\right). \tag{13}$$

Notice that here, quantum success probability $p_{\mathcal{Q}_d}$ is not required to be maximal. Now, we present our result concerning PC manifest in advantageous prepare and measure quantum CC protocols.

Result 1: Given a prepare and measure quantum CC protocol, an advantage is obtained in the OC task described in (7) ($p_{\mathcal{Q}} > p_{\mathrm{NC}}$) whenever the following condition holds,

$$\frac{1}{d}(2p_{\mathcal{Q}_d} + d - 1 - \chi) > p_{\mathcal{C}_2}, \tag{14}$$

where $\chi = \sum_{x,y} p(x,y)\,\mathrm{Tr}\,(M^y_{z=f(x,y)})$ and $\{M_z^y\}$ are Bob's measurements employed in quantum CC protocol.

Proof. Our quantum strategy for the OC task described in (7) involves Alice preparing the same states (as in the quantum CC protocol described above) when $a_2 = 0$, i.e., $\rho_{x,a_2=0} = \rho_x$ and their orthogonal mixtures when $a_2 = 1$, i.e., $\rho_{x,a_2=1} = \frac{\mathbb{I}-\rho_x}{d-1}$. Alice's preparations are therefore oblivious to x, as $\forall\, x:\ \sum_{a_2} p(a_2|x)\rho_{x,a_2} = \frac{\mathbb{I}}{d}$. Bob's measurements remain unaltered from the quantum CC protocol. Plugging the expressions of $p(x,a_2,y)$ from (7) and $p_{\mathcal{Q}_d}$ from (13), we obtain the following success probability for this strategy:

$$\begin{aligned} p_{\mathcal{Q}} =& \sum_{x,a_2=0,y} p(x,a_2,y)\,\mathrm{Tr}(\rho_x M^y_{z=f(x,y)}) \\ &+ \sum_{x,a_2=1,y} p(x,a_2,y)\,\mathrm{Tr}\left(\frac{\mathbb{I}-\rho_x}{d-1} M^y_{z=1\oplus f(x,y)}\right) \\ =& \frac{1}{d}\left(2p_{\mathcal{Q}_d} + d - 1 - \chi\right), \end{aligned} \tag{15}$$

where $\chi = \sum_{x,y} p(x,y)\,\mathrm{Tr}\,(M^y_{z=f(x,y)})$. Now our desired result simply follows from (8). ∎

Now, given that the CC protocol under consideration is advantageous, i.e., $p_{\mathcal{Q}_d} > p_{\mathcal{C}_d}$, if follows that a quantum advantage in the OC task is obtained ($p_{\mathcal{Q}} > p_{\mathrm{NC}}$) whenever the following condition holds,

$$\frac{1}{d}(2p_{\mathcal{C}_d} + d - 1 - \chi) \geqslant p_{\mathcal{C}_2}. \tag{16}$$

To aid intuition and accessibility, we simplify the above condition (14) employing two lemmas (the proofs are deferred to the Appendix):

Lemma 3: For a given prepare and measure quantum CC protocol the following holds,

$$\chi \leqslant d\,p_G, \tag{17}$$

where $\chi = \sum_{x,y} p(x,y)\,\mathrm{Tr}\,(M^y_{z=f(x,y)})$, d is dimension of the communicated system and p_G is guessing probability without communication.

Lemma 4: Given a CC problem and a classical protocol using a two-leveled classical message with a success probability $p_{\mathcal{C}_2}$, the success probability of a protocol using a d-leveled classical message is lower bounded in the following way:

$$p_{\mathcal{C}_d} \geqslant 1 - \exp\left[-\frac{\log d}{2p_{\mathcal{C}_2}}\left(p_{\mathcal{C}_2} - \frac{1}{2}\right)^2\right]. \tag{18}$$

Corollary 1: By substituting the upper bound of χ from (17) in the condition (14), we find that $p_{\mathcal{Q}} > p_{NC}$ whenever $p_{\mathcal{Q}_2} > p_{\mathcal{C}_2}$ in any CC task with $p_G = \frac{1}{2}$.

Corollary 2: By imposing *Lemmas* 3 and 4 into (16), we find that $p_{\mathcal{Q}} > p_{NC}$ whenever the following condition holds:

$$d(p_{\mathcal{C}_2} + p_G - 1) + 2\exp\left[-\frac{\log d}{2p_{\mathcal{C}_2}}\left(p_{\mathcal{C}_2} - \frac{1}{2}\right)^2\right] \leqslant 1. \tag{19}$$

Notice, (19) relies only on classical success probability of the CC task with a two-leveled message $p_{\mathcal{C}_2}$ and success probability of the CC task without any communication p_G. This in turn deems (19) to be independent of the specifics of the implementation of classical or quantum CC protocols including the dimension of the communicated system.

2. Two-way multiround quantum CC protocols

Even though one-way CC protocols form a predominant subclass of quantum CC protocols, two-way multiround CC protocols employ relatively more involved features of quantum theory to facilitate an advantage [12]. In two-way multiround CC protocols, Alice and Bob have access to local quantum memories and exchange messages over multiple rounds of communication. In each round they use local operations to store an imprint of the message on their respective local memories and prepare a message for the next round. This results in complex premeasurement states wherein Alice's local memory may be entangled with Bob's local memory. Remarkably, our results hold intact for quantum advantage in CC tasks obtained via two-way multiround CC protocols.

We start by presenting a general two-way multiround CC protocol denoted by $\mathcal{P}$ (first described in [19]). Alice and Bob have access to some quantum memory, the states of respective quantum memory in the round r are symbolized by $A_r^{x,y}$ and $B_r^{x,y}$. These symbols serve for the convenience of description and for mere subscripts of the quantum state ρ. Each round consists of transmission of a message from Alice to Bob and back. We symbolize the communicated quantum system from Alice to Bob and from Bob to Alice in the round r by α_r and β_r, respectively. Let the total number of rounds be R. The protocol proceeds as follows.

(1) Depending on the input x, Alice applies a local operation U_1^x on the joint system of her initial memory A_0 and the blank message α to obtain an updated combined state ρ_{α_1,A_1^x} with local memory A_1^x and the message α_1. Alice then sends the message, i.e., the reduced state ρ_{α_1} to Bob. In general, the updated local memory and the message may now be entangled.

(2) Depending on the input y, Bob applies a local operation U_1^y on the joint system of his local memory B_0 and the message from Alice α_1 to obtain his updated combined system $\rho_{\beta_1,B_1^{x,y}}$ with local memory $B_1^{x,y}$ and the message β_1 which is then communicated back to Alice. As a result, Bob's local memory $B_1^{x,y}$ may be entangled with Alice's local memory A_1^x.

(3) This marks the completion of the first round. Alice and Bob repeat these steps for $R-1$ rounds. In the last round ($r=R$) upon receiving the message from Alice (α_R) instead of sending a message back to Alice, Bob performs the measurement $\{M_z^y\}$ on the joint system of the message and Bob's local memory from the previous round ($B_{R-1}^{x,y}$).

Given an upper bound on total dimension of communication d, they achieve success with probability $p_{\mathcal{Q}_d}=\sum_{x,y}p(x,y)\,\mathrm{Tr}(\rho_{\alpha_R,B_{R-1}^{x,y}}M_{z=f(x,y)}^y)$, where $\rho_{\alpha_R,B_{R-1}^{x,y}}$ is the reduced density matrix corresponding to the joint system of the message from Alice (α_R) and Bob's local memory from the penultimate round $B_{R-1}^{x,y}$.

To what follows, it is crucial to obtain an upper bound on the dimension of Bob's premeasurement state. We achieve this by employing the following steps.

(1) Following the methodology in [19], we first convert a given two-way multiround quantum communication protocol $\mathcal{P}$ utilizing $\log_2 d$ qubit (i.e., d-dimensional communication) communication to another protocol $\tilde{\mathcal{P}}$ that employs $2\log_2 d$ single-qubit exchanges. One can achieve this by splitting a q-qubit message from Alice to Bob (or the other way round) into q rounds of one qubit exchanges. The new protocol $\tilde{\mathcal{P}}$ has a total of $\tilde{R}=\log_2 d-1$ rounds, with each round involving transmission of a qubit from Alice to Bob and back. In the last round Alice sends a qubit $\tilde{\alpha}_{\tilde{R}}$ and Bob instead of sending back one, measures using another measurement $\{\tilde{M}_z^y\}$ the joint system of her local memory $\tilde{B}_{\tilde{R}-1}^{x,y}$ and the qubit message from Alice $\tilde{\alpha}_{\tilde{R}}$. The winning probability for $\tilde{\mathcal{P}}$ is equal to success probability of $\mathcal{P}$ but has the expression

$$p_{\mathcal{Q}_d}=\sum_{x,y}p(x,y)\,\mathrm{Tr}\left(\rho_{\tilde{\alpha}_{\tilde{R}},\tilde{B}_{\tilde{R}-1}^{x,y}}\tilde{M}_z^y\right). \tag{20}$$

(2) In the protocol $\tilde{\mathcal{P}}$, in each round r Bob applies a unitary $\tilde{U}_r^y$ on the one-qubit message from Alice from the previous round $\tilde{\alpha}_{r-1}$ and her local memory $\tilde{B}_{r-1}^{x,y}$. One can view the unitary operation as a controlled gate acting on the memory with one-qubit message being the control. This observation implies that for a fixed input x, for round r (i.e., after $r-1$ rounds), Bob's memory is spanned on at most 2^{r-1} orthogonal vectors (see Lemma 2 in [19]). This implies that for the last round Bob's memory in $\tilde{\mathcal{P}}$ requires at most $\tilde{R}-1$ qubits and the state $\rho_{\tilde{\alpha}_{\tilde{R}},\tilde{B}_{\tilde{R}-1}^{x,y}}$ is at most d dimensional (or equivalently $\log_2 d$ qubits).

Now we are prepared to present our result concerning PC manifest in advantageous two-way multiround quantum CC protocols,

Result 2: Given a two-way multiround quantum CC protocol $\mathcal{P}$, an advantage is obtained in the OC task described in (7) with $p(a_2=0|x)=1/d^{n_y}$ ($p_{\mathcal{Q}}>p_{\mathrm{NC}}$) whenever the following condition holds,

$$\frac{1}{d^{n_y}}(2p_{\mathcal{Q}_d}+d^{n_y}-1-d^{n_y-1}\chi)>p_{\mathcal{C}_2}, \tag{21}$$

where $\chi=\sum_{x,y}p(x,y)\,\mathrm{Tr}\,(\tilde{M}_{z=f(x,y)}^y)$ and $\{\tilde{M}_z^y\}$ are Bob's measurements employed in the derived quantum CC protocol $\tilde{\mathcal{P}}$.

Proof. We begin by devising a quantum strategy for the OC task. We orchestrate a quantum strategy for the OC task based on the quantum two-way multiround CC protocol. To achieve this we exploit the fact that there is no restriction on the amount of communication in the OC task. The core idea remains the same as in one-way CC case, Alice sends Bob's premeasurement state when $a_2=0$ and its orthogonal mixture when $a_2=1$. We start with converting the given quantum two-way multiround CC protocol $\mathcal{P}$ which uses d-dimensional communication in total, to one that uses $2\log_2 d$ qubits of communication $\tilde{\mathcal{P}}$. There is still an issue with this approach; Alice does not know the value y in advance, and the premeasurement state may depend on y. In order to deal with this issue, when $a_2=0$ Alice simply prepares the premeasurement states for all values of y and sends a tensor product of these states as the message $\Theta_{x,a_2=0}=\bigotimes_y\rho_{\tilde{\alpha}_{\tilde{R}},\tilde{B}_{\tilde{R}-1}^{x,y}}$. Recall that the states $\rho_{\tilde{\alpha}_{\tilde{R}},\tilde{B}_{\tilde{R}-1}^{x,y}}$ are at most d dimensional. When $a_2=1$, Alice sends the orthogonal mixture of $\Theta_{x,a_2=0}$, $\Theta_{x,a_2=1}=\frac{\mathbb{I}-\bigotimes_y\rho_{\tilde{\alpha}_{\tilde{R}},\tilde{B}_{\tilde{R}-1}^{x,y}}}{d^{n_y}-1}$. It is straightforward to see that Alice's preparations are oblivious to x, as $\forall\, x,x'\in[n_x]$, $\sum_{a_2}p(a_2,x)\Theta_{x,a_2}=\sum_{a_2}p(a_2,x')\Theta_{x',a_2}=\frac{\mathbb{I}}{d^{n_y}}$. Now, upon receiving the message from Alice, Bob performs the measurement $\tilde{M}_z^y$ on the relevant part (depending on his input y) of the message, i.e., either $\rho_{\tilde{\alpha}_{\tilde{R}},\tilde{B}_{\tilde{R}-1}^{x,y}}$ or $\mathrm{tr}_{\neg y}(\Theta_{x,a_2=1})=\frac{d^{n_y-1}\mathbb{I}-\rho_{\tilde{\alpha}_{\tilde{R}},\tilde{B}_{\tilde{R}-1}^{x,y}}}{d^{n_y}-1}$. This strategy yields the following success probability:

$$\begin{aligned}p_{\mathcal{Q}}&=\sum_{x,a_2=0,y}p(x,a_2,y)\,\mathrm{Tr}\left(\rho_{\tilde{\alpha}_{\tilde{R}},\tilde{B}_{\tilde{R}-1}^{x,y}}\tilde{M}_{z=f(x,y)}^y\right)\\&\quad+\sum_{x,a_2=1,y}p(x,a_2,y)\,\mathrm{Tr}\left(\frac{d^{n_y-1}\mathbb{I}-\rho_{\tilde{\alpha}_{\tilde{R}},\tilde{B}_{\tilde{R}-1}^{x,y}}}{d^{n_y}-1}\tilde{M}_{z=1\oplus f(x,y)}^y\right)\\&=\frac{1}{d^{n_y}}\left(2p_{\mathcal{C}_d}+d^{n_y}-1-d^{n_y-1}\chi\right),\end{aligned} \tag{22}$$

where $\chi=\sum_{x,y}p(x,y)\,\mathrm{Tr}\,(\tilde{M}_{z=f(x,y)}^y)$ and $p_{\mathcal{Q}_d}$ is given by (20). Now our desired result simply follows from (8). ■

Given quantum advantage in CC problem ($p_{\mathcal{Q}_d}>p_{\mathcal{C}_d}$) and (22), an advantage is obtained in the OC task ($p_{\mathcal{Q}}>p_{\mathrm{NC}}$) described in (7) with $p(a_2=0|x)=1/d^{n_y}$ whenever the following holds:

$$\frac{1}{d^{n_y}}(2p_{\mathcal{C}_d}+d^{n_y}-1-d^{n_y-1}\chi)>p_{\mathcal{C}_2}.$$

3. *Entanglement assisted classical communication protocols*

Another nonequivalent [20,21] class of advantageous quantum CC protocols is that of entanglement assisted classical communication protocols, wherein Alice and Bob share an

entangled state ρ_{AB} (a density operator on $\mathcal{H}_A \otimes \mathcal{H}_B$), Alice performs a d outcome measurement ($\{M_m^x\}$) and sends her outcome m as the message. Upon receiving the message m, Bob performs a binary outcome measurement ($\{M_z^{y,m}\}$). The quantum guessing probability is expressed as

$$p_{\mathcal{Q}_d} = \sum_{x,y} p(x,y) \sum_{m=0}^{d-1} \mathrm{Tr}\big(\rho_{AB} M_m^x \otimes M_{z=f(x,y)}^{y,m}\big). \tag{23}$$

Let the reduced density matrix of Bob's part of the entangled state ρ_B be of dimension e, i.e., $e = \dim(\mathcal{H}_B)$. A quantum strategy for the OC task (7) based on advantageous entanglement assisted classical communication CC protocols and the corresponding condition for retrieving an advantage is presented in the following result.

Result 3: Given a entanglement assisted classical communication CC protocol, an advantage is obtained in the OC task described in (7) with $p(a_2 = 0|x) = 1/d'$ ($p_{\mathcal{Q}} > p_{\mathrm{NC}}$) whenever the following condition holds:

$$\frac{1}{d'}(2p_{\mathcal{Q}_d} + d' - 1 - \chi) > p_{\mathcal{C}_2}, \tag{24}$$

where $\chi = \sum_{x,y} p(x,y)\,\mathrm{Tr}\,(M_{z=f(x,y)}^y)$ and $\{M_z^y\}$ are Bob's measurements employed in the CC protocol, $d' = de$, and e is the dimension of Bob's local part of the shared entangled state.

Proof. In this case, we capitalize over the fact that the amount of communication is unrestricted in the OC task and convert the given entanglement assisted classical communication protocol to a prepare and measure protocol wherein Alice simply sends Bob the corresponding premeasurement state (Bob's marginal state along with the classical message). This in turn enables us to construct quantum strategies for the OC task employing the aforementioned methodology.

In order to utilize the machinery developed so far, we first construct a quantum prepare and measure protocol deploying a $d' = de$ dimensional communicated system but with the same probability of success $p_{\mathcal{Q}_d}$ as the given entanglement assisted classical communication protocol. Upon receiving x Alice prepares the state $\rho_x = |m\rangle\langle m| \otimes \rho_B$ where the state $|m\rangle\langle m|$ is simply the quantum encoding of the classical message m into d orthogonal states. She accomplishes this feat by measuring $\{M_m^x \otimes \mathbb{I}\}$ on the entangled state ρ_{AB} to which we assume she has access to. The communicated system is of dimension $d' = de$. Bob first retrieves the message by performing the measurement $\{M_m\}$ on the appropriate subsystem of the communicated system and depending on it performs the measurement $\{M_z^{y,m}\}$ on rest of the communicated system, captured conveniently in a joint measurement $\{\tilde{M}_z^y = M_m \otimes M_z^{y,m}\}$. This yields the same success probability $p_{\mathcal{Q}_d}$. Now, we convert this prepare and measure protocol into an OC protocol utilizing the methodology described in the proof of Result 1 and obtain the following lower bound on quantum success probability for the OC task: $p_{\mathcal{Q}} \geqslant \frac{1}{d'}(2p_{\mathcal{Q}_d} + d' - 1 - \chi)$ where $\chi = \sum_{x,y} p(x,y)\,\mathrm{Tr}\,(M_{z=f(x,y)}^y)$ and $p_{\mathcal{Q}_d}$ is given in (23). This in turn leads us to the condition for quantum advantage in the OC task (24). ■

Notice that in a rather predominant subclass of entanglement assisted classical communication protocols, Bob applies a completely positive trace0preserving map Λ_m on his part of the entangled state $\rho_{\mathcal{B}}$ and performs the measurement $\{M_z^y\}$ on $\Lambda_m(\rho_B)$. In such cases, Alice having access to the message m sends $\rho_x = \Lambda_m(\rho_B)$, effectively reducing the dimension of the communicated system in the prepare measure protocol to $d' = e$, thereby improving the feasibility of the quantum advantage in the OC task.

D. Unbounded violation of PNC inequalities

To demonstrate the vitality of the results obtained so far, we illustrate two examples of unbounded quantum violations of PNC inequalities based of two widely studied CC problems and associated prepare and measure protocols with exponential quantum advantage. Let us rewrite the PNC inequality (8) as $\alpha_{\mathrm{NC}} \leqslant \alpha_{\mathcal{C}_2}$, where $\alpha_{\mathrm{NC}} = p_{\mathrm{NC}} - \frac{1}{2}$, $\alpha_{\mathcal{C}_2} = p_{\mathcal{C}_2} - \frac{1}{2}$. Then, a quantum advantage in a CC problem adhering to the condition (14) implies that there exists quantum protocol for the OC task with $\alpha_{\mathcal{Q}} = \frac{1}{d}(2p_{\mathcal{Q}_d} + d - 1 - \chi) - \frac{1}{2}$. Quantum advantage in CC problems is prevalently reported in terms of the amount of communication required to achieve a bounded probability of success p_S, i.e., $\mathcal{Q}(f, p_S) < \mathcal{C}(f, p_S)$. To apply our results to the innumerable instances of quantum advantage reported in this fashion, we employ the following lemma.

Lemma 5: Given a CC problem and a protocol which achieves a success probability p_S using $\mathcal{C}(f, p_S)$ bits, the success probability of a protocol using a two-leveled classical message is upper bounded in the following way:

$$p_{\mathcal{C}_2} \leqslant \frac{1}{2} + \sqrt{\frac{2p_S}{\mathcal{C}(f, p_S)}}. \tag{25}$$

The proof has been deferred to the Appendix.

Corollary 3: The ratio of quantum and PNC values of α (denoted by β) can be lower bounded with help of Lemma 3 in the following way:

$$\begin{aligned}\beta &\geqslant \frac{\alpha_{\mathcal{Q}}}{\alpha_{\mathrm{NC}}} \geqslant \frac{\frac{1}{d}(2p_{\mathcal{Q}_d} + d - 1 - \chi) - \frac{1}{2}}{p_{\mathcal{C}_2} - \frac{1}{2}} \\ &\geqslant \frac{\sqrt{\mathcal{C}(f, p_S)}(2p_{\mathcal{Q}_d} + d/2 - dp_G - 1)}{d\sqrt{2p_S}}.\end{aligned} \tag{26}$$

To obtain an unbounded violation of the PNC inequality $\alpha_{\mathrm{NC}} \leqslant \alpha_{\mathcal{C}_2}$, it suffices to show that β could be arbitrarily large ($\gg 1$) [22]. We demonstrate the same for two widely studied CC problems [23,24] with exponential quantum advantage:

(1) *Vector in a subspace.* Alice is given an n-dimensional unit vector u and Bob is given a subspace of dimension $n/2$, S with the promise that either $u \in S$ or $u \in S^{\perp}$. Their goal is to decide which is the case. Here, $p_{\mathcal{Q}_d = \log n} = 1$, i.e., $\mathcal{Q}(f, 1) = \log n$, $\mathcal{C}(f, p_S = \frac{2}{3}) = \Omega(\sqrt[3]{n})$ (Theorem 4.2 in [23]) and a simple calculation yields $\chi = \frac{\log n}{2}$, $p_G = \frac{1}{2}$. Inserting these into (26) one obtains an arbitrarily large lower bound for the ratio $\beta \geqslant \Omega(\frac{\sqrt[6]{n}}{\log n})$.

(2) *Hidden matching.* Alice is given a bit string $x \in \{0,1\}^n$ of length n and Bob is given $y \in M_n$ (M_n denotes the family of all possible perfect matchings on n nodes). Their goal is to output a tuple (i, j, t) such that the edge (i, j) belongs to the matching y and $t = x_i \oplus x_j$. Clearly, the hidden matching problem is not a typical CC problem, specifically, it is a relational problem. Nevertheless, we can find that the machinery

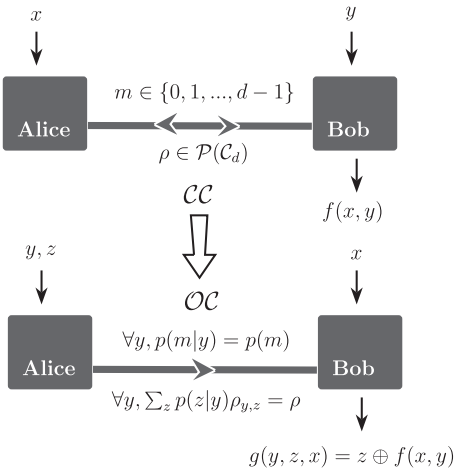

FIG. 2. Alternative construction of OC task based on a given CC task. The communication is restricted so as not to reveal any information about a oblivious variable y.

developed so far including the Proposition 1 and Corollary 3 still hold for relational CC problem.

Lemma 6: For hidden matching problem an OC task can be constructed with a success probability p_{NC}, such that $p_{\text{NC}} \leqslant p_{\mathcal{C}_2}$.

The proof is similar to the proof of Proposition 1 (see Appendix). This proof provides for our insight that our results persist in case of relational CC problems beyond mainstream functional CC problems. For hidden matching $p_{\mathcal{Q}_d} = 1$, $\mathcal{Q}(f, 1) = d = \log n$, $p_G = \frac{1}{2}$, $\chi = \frac{\log n}{2}$, and $\mathcal{C}(f, 1) = \Omega(\sqrt{n})$ [24]. Inserting these observations into (26) one obtains an even larger violation as the lower bound on β grows faster, i.e., $\beta \geqslant \Omega(\frac{\sqrt[4]{n}}{\log n})$.

E. Alternative construction of OC task

An equivalent alternative construction of the OC task tailored to a given CC problem is presented here. Given a general CC problem and an advantageous quantum CC protocol, i.e., $p_{\mathcal{Q}_d} > p_{\mathcal{C}_d}$, we construct the following OC task (shown in Fig. 2):

$$\begin{aligned} a = (y, z),\ b = x,\ c \in \{0, 1\}, \\ p(a, b) = p(y, z, x) = p(x)p(y|x)p(z|y), \\ \text{where } p(z|y) = \frac{\text{Tr}(M_z^y)}{d}, \\ g(y, z, x) = f(x, y) \oplus z. \end{aligned} \tag{27}$$

Here, $\{M_z^y\}$ are Bob's measurements employed in the given quantum CC protocol under consideration, and the oblivious condition constrains the communicated system to not carry any information about y.

Proposition 2: The PNC success probability of the OC task described in (27) is upper bounded by the maximal classical success probability of the CC problem wherein Alice is restricted to communicate a two-leveled system, i.e., $p_{\text{NC}} \leqslant p_{\mathcal{C}_2}$.

Proof. We follow the same steps as in the proof of Proposition 1. Again employing Lemmas 1 and 2 we arrive at the following upper on the classical success probability of the OC task described in (27):

$$\begin{aligned} p_{\text{NC}} &\leqslant \sum_x p(x) \sum_{y,z} p(y|x)\ \delta_{e_y,z}\ \delta_{c_x,z\oplus f(x,y)} \\ &= \sum_{x,y} p(x, y)\ \delta_{e_y,c_x\oplus f(x,y)}\ . \end{aligned} \tag{28}$$

Let us consider the following classical protocol employing a two-leveled message $m \in \{0, 1\}$ for the CC problem:

$$p_E(m|x) = \delta_{m,c_x},\ p_D(z|y, m) = \delta_{z,m\oplus e_y}. \tag{29}$$

Inserting the above strategy in (9), one obtains the same success probability in CC) problem as given in the right side of (28). ■

The contrasting feature of this construction is that the exact duals of the states and measurements used in the advantageous quantum CC protocol form the corresponding measurements and states, respectively, for the quantum OC protocol. That is, Alice's preparation for the OC task is $\rho_{y,z} = \frac{M_z^y}{\text{Tr}(M_z^y)}$ and Bob's measurement for his input x is $\{\rho_x, \mathbb{I} - \rho_x\}$. Clearly, Bob remains oblivious to y due to the completeness of quantum measurements, i.e., $\forall\ y,\ \sum_z p(z|y)\rho_{y,z} = \frac{\mathbb{I}}{d}$. Subsequently, plugging the expressions of $p(y, z, x)$ from (27) and $p_{\mathcal{Q}_d}$ from (13), a simple calculation leads to the same expression as in (15),

$$\begin{aligned} p_{\mathcal{Q}} = &\sum_{y,z=f(x,y),x} p(y, z, x)\, \text{Tr}\left(\rho_x \frac{M_z^y}{\text{Tr}(M_z^y)}\right) \\ &+ \sum_{y,z=1\oplus f(x,y),x} p(y, z, x)\, \text{Tr}\left((\mathbb{I} - \rho_x)\frac{M_z^y}{\text{Tr}\left(M_z^y\right)}\right) \\ = &\frac{1}{d}\left(2p_{\mathcal{Q}_d} + d - 1 - \chi\right), \end{aligned} \tag{30}$$

where $\chi = \sum_{x,y} p(x, y)\, \text{Tr}\,(M^y_{z=f(x,y)})$. Thus, all the results derived previously remain intact for this alternative construction of OC task.

This construction provides for our inference that our main results can be extended to general probabilistic theories with the feature of self-duality of states and measurement effects [1,25]. This follows from the fact that the states and measurements that reveal PC in the alternative OC task are just the dual of the measurement effects and states employed in the CC. The property of self-duality emerges from a set of natural postulates in the framework of general probabilistic theories [25]. However, this implication is not true in any operational theory. Here, we demonstrate a toy theory and an ontic model with CC advantage but no possibility of PC. Consider a well-known CC task, the $(2 \to 1)$ random access code [26], wherein Alice receives two random input bits x_1, x_2 to be encoded into a two-dimensional system and sends it to Bob. Bob receives a random input bit y along with the message from Alice and is required to guess x_y. This theory, having only three preparations and just two measurements, is a fragment of quantum theory. This fragment of quantum theory does not adhere to self-duality. Clearly, the theory admits advantage in this task as the average success probability $p_{\mathcal{Q}_2} \approx 0.8 > p_{\mathcal{C}_2} = 0.75$. In an ontological model

underlying this toy theory there are only three ontic states labeled as $\psi_{x_1x_2}$ which correspond to pure quantum preparations as $\psi_{11,10} = |1\rangle$, $\psi_{00} = \cos(\theta)|0\rangle + \sin(\theta)|1\rangle$, $\psi_{01} = \cos(\theta)|0\rangle - \sin(\theta)|1\rangle$ where $\theta = \frac{\pi}{8}$ and two binary-outcome response schemes corresponding to Bob's setting $y = 0, 1$ and measurements σ_z, σ_x, respectively. However, since this ontological model has only three ontic states, any mixed preparation in this theory has a unique decomposition, thus ruling out the possibility of PC [27]. This shows from the basis of the inference that self-duality of states and measurements is a necessary requirement for our results to persist in general probabilistic theories.

IV. BELL INEQUALITY VIOLATION IMPLIES ADVANTAGE IN OC

With the help of the tools developed so far we now present the complete proof of the fact that Bell inequality violations imply advantage in an associated OC task. For any Bell inequality an OC task can be constructed porting Bell inequality violation to an advantageous strategy for the OC task. For the spacelike separated scenario the collapsed state on Bob's end is prepared and sent in the OC task and for the timelike separated case [18] the premeasurement state at Bob's end is prepared and sent in the $\mathcal{OC}$ task. This would make all Bell inequality violation operationally reveal PC. However, there is a subtlety here, while deterministic encoding strategies yield bounds on Bell inequalities, the PNC bounds on the success parameter of the OC tasks might spring from probabilistic encoding schemes [5]. An inadequate attempt to prove the above thesis was made in [6], as the authors explicitly assume deterministic encoding schemes for the constructed OC task. We use the tools developed in this paper to provide the complete proof for the thesis.

The setup for a spacelike separated Bell experiment does not involve any communication, instead two spatially separated parties Alice and Bob are provided with inputs $x \in [n_x]$, $y \in [n_y]$, respectively. Their objective is to return outputs $u \in [n_u]$, $v \in [n_v]$, respectively, so as to maximize an expression of the form

$$\mathcal{B} = \sum_{u,v,x,y} s_{x,y,u,v}\ p(x, y)p(u, v|x, y), \tag{31}$$

where $s_{x,y,u,v} \geqslant 0$. The parties may share correlations (classical: shared randomness or quantum: entangled states) which essentially yield advice in the form of conditional probability distributions $p(u, v|x, y)$. If Alice and Bob share a local-realist (classical) correlation, the maximum they can achieve is

$$\mathcal{B}_{\mathcal{L}} = \sum_{\lambda,u,v,x,y} s_{x,y,u,v}\ p(x, y)p(\lambda)p_\lambda(u|x)p_\lambda(v|y). \tag{32}$$

This fact is captured in Bell inequalities.

Consider a quantum strategy which violates a Bell inequality, i.e., $\mathcal{B}_{\mathcal{Q}} > \mathcal{B}_{\mathcal{L}}$. The probability of getting outcome u when measurement x is performed on the shared quantum state is $p_{\mathcal{Q}}(u|x)$ and the reduced quantum state on Bob's subsystem is denoted by $\rho^B_{u|x}$. We follow the construction of OC presented in [6],

$$\begin{aligned} a = (a_1, a_2) = (x, u),\ b = y,\ c = v,\\ p(a, b) = p(x, u, y) = p(y)p(x|y)p_{\mathcal{Q}}(u|x), \end{aligned} \tag{33}$$

where communication is constrained to oblivious to x. The figure of merit in the OC is given by

$$p = \sum_{u,v,x,y} s_{x,y,u,v}\ p(x, u, y)p(v|x, u, y). \tag{34}$$

Proposition 3 The noncontextual success probability of the OC task is upper bounded by the optimal local-realist value of Bell expression, i.e., $p_{\text{NC}} \leqslant \mathcal{B}_{\mathcal{L}}$.

Proof. It is straightforward to see that Lemmas 1 and 2 apply just as well to the above OC task and similar to (6) we retrieve an upper bound on the associated p_{NC} as follows:

$$\begin{aligned} p_{\text{NC}} &\leqslant \sum_y p(y) \sum_{x,u,v} p(x|y)s_{x,y,u,v}\ \delta_{e_x,u}\ \delta_{v_y,v} \\ &= \sum_{x,y,u,v} p(x, y)s_{x,y,u,v}\ \delta_{e_x,u}\ \delta_{v_y,v}\ . \end{aligned} \tag{35}$$

Now, we detail the proof of the above observation. The expression for maximal classical success probability (34) is

$$\begin{aligned} p_{\text{NC}} = \max_{\{\mathcal{E}\}\{\mathcal{D}\}} \Bigg\{ \sum_m \sum_y p(y) \\ \times \Bigg(\sum_{x,u} p(x|y)p_{\mathcal{Q}}(u|x)s_{x,y,u,v}\ p_{\mathcal{E}}(m|x, u)p_{\mathcal{D}}(v|y, m) \Bigg) \Bigg\}, \end{aligned} \tag{36}$$

and the oblivious constraints imply

$$\begin{aligned} \forall\ m, \forall\ x, x' \in [n_x], \\ p_{\mathcal{E}}(m) &:= p_{\mathcal{E}}(m|x) \\ &= \sum_u p_{\mathcal{Q}}(u|x)p_{\mathcal{E}}(m|x, u) \\ &= p_{\mathcal{E}}(m|x'). \end{aligned} \tag{37}$$

Now, following the same argument as in the proof of Lemma 1 one obtains

$$\begin{aligned} p_{\text{NC}} \leqslant \max_{\{q_{x,u}\}} \Bigg\{ \sum_y p(y) \max_v \Bigg\{ \sum_{x,u} p(x|y)q_{x,u}s_{x,y,u,v} \Bigg\} \Bigg\}, \\ \text{where} \quad \forall\ x, u,\ q_{x,u} \geqslant 0,\ \sum_u q_{x,u} = 1. \end{aligned} \tag{38}$$

Now invoking Lemma 2, suppose the extremal point yielding the optimal value of right-hand side of (38) corresponds to $u^{\text{ext}} = e_x$ for each x, i.e., $q_{x,u} = \delta_{u,e_x}$, and for that extremal point $\max_v\{\sum_{x,u} p(x|y)q_{x,u}s_{x,y,u,v}\}$ is achieved for v_y for each y. Subsequently, (38) can be expressed as (35).

Now, we propose a hidden variable model such that $p_\lambda(u|x) = \delta_{u,e_x}$, $p_\lambda(v|y) = \delta_{v,v_y}$. Plugging this local strategy into (32), one obtains the same the expression for $\mathcal{B}_{\mathcal{L}}$ as the right-hand side of (35), thus completing the proof. ■

A quantum strategy for the OC task can be easily constructed from the states and measurements responsible for violation of Bell inequality: Alice sends $\rho^B_{u|x}$ for input (x, u) and Bob's measurement settings are the same as in the given Bell experiment. Adherence of oblivious condition for this strategy simply follows from the no-signaling condition. Thus, we conclude $p_{\mathcal{Q}} = \mathcal{B}_{\mathcal{Q}} > \mathcal{B}_{\mathcal{L}} \geqslant p_{\text{NC}}$.

V. CONCEPTUAL INSIGHT AND IMPLICATIONS

The early stages of the quantum information epoch focused primarily on finding communication, computation, and information processing tasks wherein quantum resources and protocols provide advantage over their classical counterparts. As a consequence, the quantum departure from classical limits in such tasks has been significantly substantiated in innumerable and variegated classes of tasks; this perception is now commonly referred to as the "quantum advantage." However, there is little insight into what feature of quantum theory is underneath such a remarkable feat. Consequently, further search for such tasks usually employs narrowing heuristic intuition. The answers to such questions carry with them the potential of directing and broadening the search for tasks with quantum advantage. However, this seemingly simple question turns out to be substantially arduous and rich in complexity. We must begin by discarding the cyclic answers that inherently refer back to the operational quantum formalism which was *a priori* responsible for the advantageous predictions such as superposition of states. While these answers might lead to sharpening intuition, they do not lead to any significant insights. To further insight, the answers must arguably pertain to a ground common to classical and quantum theory, where nonclassical features underlying the quantum formalism are uncovered. The study of ontology or "underlying hidden variables" provides for such a ground. On the other hand, quantum communication advantage has a vast variety of manifestations, however, quantum CC advantage and device-independent information processing form the most prominent of them. In this article, we sought to find the quantum ontic feature that underlies quantum CC advantage.

In a nutshell, this work exposes the essential connection between operational quantum communication advantage and the ontic feature of PC, via operational OC tasks. In other words, we unveil a unifying connection between quantum CC advantage and quantum advantage in OC tasks, where the latter forms the operational signature of PC. We provide two intuitive ways of constructing an OC task tailored to any given CC task (7) and (27). The OC tasks thus obtained have two salient features: First, the maximal achievable classical success probability in both OC tasks is bounded by the maximal achievable classical success probability in the CC problem when the communicated system is restricted to be two dimensional. This in turn provides for two distinct PNC inequalities corresponding to every CC problem. Second, for any advantageous quantum (i) prepare and measure, (ii) two-way multiround and, (iii) entanglement assisted classical communication CC protocols, we obtain quantum OC strategies which utilize the same states and measurements. An advantage is obtained in the constructed OC task revealing PC whenever the conditions (14), (21), and (24) are met, respectively. It is a remarkable accomplishment of our construction that these conditions feature a comparison between CC performance of quantum d-level and CC performance of classical two-level systems. Notably, these conditions allow us to demonstrate first instances of unbounded violation of PNC inequalities from exponential quantum CC advantage. We remark that there exists a tradeoff between generality of our results and the tightness of these conditions for higher-dimensional quantum CC protocols. Because in this work we concern ourselves with general implications, these already substantially tight conditions might be tightened even further by fine tuning our constructions to specific CC problems and associated higher-dimensional quantum CC protocols. For instance, these conditions base themselves on the PNC inequality in Proposition 1 which in turn relies on a state-of-the-art technique we employed to obtain upper bounds on maximal classical (PNC) success probability of OC tasks. A tighter upper bound on maximal classical success probability p_{NC} or finding out the exact value will further tighten the conditions under consideration. In summary, not only do our results capture PC manifest in all predominant classes of advantageous quantum CC protocols, but they also hold beyond mainstream functional CC problems, i.e., even in case of relational CC problems (see proof of Lemma 6).

Our two constructions underscore two distinct ways in which PC is manifest in an advantageous CC protocol. An advantage in the first OC task (7) reveals PC manifest in the states from the CC protocol and their orthogonal mixtures, using the same measurements from the CC protocol. Whereas an advantage in the second OC task (27) reveals PC manifest in the states corresponding to the measurement effects from the CC protocol, with the aid of measurements corresponding to the states employed in the CC task. The second construction (27) enables a direct inference that our results and implications can be extended beyond quantum theory in general probabilistic theories with the property of self-duality of states and measurements effects.

Concerning other ontic features as plausible ground of quantum CC advantage, the connection between quantum advantage in CC and nonlocality has been explored in [19,28,29]. Given any protocol offering a sufficiently large quantum CC advantage, Refs. [19,29] provide a way for obtaining measurement statistics that violate some Bell inequality. These approaches basically employ an independent teleportation subroutine to transmit Alice's preparations (from quantum CC protocol). This in turn implies that the nonlocality thus revealed stems from additional entangled states and measurements associated with the teleportation protocol, which are unrelated to the ones employed in the advantageous quantum CC protocol. Therefore, the assertion that quantum CC advantage implies nonlocality is rather weak. Whereas, along with the very states and measurements responsible for the quantum CC advantage we use additional preparations, but these preparations are orthogonal mixtures of these states and therefore depend on the advantageous protocol. Therefore, in this sense, our results reveal a substantially more intimate connection between quantum CC advantage and PC. Furthermore, we provide a complete proof of the fact that any Bell inequality violation implies an advantage in an associated OC task, thereby porting even the weak implication along with device-independent information processing operationally to PC. Moreover, [5] shows that all logical proofs of Kochen-Specker contextuality yield an advantage in the OC task. It is a well-known fact that while a two-dimensional quantum system is enough to demonstrate PC, Kochen-Specker contextuality and nonlocality require at least three- and four-dimensional quantum systems, respectively. In summary, not only a wide spectrum of quantum communication advantage

reveals PC, even the operational witnesses of other well-known ontic features imply PC. This leads us to our tentative assertion that PC is innately related to quantum communication advantage.

While our implications are ontological, our methodology is strictly operational and employs advantage in OC tasks as the intermediary between operational CC advantage and the ontic feature of PC. Our results therefore indicate the fundamental significance of OC tasks to quantum advantage in communication. Furthermore, OC tasks form primitives for a range of cryptographic protocols [30,31] and have found applications in privacy-preserving computation [32]. Apart from the aforementioned implications, our methodology has exposed a large class of OC tasks with quantum advantage.

The question "why quantum advantage?" is far from settled. While the results of this article point to PC, they in no way close the door to more fundamental ontological or causal features of quantum theory. A much more arduous question of whether PC with self-duality (or some other set of features) ensures a CC advantage remains to be addressed. Given the significance of OC tasks, it might prove worthwhile to consider their generalizations to multipartite scenarios and explore potential application to the semi-device-independent paradigm. Another natural direction for future research is to look for information theoretic principles [33] that restrict success in $\mathcal{OC}$ tasks to quantum maximum.

ACKNOWLEDGMENTS

We thank M. Pawłowski, M. Horodecki, M. Oszmaniec, and C. M. Scandolo for helpful discussion. This research was conducted in National Quantum Information Centre Gdansk. This work is supported by NCN Grants No. 2016/23/N/ST2/02817 and No. 2014/14/E/ST2/00020, and FNP grant First TEAM (Grant No. First TEAM/2016-1/5).

APPENDIX: PROOFS OF LEMMAS

In this Appendix we provide the proofs of all the lemmas used in the article.

Lemma 7: For an instance of the subclass of OC tasks defined in Sec. II B, the classical success probability p_{NC} is upper bounded in the following way,

$$p_{\mathrm{NC}} \leqslant \max_{\{q_{a_1,a_2}\}} \left\{ \sum_b p(b) \max_c \left\{ \sum_{a_1,a_2} p(a_1|b) q_{a_1,a_2} \delta_{c,g(a,b)} \right\} \right\}, \tag{A1}$$

where the outer maximization is over a set of variables $\{q_{a_1,a_2}\}$ satisfying the conditions,

$$q_{a_1,a_2} \geqslant 0, \ \sum_{a_2} q_{a_1,a_2} = 1. \tag{A2}$$

Proof. We follow the method introduced in [5]. Let us recall that the expression for maximal classical success probability for the OC task described in Eq. (7) is

$$p_{\mathrm{NC}} = \max_{\{\mathcal{E}\}\{\mathcal{D}\}} \left\{ \sum_m \sum_b p(b) \Bigg(\sum_a p(a|b) p_{\mathcal{E}}(m|a) p_{\mathcal{D}}(c = g(a,b)|b,m) \Bigg) \right\}, \tag{A3}$$

where the message m can take arbitrary number of distinct values. And we seek to obtain an upper bound of p_{NC} under the oblivious constraints

$$\forall\, m, \forall\, a_1, a_1' \in [n_{a_1}], \ p_{\mathcal{E}}(m) = p_{\mathcal{E}}(m|a_1) = \sum_{a_2} p(a_2|a_1) p_{\mathcal{E}}(m|a_1,a_2) = p_{\mathcal{E}}(m|a_1'). \tag{A4}$$

We proceed in two steps: first, we observe that given an encoding scheme, the optimal decoding scheme $\mathcal{D}^*$ for OC task is fixed and deterministic. Then, we provide a technique for recovering an upper bound on p_{NC} by finding the optimal encoding scheme $\mathcal{E}^*$ for a single level of the message.

Decoding in an OC task: In order to attain the maximal success probability, Bob's decoding strategy $p_{\mathcal{D}}(c|b,m)$ is to output the most probable value $g(a,b)$ given Alice's message m pertaining to an encoding $\mathcal{E}$ and his input b. The right-hand side of (A3) can be interpreted as the convex combination of elements $(\sum_a p(a,b) p_{\mathcal{E}}(m|a))$ with the weightage $p_{\mathcal{D}}(c|b,m)$ for each pair of b,m. This in turn implies that for a fixed encoding strategy Bob's optimal decoding strategy $\mathcal{D}^*$ is deterministic, i.e.,

$$p_{\mathcal{D}^*}(c|b,m) = \begin{cases} 1, & \text{if } \sum_{a|g(a,b)=c} p(a,b) p_{\mathcal{E}}(m|a) \geqslant \sum_{a|g(a,b)\neq c} p(a,b) p_{\mathcal{E}}(m|a), \\ 0, & \text{else.} \end{cases} \tag{A5}$$

This allows us to reexpress (A3) as

$$p_{\mathrm{NC}} = \max_{\mathcal{E}} \left\{ \sum_m \sum_b p(b) \max_c \left(\sum_a p(a|b) p_{\mathcal{E}}(m|a) \delta_{c,g(a,b)} \right) \right\}. \tag{A6}$$

Encoding in an OC task: For any classical encoding strategy $\mathcal{E}$ define a set of non-negative parameters $\{q_{\mathcal{E},m}(a_1,a_2) := \frac{p(a_2|a_1) p_{\mathcal{E}}(m|a_1,a_2)}{p_{\mathcal{E}}(m)}\}$. It follows from the oblivious constraint (A4) that

$$\forall\, m, a_1, \ \sum_{a_2} q_{\mathcal{E},m}(a_1,a_2) = 1. \tag{A7}$$

Using the additional condition $p(a_2|a_1, b) = p(a_2|a_1)$ we may now rewrite (A6) in terms of $q_{\mathcal{E},m}(a_1, a_2)$ as

$$p_{\mathrm{NC}} = \max_{\mathcal{E}} \left\{ \sum_m p_{\mathcal{E}}(m) \sum_b p(b) \max_c \left\{ \sum_{a_1,a_2} p(a_1|b) q_{\mathcal{E},m}(a_1, a_2) \delta_{c,g(a,b)} \right\} \right\}$$
$$\leqslant \max_{\{q_{a_1,a_2}\}} \left\{ \sum_b p(b) \max_c \left\{ \sum_{a_1,a_2} p(a_1|b) q_{a_1,a_2} \delta_{c,g(a,b)} \right\} \right\}. \tag{A8}$$

The last inequality is implied by the fact that $\sum_m p_{\mathcal{E}}(m) = 1$. Specifically, the last inequality states that in order to obtain an upper bound on p_{NC} its enough to find the optimal encoding strategy $\mathcal{E}^*$ for a single level of the message, which justifies the use of the symbol q_{a_1,a_2}. The constraint (A7) along with the fact that $\forall\ a_1, a_2,\ q_{a_1,a_2} \geqslant 0$ implies that the set of all valid instances of q_{a_1,a_2} form a convex polytope. Since the "max" function is convex, hence with regard to find a upper bound on p_{NC} it is sufficient to evaluate the expression (A8) at the extremal points of that polytope and find the optimal. ■

Lemma 8: The set of valid assignments of $\{q_{a_1,a_2}\}$ satisfying the linear constraints (A2) form a convex polytope. The extremal points of this polytope resemble deterministic probability distributions, i.e., any extremal point $\{q^{\mathrm{ext}}_{a_1,a_2}\}$ is of the following form: for each a_1, $q^{\mathrm{ext}}_{a_1,a_2} = 0$ for all values of a_2 except a specific $\tilde{a}_2$ for which $q^{\mathrm{ext}}_{a_1,\tilde{a}_2} = 1$.

Proof. Let us represent the variables by a $n_{a_1} \times n_{a_2}$ matrix whose (a_1, a_2)th element is q_{a_1,a_2}. Since $\sum_{a_2} q_{a_1,a_2} = 1$, each row of such matrix sums to 1. The extremal points are described as follows. We consider a string $(e_0, e_1, \ldots, e_{n_{a_1}-1})$ where $e_{a_1} \in \{0, \ldots, n_{a_2} - 1\}$. Each extremal matrix is defined by this string such that $q_{a_1,a_2} = \delta_{a_2,e_{a_1}}$. There are $n_{a_2}^{n_{a_1}}$ number of such strings and each corresponds to an extremal point. One can check that any arbitrary matrix whose elements are $\tilde{q}_{a_1,a_2}$ can be obtained by the convex combination of these extremal points, in which the coefficient of the matrix corresponds to the string $(e_0, e_1, \ldots, e_{n_{a_1}-1})$ is $\prod_{i=0}^{n_{a_1}-1} \tilde{q}_{i,e_i}$. ■

Lemma 9: For a given quantum prepare and measure communication complexity protocol the following holds,

$$\chi \leqslant d p_G, \tag{A9}$$

where $\chi = \sum_{x,y} p(x, y) \operatorname{Tr}(M^y_{z=f(x,y)})$, d is dimension of the communicated system, and p_G is guessing probability without communication.

Proof. It is straightforward to see that, when there is no communication, given y the best strategy for Bob would be to output $f(x, y)$ which is more likely according to the prior probability of the inputs, i.e.,

$$p_G = \sum_y p(y) \max \left(\sum_{x|f(x,y)=0} p(x|y), \sum_{x|f(x,y)=1} p(x|y) \right).$$

By denoting $\chi^y_z = \operatorname{Tr}(M^y_z)$, and imposing the fact $\chi^y_0 + \chi^y_1 = d$, one obtains

$$\chi = \sum_{x,y} p(x, y) \chi^y_{z=f(x,y)}$$
$$= d \sum_y p(y) \left(\sum_{x|f(x,y)=0} p(x|y) \frac{\chi^y_0}{d} + \sum_{x|f(x,y)=1} p(x|y) \frac{\chi^y_1}{d} \right)$$
$$\leqslant d \sum_y p(y) \max \left(\sum_{x|f(x,y)=0} p(x|y), \sum_{x|f(x,y)=1} p(x|y) \right)$$
$$= d p_G.$$

■

Lemma 10: Given a CC problem and a protocol using a two-leveled classical message with a success probability $p_{\mathcal{C}_2}$, the success probability of a protocol using a d-leveled classical message is lower bounded in the following way:

$$p_{\mathcal{C}_d} \geqslant 1 - \exp\left[-\frac{1}{2p_{\mathcal{C}_2}} \log d \left(p_{\mathcal{C}_2} - \frac{1}{2} \right)^2 \right]. \tag{A10}$$

Proof. We have a communication complexity protocol $\mathcal{P}$ which uses a bit of communication to obtain a success probability of $p_{\mathcal{C}_2}$. Now, we shall use the *pumping argument* to discern the desired thesis (A10). Consider yet another protocol $\mathcal{P}'$ wherein Alice and Bob repeat protocol $\mathcal{P}$ $\log d$ times. They produce as their final outcome the majority of outcomes obtained in $\log d$ runs of $\mathcal{P}$. If $\lceil \log d \rceil$ is even they succeed if $\mathcal{P}$ succeeds $\lceil \frac{\log d}{2} \rceil + 1$ times, and if $\lceil \log d \rceil$ is odd they succeed if $\mathcal{P}$ succeeds $\lceil \frac{\log d}{2} \rceil$ times. Consider the event that the protocol $\mathcal{P}$ succeeds and the number of simultaneous occurrence of such event is captured in the variable τ. This allows us to lower bound $p_{\mathcal{C}_d}$ as

$$p_{\mathcal{C}_d} \geqslant p\left(\tau > \left\lceil \frac{\log d}{2} \right\rceil \right)$$
$$= \sum_{i=\lceil \frac{\log d}{2} \rceil + 1}^{\lceil \log d \rceil} \binom{\lceil \log d \rceil}{i} p^i_{\mathcal{C}_2} (1 - p_{\mathcal{C}_2})^{\lceil \log d \rceil - i}.$$

The right-hand side of the above equation is further lower bounded based on Chernoff's inequality as

$$p\left(\tau > \left\lceil \frac{\log d}{2} \right\rceil \right) \geqslant 1 - \exp\left(-\frac{1}{2p_{\mathcal{C}_2}} \log d \left(p_{\mathcal{C}_2} - \frac{1}{2} \right)^2 \right).$$

■

Lemma 11: Given a CC problem and a protocol which achieves a success probability p_S using $\mathcal{C}(f, p_S)$ bits, the success probability of a protocol using a two-leveled classical message is upper bounded in the following way:

$$p_{\mathcal{C}_2} \leqslant \frac{1}{2} + \sqrt{\frac{2p_S}{\mathcal{C}(f, p_S)}}. \tag{A11}$$

Proof. We have a communication complexity protocol which achieves success probability p_S using $\mathcal{C}(f, p_S)$ bits of

communication. We know from the *pumping argument* used in the proof for Lemma 4,

$$p_S \geqslant 1 - \exp\left[-\frac{1}{2p_{\mathcal{C}_2}}\mathcal{C}(f, p_S)\left(p_{\mathcal{C}_2} - \frac{1}{2}\right)^2\right].$$

Now expanding the above exponential term in the above inequality and taking the first two terms one retrieves

$$p_S \geqslant \left[\frac{1}{2p_{\mathcal{C}_2}}\mathcal{C}\left(f, p_S\right)\left(p_{\mathcal{C}_2} - \frac{1}{2}\right)^2\right].$$

This is conveniently reexpressed as

$$\frac{2p_S}{C(f, p_S)} \geqslant \frac{(p_{\mathcal{C}_2} - \frac{1}{2})^2}{p_{\mathcal{C}_2}} \geqslant \left(p_{\mathcal{C}_2} - \frac{1}{2}\right)^2,$$

where the second inequality follows from the observation that $0 \leqslant p_{\mathcal{C}_2} \leqslant 1$ and subsequently yields the desired thesis (A11). ■

Lemma 12: For hidden matching problem an OC task can be constructed with a success probability p_{NC}, such that $p_{\mathcal{NC}} \leqslant p_{\mathcal{C}_2}$.

Proof. In the hidden matching task, Alice is given a bit string $x \in \{0, 1\}^n$ of length n and Bob is given $y \in M_n$ where M_n denotes the family of all possible perfect matchings on n nodes. Their goal is to output a tuple $z = (i, j, t)$ such that the edge (i, j) belongs to the matching y and $t = x_i \oplus x_j$. Being a relational problem, given an input (x, y), Bob's task is to return z from a set of possible relations, i.e., $R(x, y) = \{(i, j, t)\}$ such that $(i, j) \in y$ and $t = x_i \oplus x_j$. Subsequently, the success probability is given by $\sum_{x,y} p(x, y) \sum_{z \in R(x,y)} p(z|x, y)$, and in classical communication with two-dimensional system

$$p_{\mathcal{C}_2} = \max_{\{E\}\{D\}} \sum_{m=0}^{1} \sum_{y} p(y) \left(\sum_{x, z \in R(x,y)} p(x|y) p_E(m|x) p_D(z|y, m) \right). \tag{A12}$$

We follow the same construction of the OC task described in Fig. 1. The corresponding OC is also a relational problem in which

$$g(a, b) = \begin{cases} R(x, y) & \text{for } a_2 = 0, \\ \tilde{R}(x, y) & \text{for } a_2 = 1, \end{cases}$$

where $\tilde{R}(x, y) = \{(i, j, 1 \oplus t)\}$ such that $(i, j) \in y$ and $t = x_i \oplus x_j$. In other words, the hidden matching task is unaltered in the case of $a_2 = 0$, while for $a_2 = 1$, Bob's objective is to output one edge (i, j) from the matching y together with the complement of their x or, i.e., $i \oplus j \oplus 1$. Following Lemmas 7 and 8 we first state the expression as given in (6),

$$\begin{aligned} p_{\mathrm{NC}} &= \max_{\{\mathcal{E}\}\{\mathcal{D}\}} \left\{ \sum_m \sum_b p(b) \right. \\ &\quad \left. \times \left(\sum_{a, c \in g(a,b)} p(a|b) p_{\mathcal{E}}(m|a) p_{\mathcal{D}}(c|b, m) \right) \right\} \\ &\leqslant \sum_b p(b) \sum_{a_1, a_2} p(a_1|b)\, \delta_{e_{a_1}, a_2}\, \Delta_{c_b, g(a,b)}\,, \end{aligned} \tag{A13}$$

where $\Delta_{c_b, g(a,b)} = 1$ if $c_b \in g(a, b)$, otherwise 0. Recall that in the proposed OC task $a_1 = x,\ b = y,\ c = (i, j, t)$. Subsequently, by denoting $c_y = (i^*, j^*, t^*)_y$ we rewrite the above expression of p_{NC}:

$$\begin{aligned} p_{\mathrm{NC}} &\leqslant \sum_y p(y) \sum_{x|e_x=0, (i^*,j^*,t^*)_y \in R(x,y)} p(x|y) \\ &\quad + \sum_y p(y) \sum_{x|e_x=1, (i^*,j^*,t^*)_y \in \tilde{R}(x,y)} p(x|y). \end{aligned} \tag{A14}$$

Further, consider the following classical strategy employing two-leveled message $m \in \{0, 1\}$,

$$p_E(m|x) = \delta_{m, e_x}\,,\ p_D(i, j, t|y, m) = \delta_{(i,j,t),(i^*,j^*,m \oplus t^*)_y}\,.$$

Inserting this strategy in (A12), and using the following feature of hidden matching problem,

$$\forall\, y, (i, j, t), \quad \sum_{x|(i,j,1\oplus t) \in R(x,y)} p(x|y) = \sum_{x|(i,j,t) \in \tilde{R}(x,y)} p(x|y),$$

one obtains the same expression of success probability in CC problem as given in the right side of (A14):

$$\begin{aligned} p_{\mathcal{C}_2} &\geqslant \sum_y p(y) \sum_{x|m=0, (i^*,j^*,t^*)_y \in R(x,y)} p(x|y) \\ &\quad + \sum_y p(y) \sum_{x|m=1, (i^*,j^*,1\oplus t^*)_y \in R(x,y)} p(x|y) \\ &= \sum_y p(y) \sum_{x|m=0, (i^*,j^*,t^*)_y \in R(x,y)} p(x|y) \\ &\quad + \sum_y p(y) \sum_{x|m=1, (i^*,j^*,t^*)_y \in \tilde{R}(x,y)} p(x|y) \\ &\geqslant p_{\mathrm{NC}}. \end{aligned}$$

Note that to show the quantum advantage in the OC task, we consider the same quantum strategy as described in Result 1 which leads to $p_{\mathcal{Q}} = \frac{1}{d}(2p_{\mathcal{Q}_d} + d - 1 - \chi)$ where $\chi = \sum_{x,y,z \in R(x,y)} p(x, y) \operatorname{Tr}(M_z^y)$. Subsequently, one can show the validity of Corollary 3. ■

[1] *Quantum Theory: Informational Foundations and Foils*, edited by G. Chiribella, and R. W. Spekkens (Springer, Dordrecht, 2016).

[2] A. Cabello, in *What is Quantum Information?* edited by O. Lombardi, S. Fortin, F. Holik, and C. Lpez (Cambridge University Press, 2017), pp. 138–144.

[3] R. W. Spekkens, Phys. Rev. A **71**, 052108 (2005).

[4] R. W. Spekkens, D. H. Buzacott, A. J. Keehn, B. Toner, and G. J. Pryde, Phys. Rev. Lett. **102**, 010401 (2009).

[5] D. Saha, P. Horodecki, and M. Pawlowski, arXiv:1708.04751.

[6] A. Hameedi, A. Tavakoli, B. Marques, and M. Bourennane, Phys. Rev. Lett. **119**, 220402 (2017).

[7] To avoid confusion, note that, communication tasks' referred in [6] are solely based on oblivious constraints. In

this paper, we call the same as oblivious communication tasks.

[8] A. C. Yao, in *Proceedings of the Eleventh Annual ACM Symposium on Theory of Computing* (ACM, New York, 1979), p. 209.

[9] E. Kushilevitz and N. Nisan, *Communication Complexity* (Cambridge University Press, Cambridge, UK, 2006).

[10] G. Brassard, Found. Phys. **33**, 1593 (2003).

[11] R. de Wolf, Theor. Comput. Sci. **287**, 337 (2002).

[12] R. Raz, in *Proceedings of the 31st Annual ACM Symposium on Theory of Computing* (ACM, New York, 1999), p. 358.

[13] H. Buhrman, R. Cleve, S. Massar, and R. de Wolf, Rev. Mod. Phys. **82**, 665 (2010).

[14] H. Buhrman, R. Cleve, and A. Wigderson, in *Proceedings of 30th Annual ACM Symposium on Theory of Computing* (ACM, New York, 1998), p. 63, arXiv:quant-ph/9802040.

[15] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf, Phys. Rev. Lett. **87**, 167902 (2001).

[16] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Rev. Mod. Phys. **86**, 419 (2014).

[17] J. S. Bell, Rev. Mod. Phys. **38**, 447 (1966).

[18] M. S. Leifer and M. Pusey, Proc. R. Soc. A **473**, 20160607 (2017).

[19] H. Buhrman *et al.*, Proc. Natl. Acad. Sci. USA **113**, 3191 (2016).

[20] A. Tavakoli, M. Pawłowski, M. Zukowski, and M. Bourennane, Phys. Rev. A **95**, 020302(R) (2017).

[21] A. Hameedi, D. Saha, P. Mironowicz, M. Pawlowski, and M. Bourennane, Phys. Rev. A **95**, 052345 (2017).

[22] M. Junge *et al.*, Commun. Math. Phys. **300**, 715 (2010).

[23] O. Regev, and B. Klartag, Proceedings of the 43rd Annual ACM Symposium on Theory of Computing (ACM, New York, 2011), p. 31.

[24] Z. B.- Yossef, T. S. Jayram, and I. Kerenidis, in *Proceedings of the 36th Annual ACM Symposium on Theory of Computing* (ACM, New York, 2004), p. 128.

[25] G. Chiribella and C. M. Scandolo, arXiv:1608.04459.

[26] A. Ambainis, D. Leung, L. Mancinska, and M. Ozols, arXiv:0810.2937.

[27] M. F. Pusey, Phys. Rev. A **98**, 022112 (2018).

[28] Č. Brukner, M. Żukowski, J.-W. Pan, and A. Zeilinger, Phys. Rev. Lett. **92**, 127901 (2004).

[29] S. Laplante *et al.*, Quantum **2**, 72 (2018).

[30] C. Crepeau, Equivalence between two flavours of oblivious transfer, *Advances in Cryptology: CRYPTO '87*, Vol. 293 of Lecture Notes in Computer Science (Springer, Berlin, 1988), pp. 350–354.

[31] C. H. Bennett, G. Brassard, C. Crépeau, and M.-H. Skubiszewska, Practical quantum oblivious transfer, *Advances in Cryptology-CRYPTO'91*, Lecture Notes in Computer Science Vol. 576 (Springer, Berlin, 1991) p. 351.

[32] A. Ch.-Ch. Yao, *27th Annual Symposium on Foundations of Computer Science (FOCS)* (IEEE, Piscataway, NJ, 1986), p. 162–167.

[33] M. Pawłowski *et al.*, Nature (London) **461**, 1101 (2009).