State independent contextuality advances one-way communication

Debashis Saha,1 Paweł Horodecki,2 and Marcin Pawłowski1

1Institute of Theoretical Physics and Astrophysics, National Quantum Information Centre, Faculty of Mathematics, Physics and Informatics, University of Gdańsk, 80-952 Gdańsk, Poland
2Faculty of Applied Physics and Mathematics, National Quantum Information Center, Gdańsk University of Technology, 80-233 Gdańsk, Poland

Despite ‘quantum contextuality’ being one of the most fundamental non-classical features, its generic role in information processing and computation is an open quest. This article shows that quantum contextuality is a potential resource for communication. We introduce a general framework of one-way oblivious communication (OC) tasks in which certain information about the sender’s input should be secure. A methodology for obtaining an upper bound on the success of the tasks in classical communication is provided. Particularly, we study a family of OC tasks based on Kochen-Specker (KS) sets of vectors and show that quantum strategy corresponding to every KS set outperforms classical communication of arbitrarily large dimensional system. The quantum advantage is extended to the state independent contextuality (SIC) proofs that go beyond KS argument. The optimal classical protocols for the simplest SIC sets in dimension three and four are explicitly derived. Our results provide an operational significance to single system SIC and open up the possibility of quantum information processing based on that.

I. INTRODUCTION

The seminal works by Bell-Kochen-Specker [1–3] show that objective reality of sharp values of quantum observables cannot be independent of the measurement context. The Kochen-Specker (KS) reasoning of contextuality stands on the incompatibility of noncontextual assignment of binary values to a set of projectors. The general approach to test state independent contextuality (SIC) is based on an inequality consisting of experimentally observed quantities. All noncontextual models satisfy this inequality, while the quantum predictions for any state of certain dimension violate it [4–6]. Despite of being one of the most fundamental non-classical features, the generic role of quantum contextuality in information processing and computation is far from settled. Many attempts have been made to answer this question in multiple directions. For instance, it is shown that some aspects of quantum computation reveal contextuality [7–9]; contextual correlations are also valuable in several information processing [10–14] and originates novel applications of quantum nonlocality [15–20].

In this article, we provide a new perspective to quantum contextuality by showing every proof of KS contextuality gives an advantage over classical system in communication. We introduce a family of one-way communication tasks, which we refer to as vertex equality problem, based on the orthogonal graph of every SIC set. We consider two different scenarios: (I) communication in bounded dimension where the dimension of the communicated system (classical or quantum) is restricted, and (II) oblivious communication upon the constraint that certain information about the sender’s input is not revealed in communication. In the former, it is shown that, for every SIC set, quantum communication provides an advantage over classical. The later contributes to the central result of this article. We first demonstrate a general framework for oblivious communication (OC) and provide a method to obtain classical optimal bounds. We show that quantum strategies based on each KS set always outperforms classical communication. Significantly, OC does not impose restriction on the dimensional of the communicated system. This implies that even unbounded classical resource cannot reproduce quantum contextual statistics satisfying certain oblivious conditions. We explicitly derive the optimal classical strategies for Cabello-Estebaranz-GarciaAlcaine (CEG-18) [21] and Yu-Oh (YO-13) [5] vector sets in both the aforementioned scenarios. However, we provide the general analytical expression for the same applicable to any SIC set. The robustness of quantum communication against white noise is studied. Finally, we show that any advantage over classical channel in OC implies preparation contextuality. Our results suggest that, any SIC set can be a resource in semi-device independent quantum key distribution [22], randomness generation [23] and other information processing.

II. COMMUNICATION TASKS

In general, a one-way communication task involves a sender (Alice) and a receiver (Bob). In each round of the task Alice receives an input $x$ from a set $\{x\}$ and sends a message (classical or quantum) to Bob. Bob receives input $y$ from a set $\{y\}$ and is required to guess $f(x, y)$. Bob’s answer is encoded in an output variable $z$. In this article, we deal with the communication tasks where $f(x, y)$ is binary, i.e., $z \in \{0, 1\}$. We assume that the inputs $x, y$ are uniformly distributed. Let $p(z|x, y)$ represent the probability of obtaining an output $z$ given inputs $x, y$. Any figure of merit, i.e., the guessing probability of $f(x, y)$, of the communication problem can be considered as a linear function of these observed proba-
biabilities. For convenience, one can always normalize the figure of merit such that it takes value within [0, 1]. Thus, any figure of merit is expressed as,

\[ S = \sum_{x,y} t(x,y)p(z = f(x,y)|x,y), \quad (1) \]

where \( t(x,y) \geq 0, \sum_{x,y} t(x,y) = 1 \). Here \( t(x,y) \) can be interpreted as the normalized weightage for inputs \( x,y \). Two distinct scenarios have been taken in account for carrying out the communication task. We now illustrate these.

**Communication in bounded dimension.** In this scenario, the dimension of the communicated system is bounded. In other words, for classical channel, the communicated message from Alice (say \( \tau \)) can be \( d \) distinct levels \( \{1,\ldots,d\} \). Depending on the received message and the input \( y \), Bob provides his answer \( z \). While in the case of quantum channel, the communicated quantum state, say \( \rho_x \), should belong to \( d \)-dimensional Hilbert space. And subject to his input \( y \), Bob performs a measurement on the communicated system and returns the measurement outcome \( z \). The advantages of quantum communication in bounded dimension have been extensively explored within the scope of quantum communication complexity [24, 25] and dimension witness of quantum system [26, 27].

**Oblivious communication.** On the contrary, OC task with quantum resources is mostly unexplored. In OC, there is no restriction on the dimension of the communicated system. Instead, we impose secrecy to certain information in the communication. Let us first provide a general framework for OC (see Fig. 1). Here, Alice’s input \( x \) comes through a local channel described by the conditional probability \( p(x|w) \) where \( w \) is the input variable of that channel. The communication is unbounded. The only condition is that the information about \( w \), referred as the oblivious variable, should not be revealed in the communication including Bob.

![Fig. 1: Oblivious communication problem between a sender (Alice) and a receiver (Bob) who receive inputs \( x \) and \( y \) respectively. Alice’s input \( x \) comes through a local channel whose input variable is \( w \). Alice communicates arbitrary large number of classical messages \( \tau \) to Bob which do not contain any information about the oblivious variable \( w \). The goal is to guess \( f(x,y) \) with maximum probability.](image)

More formally, let us denote the classical message \( \tau \in \{1,\ldots,N\} \) where \( N \) can be arbitrary large, and Alice’s encoding strategy \( p_c(\tau|x) \) as the probability of sending a level \( \tau \) for input \( x \). Obviously, \( \forall x, \sum_{\tau} p_c(\tau|x) = 1 \). The oblivious condition implies Alice’s encoding strategy should be such that for all \( \tau, p_c(\tau|w) = \sum_z p(x|w)p_c(\tau|x) \) is independent of \( w \). Here, it suffices to consider the OC protocols without shared classical randomness. If Alice and Bob share a classical random variable \( r \), the oblivious constraint will imply, \( \forall \tau, r, p_c(\tau|w,r) = p_c(\tau|r) \). Using the fact that the input variable \( w \) is independent of \( r \), one obtains, \( \forall \tau, r, p_c(\tau,r|w) = p_c(\tau,r) \). As the dimension of the message can be arbitrarily large, we can include the shared randomness into a larger message \( \tau' = (\tau, r) \). This fact also suggests that whenever Alice’s encoding strategy is probabilistic, it should be realized using Alice’s local randomness and uncorrelated with any shared randomness. It is noteworthy that from the input \( x \) Alice has some (or full) information about \( w \), but the primary goal is to encode the input \( x \) efficiently in such a way that information about \( w \) should be utterly oblivious to any other party who does not have access to Alice’s lab.

In the case of quantum channel, for input \( x \) Alice sends a quantum state \( \rho_x \) which belongs to a Hilbert space of any dimension. The oblivious condition demands the effective quantum state (say \( \rho_w \)) is same for all \( w \), i.e., \( \forall w, \rho_w = \sum_z p(x|w)\rho_z \).

**Classical bound in oblivious communication.** Although any probabilistic encoding strategy which satisfies the oblivious constraints is a convex combination of deterministic strategies, but these deterministic strategies might not satisfy the oblivious constraints. Therefore, the general encoding strategy \( p_c(\tau|x) \) for Alice might not be deterministic. On the other hand, Bob receives input \( y \) and the message \( \tau \) from Alice. Let us denote Bob’s decoding strategy by \( p_d(z|y,\tau) \) that represents the probability of returning \( z \) given \( y, \tau \). For each \( y \), we define a set \( F_y^z \subset \{x\} \) such that \( f(x,y) = z \). The expression \( S \) in Eq.(1) can be simplified as follows,

\[ S = \sum_y \left( \sum_x t(x,y)p(z = f(x,y)|x,y) \right) \]

\[ = \sum_y \sum_{\tau} \left( \sum_{x \in F_y^z} t(x,y)p_c(\tau|x)p_d(0|y,\tau) \right. \]

\[ + \left. \sum_{x \in F_y^1} t(x,y)p_c(\tau|x)p_d(1|y,\tau) \right) \]

\[ \leq \sum_y \sum_{\tau} \max \left( \sum_{x \in F_y^0} t(x,y)p_c(\tau|x), \sum_{x \in F_y^1} t(x,y)p_c(\tau|x) \right) \quad (2) \]

The above observation implies, given any encoding strategy the optimal decoding strategy for Bob is fixed and deterministic, i.e.,

\[ p_d(0|y,\tau) = \begin{cases} 1, & \text{if } \sum_{x \in F_y^1} t(x,y)p_c(\tau|x) \geq \sum_{x \in F_y^0} t(x,y)p_c(\tau|x) \\ 0, & \text{if } \sum_{x \in F_y^1} t(x,y)p_c(\tau|x) < \sum_{x \in F_y^0} t(x,y)p_c(\tau|x) \end{cases} \]

\[ (3) \]
Further, we know from the oblivious condition that, \( p_e(\tau|w) = \sum_x p(x|w)p_e(\tau|x) \), is same for all \( w \). We seek to maximize the quantity on the right hand side of (2) under the following linear constraints:

\[
\forall x, \sum_{\tau} p_e(\tau|x) = 1 \quad (4a)
\]

\[
\forall \tau, w, \ p_e(\tau) = p_e(\tau|w) = \sum_x p(x|w)p_e(\tau|x). \quad (4b)
\]

By defining \( q_x^\tau = \frac{p_e(\tau|x)}{p_e(\tau)} \), we find Eq. (2) can be expressed as follows,

\[
S \leq \sum_{\tau} p_e(\tau) \left( \sum_y \max \left[ \sum_{\tau \in F_y^0} t(x,y)q_x^\tau, \sum_{\tau \in F_y^1} t(x,y)q_x^\tau \right] \right). \quad (5)
\]

Eq. (4a) and Eq. (4b) lead to,

\[
\sum_{\tau} p_e(\tau) = \sum_x p(x|w) \left( \sum_{\tau} p_e(\tau|x) \right) = 1. \quad (6)
\]

Hence, (5) can be interpreted as a convex combination of \( \chi_e(\tau) \) with coefficient \( p_e(\tau) \). This observation leads to the fact that \( S \) is bounded by the maximum value of \( \chi_e(\tau) \), i.e.,

\[
S \leq \sum_y \max \left[ \sum_{\tau \in F_y^0} t(x,y)q_x^\tau, \sum_{\tau \in F_y^1} t(x,y)q_x^\tau \right]. \quad (7)
\]

Note that, the above expression is independent of the number of \( \tau \). Coming back to variables \( q_x \), it follows from (4b) that \( q_x \) satisfies the following constraints,

\[
\forall x, \ q_x \geq 0; \ \forall w, \sum_x p(x|w)q_x = 1. \quad (8)
\]

Consequently, the upper bound of \( S \) in a classical OC task reduces to the maximum value of the right hand side of (7) under the constraints (8). In a nutshell, this method simplifies the optimization problem from arbitrarily large number of \( \tau \) to a single one. It is worthy noting that (7) provides an upper bound which might not be tight since (4b) has not been imposed for all \( \tau \).

The variable \( q_x \) satisfying (8) forms a polytope and one can obtain the extremal points of that polytope by simple linear programming. The optimal value of the right hand side of (7) can be obtained by evaluating the expression at these extremal points of the polytope. It follows from the following reason: by choosing \( \sum_{\tau \in F_y^0} t(x,y)q_x \) or \( \sum_{\tau \in F_y^1} t(x,y)q_x \) for each \( y \), a list of \( 2|y| \) linear functions can be obtained where \( |y| \) is the cardinality of the set \( \{ y \} \). The maximum value of right hand side of (7) is the maximum value of those \( 2|y| \) number of linear functions. Since the ‘max function’ of two linear functions is a convex function, it suffices to check its value by considering all the extremal points of the polytope.

**Remark.** The OC problem is a generalization of oblivious transfer which serves as a primitive for several classical and quantum cryptographic protocols [28–31]. Communications with oblivious constraints are important when some part of the sender’s data should be kept secure. It has been shown that preparation contextuality, another specific type of quantum contextuality proposed by Spekkens [32], is useful in parity oblivious random access code [10]. Parity oblivious multiplexing can be interpreted as a particular case of the above general framework. In oblivious multiplexing, the oblivious variable \( w \), that is, the parity of a set of input bits is a function of the input \( x \). While the approach in [10] to obtain the classical bound is applicable to random access code, the proposed method is universal and essentially reduces the optimization for a single message from arbitrarily large number of messages. Later, we generalize the ontological implication [10] that any advantage in OC reveals preparation contextuality.

### III. VERTEX EQUALITY PROBLEM

For simplicity, we consider SIC set consisting of only rank one projectors. A SIC set may contain projectors with rank more than one, but one can always split that projector into many rank-one projectors. The modified SIC set of vectors retain the same contextual property as before. For every SIC set of vectors, one can associate a graph \( G(V,E) \) where each vertex corresponds to a vector, and two vertices are adjacent if the corresponding vectors are orthogonal. This is known as orthogonal graph. We denote the total number of vertices, i.e., the order of graph \( G \), by \( |G| \). The neighborhood of a vertex \( v \in V \), denoted by \( N_v \), is the induced subgraph of \( G \) consisting all the adjacent vertices of \( v \). Thus, \( |N_v| \) for a SIC graph is the number of orthogonal vectors to \( v \). Let us refer \( d \) as the minimum dimension of the Hilbert space in which the SIC graph \( G \) can be non-trivially realized satisfying all the orthogonal relations faithfully.

The communication problem based on SIC graph \( G \) is defined as follows: Alice and Bob receive input from the vertex set of \( G \), i.e., \( x, y \in \{1, ..., |G|\} \), and the aim is to guess whether \( x = y \) or \( x \neq y \) encoded by \( z = 0 \) or \( 1 \) respectively. While we are only interested in those run in which \( y \) is connected or equal to \( x \) in the graph. In other words, \( t(x,y) \) is non-zero if and only if \( y \in \{ N_x, x \} \). As an equality problem where the inputs belong to the vertices of SIC graph, we call this task vertex equality problem.

#### A. Vertex equality problem in bounded dimension

First, we consider a scenario with the constraint that the dimension of the system (classical or quantum) com-
municated by Alice is bounded by $d$. For simplicity, $t(x, y)$ is taken to be uniform, and hence we seek to maximize,  

$$S = \sum_{x \neq y} t(x, y)p(0|x, y) + \sum_{y \in N_x} t(x, y)p(1|x, y),$$

where $t(x, y) = \frac{1}{N}$, $N = \sum_x |N_x| + |G|$. \hspace{1cm} (9)  

**Proposition 1.** For the vertex equality problem in bounded dimension the maximum value of $S$, i.e. one, can be achieved in quantum communication. While for the classical system the optimal bound for $S$ is given by,  

$$S \leq 1 - \frac{2\kappa}{N} \hspace{1cm} (10)$$

which is strictly less than one. Here $\kappa$ is the minimum number of edges whose adjacent vertices are assigned the same color when maximum $d$ colors are used to color all the vertices in $G$.

**Proof.** The quantum strategy which yields the maximum value of $S$ is straightforward. Alice prepares $d$-dimensional quantum state, $\rho_x = |x\rangle \langle x|$ for input $x$ that corresponds to the vector associated with the vertex $x$, and sends to Bob. For input $y$ Bob performs a binary outcome measurement $\{P^0_y, P^1_y\}$ on the received system $\rho_x$, where $P^0_y = \rho_y = |y\rangle \langle y|, P^1_y = I - \rho_y$. It is clear from the construction of SIC graph that $\rho_x$ has full support in $I - \rho_y$ if $x \in N_y$. Thus, the quantum strategy always yields the correct answer.

In the classical communication, without loss of generality, we can assume that there exists a deterministic encoding and decoding strategy that yields the maximum value of $S$. Alice sends one of $d$ levels for each input $x$ which is equivalent to assign one of $d$ colors to each vertex of $G$. Alice’s encoding for an input $x$ is ‘perfectly colored’ if all the colors assigned to adjacent vertices are different from the color assigned to $x$. From Eq.(9), we know that the relevant turns are those where Bob receives input $y \in \{N_x, x\}$. So, if Alice’s encoding for $x$ is not perfectly colored, then for any possible deterministic decoding strategy, there exists at least one input $y \in \{N_x, x\}$ for which Bob’s answer will be wrong. We know, it is not possible to perfectly color all $x$, since the chromatic number of any SIC graph is strictly greater than $d$ [33, 34]. Hence, the value of $S$ is strictly less than one. In fact, this is true for non-uniform values of $t(x, y)$.

Now, if the graph is not perfectly colored, then there will be some edge whose adjacent vertices are assigned the same color. Let us call such edge as ‘improper edge’. If an ‘improper edge’ connects vertices $x_1, x_2$, then there will be at least two turns among the inputs $\{(x_1, x_2), (x_2, x_1), (x_1, x_1), (x_2, x_2)\}$, in which Bob guesses the wrong answer. Here $(x, y)$ denotes the respective input for Alice and Bob. Moreover, noting the fact that $t(x, y)$ is uniform Eq.(9), the optimal Alice’s encoding strategy is to color all the vertices with $d$ colors such that the ‘improper edge’ is minimum. Thus, we obtain the optimal value of $S$ is given by (10).

One may quantify the quantum advantage as the difference between the dimensions of the system to accomplish vertex equality task perfectly in classical and quantum communication. For classical system, the minimum dimension required to achieve $S = 1$ is the chromatic number of the graph which is greater than $d$ for any SIC graph. It is also noteworthy that, **Proposition-1** is valid for any graph that possesses higher chromatic number than the minimum dimension of Hilbert space required to realize the graph.

A simplified version of SIC graph of CEG-18 and YO-13 are given in Figure 3 and 4. It can be checked that the independence number of CEG-18 graph is four. Thus

![FIG. 2: Vertex equality problem in bounded dimension. Alice receives an input $x$ from the vertex set of SIC graph $G$ and communicates a system to Bob. Bob obtains input $y$ from the same set and returns a binary outcome to guess if $x = y$ or not. The relevant runs are those where $y \in \{N_x, x\}$. The dimension of the communicable system is bounded by $d$, where $d$ is the minimum dimension of the Hilbert space in which the SIC graph $G$ is non-trivially realized.](image)

![FIG. 3: A simplified version of the orthogonal graph of CEG-18 set of vectors. Each vertex corresponds to a vector. Six edges of the heptagon and the three dashed rectangles connecting four vertices form the basis ($d$-clique). Each vector belongs to two different basis and orthogonal to six other vectors. The optimal classical strategy is also shown by assigning four distinct levels $\{A, B, C, D\}$ to all vertices. The assigned colors to the vertices $v_{16}$ and $v_{17}$ are already used for one of their adjacent vertices. Thus, there are two improper edges connecting $v_{13}, v_{16}$ and $v_{15}, v_{17}$.](image)
with four colors, 16 vertices can be properly colored and $\kappa$ can be at least 2. In Fig. 3 a graph coloring is shown with $\kappa = 2$. While for YO-13 vectors, $\kappa = 1$ (Fig. 4).

The general framework of OC problem was presented in section II. For the purpose of this article, here we consider a simplified situation where the oblivious variables $w$ corresponds to subsets of the input set $\{x\}$, and Alice does not want to reveal information about the subsets to which her input $x$ belongs. More formally, consider $K$ possible oblivious variables $w_i (i \in \{1, ..., K\})$ such that for each $i$, there exists a set $\Omega_i \subset \{x\}$ for which $p(x|w_i)$ is uniform if $x \in \Omega_i$, otherwise 0. So, each $w_i$ has one to one correspondence with a set $\Omega_i$, and $p(x|w_i) = 1/|\Omega_i|$ where $|\Omega_i|$ is the cardinality of $\Omega_i$.

The graph of a clique is a subset of vertices such that each pair of them are connected by edge. The maximum clique, i.e., a clique with maximum number of vertices, has $d$ elements for a SIC graph. If some vertices do not belong to maximum clique (or $d$-clique), then we consider extended SIC graph $G^e$ with additional vertices such that each vertex belongs to at least one $d$-clique. In other words, we include additional vectors in SIC set such that each vector belongs to some basis. Same as the vertex equality task (Fig. 5), here Alice and Bob receive input $x$ and $y$, respectively, from the vertex set $\{1, 2, ..., |G^e|\}$ and want to guess if $x$ and $y$ are the same or not. The oblivious variable $w_i$ corresponds to a set of vertices $\Omega_i \subset \{1, 2, ..., |G^e|\}$ forms a $d$-clique. Thus, each $\Omega_i$, representing a maximum clique of $G^e$, contains $d$ elements, and $K$ is the total number of $d$-cliques in $G^e$. Such oblivious constraints, referred as clique-oblivious condition, imply no information can be communicated about the maximum clique (\(\Omega_i\)) to which input $x$ belongs. More precisely, for the inputs belong to different $d$-cliques, the statistics on the effective communicated system of all possible measurements should be the same. Consequently, the effective constraints on classical and quantum communication, are as follows:

$$\forall \tau, \ p(\tau|w) = \frac{1}{|\Omega_1|} \sum_{x \in \Omega_1} p_x(\tau|x) = \ldots = \frac{1}{|\Omega_K|} \sum_{x \in \Omega_K} p_x(\tau|x);$$

$$\rho_w = \frac{1}{|\Omega_1|} \sum_{x \in \Omega_1} \rho_x = \ldots = \frac{1}{|\Omega_K|} \sum_{x \in \Omega_K} \rho_x. \ \ (11)$$

Under clique-oblivious conditions, Alice and Bob seek to maximize the following quantity,

$$S = \sum_{x, y \in \mathcal{N}_x} t(x, y)p(0|x, y) + \sum_{x, y \in \mathcal{N}_y} t(x, y)p(1|x, y),$$

taking $t(x, y) = \frac{n_x}{N}$, $N = \sum_{i=1}^{K} |\Omega_i|$, $n_x = \frac{m_x}{|\mathcal{N}_x|+t}$, \ (12)

where $m_x$ is the number of sets ($\Omega_i$’s) in which $x$ appears, $|\mathcal{N}_x|$ is number of adjacent vertices of $x$, and for any KS set $|\Omega_i|$ is equal to $d$. Later, for YO-13 ray, we will consider additional $\Omega$ of different cardinality than $d$. Yet again, $y \in \{\mathcal{N}_x, x\}$ are the relevant cases for the figure of merit, but $t(x, y)$ is not uniform here.

The upper bound derived for a general OC tasks in Eq.(7)-(8) simplifies for the vertex equality problem (12) to,

$$S \leq \frac{1}{N} \sum_y \max_{y} \left( \frac{n_y q_y}{\mathcal{N}_y} \sum_{x \in \mathcal{N}_y} n_x q_x \right) \ \ (13)$$

where the variables $q_x$ satisfy the following conditions,

$$\forall x, q_x \geq 0; \ \forall i, \ \frac{1}{|\Omega_i|} \sum_{x \in \Omega_i} q_x = 1. \ \ (14)$$
Proposition 2: For the vertex equality problem based on any extended KS graph in clique-oblivious communication, quantum channel outperforms classical channel. Particularly, the value of $S$ is strictly less than one for classical systems, whereas it is one for quantum.

Proof. It can be readily verified that the same quantum strategy, comprising the encoding state $|x⟩⟨x|$ and decoding measurement $\{⟨y|y⟩, I−⟨y|y⟩\}$, mentioned in Proposition-1, produces the correct answer for all relevant inputs. By the construction of orthogonal graph, each maximum clique corresponds to some basis, resulting $ρ_w$ to be the maximally mixed state in dimension $d$. Therefore, this quantum strategy satisfies the clique-oblivious conditions.

For classical channel, let Alice sends some level $τ$, with a nonzero probability, for input $x$, i.e., $q_x > 0$. If there exists $x' ∈ N_x$, such that $q_{x'} > 0$, then either for input $(x,x')$ or $(x',x)$ there is non-zero probability that Bob guesses the wrong answer. Let us provide a rigorous explanation of this fact. By summing up over all the oblivious variables $i$ in (14), one obtains

$$\sum_i \sum_{x ∈ N_i} q_x = \sum_i |Ω_i| \implies \sum_x m_x q_x = N. \quad (15)$$

Using the above relation one may re-express (13) as follows,

$$S \leq \frac{1}{N} \sum_y \max \left( n_y q_y, \sum_{x ∈ N_y} n_x q_x \right),$$

$$= \frac{1}{N} \sum_y \left( n_y q_y + \sum_{x ∈ N_y} n_x q_x - \min \left( n_y q_y, \sum_{x ∈ N_y} n_x q_x \right) \right),$$

$$= \frac{1}{N} \sum_y m_y q_y - \frac{1}{N} \sum_y \min \left( n_y q_y, \sum_{x ∈ N_y} n_x q_x \right),$$

$$= 1 - \frac{1}{N} \sum_y \min \left( n_y q_y, \sum_{x ∈ N_y} n_x q_x \right). \quad (16)$$

Thus, the task is perfectly accomplished only if $\min(n_y q_y, \sum_{x ∈ N_y} n_x q_x) = 0$ for all $y$. This leads to the following observations.

Fact 1. If Alice sends $τ$ for input $x$, then $S = 1$ implies for all other inputs belong to $N_x$, Alice cannot communicate $τ$.

Fact 2. The clique-oblivious conditions implies that the probability of sending $τ$ for the inputs belonging to each clique is same. Therefore, in each $d$-clique there should be a unique input for which Alice sends $τ$ with the same probability $p_x(τ|x)$ to fulfill the oblivious constraints (11).

Consider an assignment of 0 or 1 to each vertex representing when Alice sends $τ$ for that input or not. Then Fact 1-2 suggests that we can assign 0 or 1 values to all vectors such that no two orthogonal vectors are assigned value 1 and exactly one vector in each basis is assigned 1. From the very definition of KS set, this implies contradiction.  

In the CEG-18 graph (Fig. 3), each vertex belongs to some maximum clique, so we do not need to consider an extended graph. The nine maximum cliques corresponds to the following oblivious variables,

$$Ω_1 = \{1, 2, 3, 4\}, Ω_2 = \{4, 5, 6, 7\}, Ω_3 = \{7, 8, 9, 10\},$$

$$Ω_4 = \{10, 11, 12, 13\}, Ω_5 = \{13, 14, 15, 16\},$$

$$Ω_6 = \{16, 17, 18, 19\}, Ω_7 = \{2, 9, 11, 18\},$$

$$Ω_8 = \{3, 5, 12, 14\}, Ω_9 = \{6, 8, 15, 17\}. \quad (17)$$

Proposition 3: The optimal classical value of $S$ is 20/21 for the clique-oblivious vertex equality problem based on CEG-18 vector.

Proof. Due to the elegant symmetry of CEG-18 set, $n_x = 2, |N_x| = 6$ for all $x$. Subsequently, Eq. (13) can be expressed as follows,

$$S \leq \frac{1}{126} \sum_{y} \max \left( q_y, \sum_{x ∈ N_y} q_x \right) \leq \frac{1}{126} \sum_{y} \max (q_y, 2 - 2q_y). \quad (18)$$

We use that fact that $\sum_{x ∈ N_y} q_x = 2\sum_{x ∈ Ω} q_x - q_y = 2 - 2q_y$. It follows from (14) and (17) that $q_x$ satisfies the following constraints,

$$∀x, q_x ≥ 0; q_1 + q_2 + q_3 + q_4 = q_4 + q_5 + q_6 + q_7 = q_7 + q_8 + q_9 + q_{10} = q_{10} + q_{11} + q_{12} + q_{13} = q_{13} + q_{14} + q_{15} + q_{16} = q_{16} + q_{17} + q_{18} + q_{19} = q_{2} + q_{18} + q_{9} + q_{11} = q_{3} + q_{5} + q_{12} + q_{14} = q_{6} + q_{8} + q_{15} + q_{17} = 4. \quad (19)$$

Therefore, one obtains the extremal points of the polytope of $q_x$ by simple linear programing. There are 146 extremal points. Following the argument given before, that the ‘max’ function of two linear functions is a convex function, the optimal value of the quantity $\sum_{x} \max(q_x, 2 - 2q_x)$ can be obtained from these extremal points of the polytope. So, one may easily retrieve the maximum value of $\sum_{x} \max(q_x, 2 - 2q_x) = 120$. The only way to realize it, is to assign 4 to three vertices and 2 to other three vertices. Thus, we establish $S ≤ \frac{120}{126} = \frac{20}{21}$. To show that the bound is tight, finally we provide a strategy in Fig. (6) using four levels that satisfies clique-oblivious conditions (14).  

YO-13 vector

First consider the extended YO-13 graph as shown in Fig. (7). In the extended YO-13 graph, there are 25 vertices and 16 maximum cliques corresponding to 16
oblivious variables,
\[
\begin{align*}
\Omega_1 &= \{1, 2, 3\}, \Omega_2 = \{1, 4, 5\}, \Omega_3 = \{2, 6, 7\}, \Omega_4 = \{3, 8, 9\}, \\
\Omega_5 &= \{5, 10, 14\}, \Omega_6 = \{6, 10, 15\}, \Omega_7 = \{7, 11, 16\}, \\
\Omega_8 &= \{8, 11, 17\}, \Omega_9 = \{9, 12, 18\}, \Omega_{10} = \{4, 12, 19\}, \\
\Omega_{11} &= \{5, 13, 20\}, \Omega_{12} = \{7, 13, 21\}, \Omega_{13} = \{9, 13, 22\}, \\
\Omega_{14} &= \{6, 12, 23\}, \Omega_{15} = \{8, 10, 24\}, \Omega_{16} = \{4, 11, 25\}.
\end{align*}
\]
Since it is not a KS set, apart from clique oblivious conditions, additionally we impose two more constraints, given by,
\[
\begin{align*}
\Omega_{17} &= \{4, 5, 6, 7, 8, 9\}, \Omega_{18} = \{10, 11, 12, 13\}.
\end{align*}
\]
Notice that, the following property is satisfied by the YO-13 set of vectors,
\[
\begin{align*}
\frac{1}{6} \sum_{i=4, 5, 6, 7, 8, 9} \Pi_i = \frac{1}{4} \sum_{i=10, 11, 12, 13} \Pi_i = \frac{1}{3},
\end{align*}
\]
Hence, the quantum strategy satisfies all the oblivious conditions and achieves the winning condition perfectly, that is, \( S = 1 \).

Proposition 4: The optimal classical value of \( S \) is 0.92 for the oblivious vertex equality problem based on extended YO-13 set.

Proof. We follow similar method demonstrated in Proposition-3. First, we simplify the expression in Eq.(13) as,
\[
S = \frac{1}{58} \sum_y \max_{x \in N_y} \left( n_yq_y, \sum_{x \in N_y} n_xq_x \right),
\]
where \( n_x = \begin{cases} 
2/5, & x \in \{1, 2, 3\} \\
4/7, & x \in \{4, ..., 13\} \\
1/3, & x \in \{14, ..., 25\}. 
\end{cases} \)
Imposing (20)-(22) on (14), we can infer that \( q_x \) satisfy the following constraints,
\[
\forall x, q_x \geq 0; \quad q_1 + q_2 + q_3 = q_1 + q_4 + q_5 = q_2 + q_6 + q_7 = q_3 + q_8 + q_9 = q_5 + q_{10} + q_{14} = q_6 + q_{10} + q_{15} = q_7 + q_{11} + q_{16} = q_8 + q_{11} + q_{17} = q_9 + q_{12} + q_{18} = q_4 + q_{12} + q_{19} = q_5 + q_{13} + q_{20} = q_7 + q_{13} + q_{21} = q_9 + q_{13} + q_{22} = q_6 + q_{12} + q_{23} = q_8 + q_{10} + q_{24} = q_4 + q_{11} + q_{25} = \frac{1}{2}(q_4 + q_5 + q_6 + q_7 + q_8 + q_9) = \frac{3}{4}(q_{10} + q_{11} + q_{12} + q_{13}) = 3.
\]
Subsequently, one gets the extremal points of the polytope of \( q_x \) by simple linear programming. In this case, there are 770 extremal points. Following the previous argument, the maximum value of \( \sum_{x} \max[q_x, \sum_{y \in N_y} n_yq_y] \) is 53.4 is obtained by considering all these extremal point. This leads to \( S \leq 0.92 \). Finally we provide an encoding in table (I) using twelve levels, each of which satisfies the oblivious conditions, thereby showing this bound is tight. \( \square \)
TABLE I: The probabilities of sending twelve levels \( \{A, B, ..., L\} \) for 25 different inputs are listed. The effective classical state is an equal mixture of twelve different levels. Considering the decoding strategy provided in (3), one can obtain \( S \approx 0.92 \).

C. Robustness in respect to white noise

We address the situation when the quantum channel is noisy. Precisely, the communicated quantum system is given by \( \mathcal{N}\psi\rangle\rangle + (1 - \nu)1/d \), where \( \nu \in [0,1] \) is the white noise parameter. Note that, this noisy quantum channel satisfies the oblivious constraints (11). Now, the observed probabilities are, \( p(x,y) = \nu + (1 - \nu)/d \) for \( x = y \), and \( p(1|x,y) = \nu + (1 - \nu)(d - 1)/d \) for \( y \neq x \). A simple calculation leads to the modified quantum values of \( S_q = \nu + (1 - \nu)/d = 1 \) for (9) and \( S_q = \nu + (1 - \nu)(\frac{d-1}{d} - \frac{\sum \nu_x(d-2)}{d}) \) for (12), in two different communication scenarios of bounded dimension and oblivious information, respectively. Thus, for the persistence of quantum violation, the following condition must hold:

(a) in communication with bounded dimension, 
\[
\nu > 1 - \frac{(1 - S_q)Nd}{N + (d - 2)|G|}, \quad \text{where} \quad N = \sum_x |N_x| + |G|;
\]

(b) in oblivious communication, 
\[
\nu > 1 - \frac{(1 - S_q)Nd}{N + (d - 2)\sum_x n_x}, \quad \text{where} \quad N = \sum_i |\Omega_i|.
\]

Here, \( S_q \) represents the classical optimal value. In the first scenario with bounded dimension, the threshold visibility for CEG-18 and YO-13 are 0.90 and 0.92 respectively. While, in the OC, the threshold visibility for CEG-18 and extended YO-13 are 0.85 and 0.80 respectively.

IV. ADVANTAGE IN OBLIVIOUS COMMUNICATION OVER CLASSICAL CHANNEL IMPLIES PREPARATION CONTEXTUALITY

The notion of preparation contextuality was proposed by Spekkens [32]. We point out that the classical bound for any OC problem is same as for any preparation noncontextual theory,

\[
S_{PNC} \leq S_c. \tag{27}
\]

This generalizes the result obtained for parity oblivious multiplexing [10]. As a consequence of our results, without imposing additional condition, operationally one may infer that any KS set provides an advantage in OC which implies preparation contextuality.

Consider the ontological model \( \{\Lambda, \mu, \xi\} \) of an operational theory, where \( \Lambda \) is the ontic state space and \( \mu(\lambda|P) \in [0,1] \) is the probability distributions over the ontic space for some preparation \( P \). Given an ontic state \( \lambda, \xi(Z|M,\lambda) \) denotes the probability for an outcome \( Z \) of measurement \( M \). Let \( p(Z|P,M) \) be the observed probability of getting the outcome \( Z \) of a measurement \( M \) on a preparation \( P \), then \( p(Z|P,M) = \sum_{\lambda \in \Lambda} \mu(\lambda|P)\xi(Z|M,\lambda) \). Denoting the set of all measurement outcome by \( \mathcal{Z}_M \) corresponding to the measurement \( M \), and \( \mathcal{M} \) as the set of all possible measurements, two different preparations \( P \) and \( P' \) are operationally equivalent if

\[
\forall Z \in \mathcal{Z}_M, \forall M \in \mathcal{M}, \quad p(Z|M,P) = p(Z|M,P'). \tag{28}
\]

In a preparation noncontextual ontological model, the ontic descriptions of two operationally equivalent preparations \( P, P' \) are the same, i.e.,

\[
\forall \lambda \in \Lambda, \mu(\lambda|P) = \mu(\lambda|P'). \tag{29}
\]
We also assume that the ontic probability distribution of a preparation which corresponds to a convex combination of two preparations, preserves the convexity at the ontic level.

In OC, the preparation device, which is possessed by Alice, performs a preparation $P_x$ for input $x$ and transmits to Bob. It is also relevant to define the effective preparation corresponding to the oblivious variable $w \in \{w\}$, denoted by $P_w$, as the convex combination of all possible preparation $P_x$ with the probability distribution $p(x|w)$. The oblivious constraints imply that the statistics of all possible measurements for different $P_w$ remain the same:

$$\forall Z \in Z_M, \forall M \in M, \forall w, w' \in \{w\}, \quad p(Z|P_w, M) = p(Z|P_{w'}, M).$$

(30)

In other words, the effective preparation $P_w$ for different $w$ are operationally equivalent. Thus, any preparation noncontextual theory implies,

$$\forall \lambda, \forall w, w' \in \{w\}, \quad p(\lambda|P_w) = p(\lambda|P_{w'}) \implies p(P_w|\lambda) = p(P_{w'}|\lambda).$$

(31)

The above relation is obtained using the Bayes’s rule,

$$p(\lambda|P_w) = p(P_w|\lambda)p(\lambda)/p(P_w)$$

(32)

where $p(\lambda) = \sum_w p(\lambda|P_w)p(P_w)$. Say, $c = p(P_w|\lambda)/p(P_w)$, and by taking summation over $w$ leads to $c = 1$. Consequently, we have

$$\forall w, \quad p(P_w|\lambda) = p(P_w).$$

(33)

This means, even if the ontic state $\lambda$ is determined, it does not contain any information about $w$. In a communication task, we seek to maximize some function of the observed probabilities $p(Z|P,M) = \sum_{\lambda} p(\lambda|P)\xi(Z|M, \lambda)$, and the best possible scenario would be the existence of a measurement which determines $\lambda$. Thus, it is sufficient to consider arbitrary number of different ontic states which can be distinguished perfectly. Equivalently, the preparation device sends arbitrary number different levels for each input $x$, exactly as considered in the OC problem with classical channel. This implies the classical bound in OC is also the bound for any preparation non-contextual models. In other words, violation of the classical bound in OC signifies preparation contextuality.

V. DISCUSSION

Test of single system contextuality is challenging to realize operationally. In particular, the compatibility loop-hole [35] and the assumption of determinism [36–38] are critically addressed. We present a universal approach to demonstrate operational significance of SIC. We introduce the vertex equality problem and explore SIC as a resource in communication in two distinct scenarios as mentioned earlier. Significantly, the quantum statistics that satisfy certain oblivious constraints cannot be reproduced by any classical resources. Moreover, by proposing the broad framework of OC, we provide a generalization to the previously studied parity oblivious multiplexing tasks [10, 39–41]. Our study points out some new interesting features. For instance, the oblivious constraints could be such that the optimal classical strategy is probabilistic. Further, the quantum strategy may attain the algebraic value of the figure of merit, perfectly satisfying the winning condition.

One may consider the vertex equality problem in OC imposing the additional restriction of bounded dimension. Interestingly, quantum success will remain certain while the optimal classical value will be less or equal to the minimum of the two scenarios. For CEG-18 set the classical success probability is same with the oblivious scenario since the optimal protocol involves four-dimensional system, but it would be interesting to know the bound for YO-13 set. Another task would be to explore the entanglement-assisted classical communication scheme for the vertex equality problem. Since OC is not restricted to the dimension of the communicated system, one can use quantum teleportation to effectively achieve any quantum OC protocol.

In future, it will be worthy to consider other SIC sets and look for the optimal separation between quantum and classical success probability in both the scenarios. Under the restriction of bounded dimension quantum key distribution [22], randomness generation [23], and device independent dimension witness [26, 27] have been studied. Our results open up whole new possibilities to implement semi-device independent information processing under bounded dimension and oblivious condition based on SIC sets. The fact that, recently several communication tasks in prepare and measure scenario have been implemented realizing higher dimensional quantum system with good visibilities [10, 41, 42], makes vertex equality problem experimentally achievable.

Acknowledgments

DS thanks Anubhav Chaturvedi for discussions. This work is supported by NCN grants 2016/23/N/ST2/02817, 2014/14/E/ST2/00020 and John Templeton Foundation.
[1] E. P. Specker, Dialectica 14, 239 (1960).
[2] J. S. Bell, Rev. Mod. Phys. 38, 447 (1966).
[3] S. Kochen and E. P. Specker, J. Math. Mech. 17, 59 (1967).
[4] A. Cabello, Phys. Rev. Lett. 101, 210401 (2008).
[5] S. Yu and C. H. Oh, Phys. Rev. Lett. 108, 030402 (2012).
[6] A. Cabello, S. Severini, and A. Winter, Phys. Rev. Lett. 112, 040401 (2014).
[7] M. Howard, J. J. Wallman, V. Veitch, and J. Emerson, Nature 510, 351 (2014).
[8] J. Anders, and D. E. Browne, Phys. Rev. Lett. 102, 050502 (2009).
[9] R. Raussendorf, Phys. Rev. A 88, 022322 (2013).
[10] R. W. Spekkens, D. H. Buzacott, A. J. Keehn, B. Toner, and G. J. Pryde, Phys. Rev. Lett. 112, 010401 (2009).
[11] M. Kleinmann, O. Gühne, J. R. Portillo, J.-A. Larsson, and A. Cabello, New J. Phys. 13, 113011 (2011).
[12] O. Gühne, C. Budroni, A. Cabello, M. Kleinmann, and J.-A. Larsson, Phys. Rev. A 89, 062107 (2014).
[13] A. Grudka, K. Horodecki, M. Horodecki, P. Horodecki, R. Horodecki, P. Joshi, W. Klobus, and A. Wojcik, Phys. Rev. Lett. 112, 120401 (2014).
[14] D. Schmid, and R. W. Spekkens, arXiv: 1706.04588 [quant-ph].
[15] G. Brassard, A. Broadbent, and A. Tapp, Alain, Foundations of Physics, 35, 1877 (2005).
[16] P. J. Cameron, A. Montanaro, M. W. Newman, S. Severini, and A. Winter, Electronic Journal of Combinatorics 14, 1 (2007).
[17] S. Abramsky, R. S. Barbosa, N. Silva, O. Zapata, arXiv: 1705.07310 [cs.LO].
[18] T. S. Cubitt, D. Leung, W. Matthews, and A. Winter, Phys. Rev. Lett. 104, 230503 (2010).
[19] P. Kurzyński, A. Cabello, and D. Kaszlikowski, Phys. Rev. Lett. 112, 100401 (2014).
[20] D. Saha, and R. Ramanathan, Phys. Rev. A 95, 030104 (R) (2017).
[21] A. Cabello, J. M. Estebaranz, and G. García-alcaine, Phys. Lett. A 212, 183 (1996).
[22] M. Pawłowski and N. Brunner, Phys. Rev. A 84, 010302(R) (2011).
[23] H-W. Li, Z.-Q. Yin, Y.-C. Wu, X.-B. Zou, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Phys. Rev. A 84, 034301 (2011).
[24] G. Brassard, Foundations of Physics 33, 1593 (2003).
[25] R. de Wolf, Theoretical Computer Science 287, 337 (2002).
[26] S. Wehner, M. Christandl, and A. C. Doherty, Phys. Rev. A 78, 062112 (2008).
[27] R. Gallego, N. Brunner, C. Hadley, and A. Acín, Phys. Rev. Lett. 105, 230501 (2010).
[28] C. Crepeau, "Equivalence between two flavours of oblivious transfer". In Advances in Cryptology: CRYPTO’87, vol. 293 of Lecture Notes in Computer Science, pages 350-354. Springer, 1988.
[29] C. H. Bennett, G. Brassard, C. Crepeau, and M.-H. Skubiszewska, Advances in Cryptology-CRYPTO’91, 576, 351 (1991).
[30] C. Crepeau, J. Mod. Opt. 41, 2445 (1994).
[31] M. Plesch, M. Pawlowski, and M. Pivoluska, Phys. Rev. A 95, 042324 (2017).
[32] R. W. Spekkens, Phys. Rev. A 71, 052108 (2005).
[33] A. Cabello, arXiv/quant-ph:1112.5149 (2011).
[34] R. Ramanathan, and P. Horodecki, Phys. Rev. Lett. 112, 040404 (2014).
[35] O. Gühne, M. Kleinmann, A. Cabello, J.-A. Larsson, G. Kirchmair, F. Zahringer, R. Gerritsma, and C. F. Roos, Phys. Rev. A 81, 022121 (2010).
[36] R. W. Spekkens, Found. Phys. 44, 11251155 (2014).
[37] R. Kunjwal and R. W. Spekkens, Phys. Rev. Lett. 115, 110403 (2015).
[38] Z.-P. Xu, D. Saha, H.-Y. Su, M. Pawlowski, and J.-L. Chen, Phys. Rev. A 94, 062103 (2016).
[39] A. Chailloux, I. Kerenidis, S. Kundu, and J. Sikora, New J. Phys. 18, 045003 (2016).
[40] A. Ambainis, M. Banik, A. Chaturvedi, D. Kravchenko, and A. Rai, arXiv:1607.05490 [quant-ph].
[41] A. Hameedi, A. Tavakoli, B. Marques, and M. Bourennane, arXiv:1704.08223 [quant-ph].
[42] J. Ahrens, P. Badziag, A. Cabello, and M. Bourennane, Nature Physics 8, 592 (2012).