Quantum Contextuality Provides Communication Complexity Advantage

Shashank Gupta,[1] Debashis Saha,[1,2] Zhen-Peng Xu,[3,4] Adán Cabello,[5,6] and A. S. Majumdar[1]
[1]S. N. Bose National Centre for Basic Sciences, Block JD, Sector III, Salt Lake, Kolkata 700106, India
[2]School of Physics, Indian Institute of Science Education and Research Thiruvananthapuram, Kerala 695551, India
[3]School of Physics and Optoelectronics Engineering, Anhui University, 230601 Hefei, People's Republic of China
[4]Naturwissenschaftlich-Technische Fakultät, Universität Siegen, Walter-Flex-Straße 3, 57068 Siegen, Germany
[5]Departamento de Física Aplicada II, Universidad de Sevilla, E-41012 Sevilla, Spain
[6]Instituto Carlos I de Física Teórica y Computacional, Universidad de Sevilla, E-41012 Sevilla, Spain

(Received 30 June 2022; accepted 31 January 2023; published 24 February 2023)

Despite the conceptual importance of contextuality in quantum mechanics, there is a hitherto limited number of applications requiring contextuality but not entanglement. Here, we show that for any quantum state and observables of sufficiently small dimensions producing contextuality, there exists a communication task with quantum advantage. Conversely, any quantum advantage in this task admits a proof of contextuality whenever an additional condition holds. We further show that given any set of observables allowing for quantum state-independent contextuality, there exists a class of communication tasks wherein the difference between classical and quantum communication complexities increases as the number of inputs grows. Finally, we show how to convert each of these communication tasks into a semi-device-independent protocol for quantum key distribution.

DOI: 10.1103/PhysRevLett.130.080802

Introduction.—Contextuality is one of the most significant properties of quantum mechanics [1–6]. It stipulates that, for some correlations, there is no probability distribution in agreement with the marginal distributions corresponding to sets of compatible (i.e., jointly measurable) observables. In particular, contextuality forbids us to assign predetermined context-independent values to the outcomes of quantum sharp measurements (defined as those that yield the same outcome when they are repeated and do not disturb any compatible observable). While nonlocality, which can be seen as a form of quantum contextuality requiring entanglement, has found many applications in quantum communication [7–9], so far, entanglement unassisted quantum contextuality has found few applications despite its conceptual importance [10–19].

Here, we first show that any contextual correlations achieved using quantum systems of sufficiently small dimensions offer a quantum advantage in a suitably designed one-way communication complexity (or distributed computation) task. Conversely, whenever an additional condition holds, any quantum protocol providing advantage in those tasks produces a proof of contextuality. By itself, this result provides an operational way to understand the sense in which some famous forms of quantum contextuality (notably, the one produced by the violation of the Klyachko-Can-Binicioğlu-Shumovsky inequality with quantum systems of dimension three [3]) are "nonclassical."

As a second result, we show that for every form of state-independent (SI) contextuality [4,24–26], the ratio between the dimensions of the classical systems and quantum systems required to accomplish the task can be made arbitrarily large by increasing the number of inputs. These communication complexity tasks are the so-called "equality problems" that appear in many practical scenarios [27–29]. Finally, we present a semi-device-independent protocol for quantum key distribution (QKD) [30], based on the quantum advantage in our communication complexity tasks, in which security is proven by using the monogamy relation [31–33] of contextuality.

Contextuality witnesses.—Given a set $\{e_i\}_{i=1}^n$ of events produced in a contextuality experiment, one can define an n-vertex graph G in which each event is represented by a vertex and exclusive events correspond to adjacent vertices. G is called the graph of exclusivity of $\{e_i\}_{i=1}^n$. In quantum mechanics, each event e_i is represented by a projector Π_i. Mutually exclusive events are represented by mutually orthogonal projectors. A quantum realization of a set of events $\{e_i\}_{i=1}^n$ with graph of exclusivity G is a set of projectors $\{\Pi_i\}_{i=1}^n$ that satisfies all the exclusivity relations in G and all the constraints imposed by the definition of the events.

Definition 1: Contextuality witness.—A functional

$$W = \sum_{i=1}^{n} w_i P(e_i), \tag{1}$$

where $w_i \geq 0$ and $P(e_i)$ is the probability of event e_i, is a quantum contextuality witness if there is a quantum realization $\{\Pi_i\}_{i=1}^n$ of $\{e_i\}_{i=0}^n$ and a quantum state ρ

such that

$$\sum_{i=1}^{n} w_i \mathrm{tr}(\rho\Pi_i) > \alpha(G,\vec{w}), \tag{2}$$

where $\alpha(G,\vec{w})$ is the independence number of the vertex-weighted graph $(G,\vec{w})$, where G is the graph of exclusivity of $\{e_i\}_{i=0}^n$ and $\vec{w} = \{w_i\}_{i=1}^n$. That is, $\alpha(G,\vec{w})$ is the largest value of $\sum_{i\in I} w_i$, where I is the set of the subsets consisting of nonadjacent vertices of G [34].

The name "contextuality witness" follows from the fact that, given W, one can find a noncontextuality inequality [35,36] whose upper bound for noncontextual models is $\alpha(G,\vec{w})$ and whose quantum value is the left-hand side of Eq. (2) [5,35,36].

We will focus on quantum realizations of contextuality witnesses constructed as follows. We first identify a vertex-weighted graph $(G,\vec{w})$ for which we can identify $\{\Pi_i\}_{i=1}^n$ and ρ such that Eq. (2) holds. We will refer to $\{(G,\vec{w}),\{\Pi_i\}_{i=1}^n,\rho\}$ as a quantum realization of a contextuality witness for $(G,\vec{w})$. In some cases, there is no need to identify a state ρ.

Definition 2: State-independent contextuality witness.—The functional Eq. (1) is a quantum state-independent contextuality witness for dimension d if there is a quantum realization $\{\Pi_i\}_{i=1}^n$ of $\{e_i\}_{i=0}^n$ such that Eq. (2) holds $\forall\,\rho \in \mathcal{O}(\mathbb{C}^d)$, where $\mathcal{O}(\mathbb{C}^d)$ denotes the set of quantum states in $\mathbb{C}^d$.

If we have $\{(G',\vec{w}),\{\Pi_i\}_{i=1}^{n'},\rho\}$ satisfying Eq. (2) that includes projectors that are not of rank one, we can obtain $\{(G,\vec{w}),\{|\psi_i\rangle\langle\psi_i|\}_{i=1}^n,\rho\}$ satisfying Eq. (2) by splitting each of the projectors that are not rank one into rank-one projectors. See Ref. [37], Appendix A.

One-way communication complexity.—Communication complexity [27] studies the amount of communication required for tasks involving inputs distributed among several parties. In one-way communication complexity [8,27,38,39], there are two parties. As shown in Fig. 1, in each round, Alice, receives a random input $x \in X$. Depending upon x, Alice sends a message (classical or quantum) to Bob. In addition, Bob receives a random input $y \in Y$. Using y and the message received from Alice, Bob outputs z, which is Bob's guess about a certain function $f(x,y)$. After many rounds, they produce the probability $p(z|x,y)$ of z, given inputs x and y. The figure of merit of the task is given by

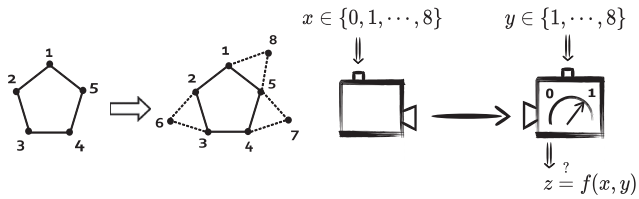

FIG. 1. On the left, the construction of the extended graph from the 5-cycle graph. Each of the 8 vertices of the extended graph belongs to at least one clique of size 3. On the right, scheme of the communication complexity task based on the extended graph.

$$S = \sum_{x,y} t(x,y)\, p(z = f(x,y)|x,y), \tag{3}$$

where $t(x,y) \geq 0$ and $\sum_{x,y} t(x,y) = 1$. We are interested in two aspects: first, the maximum value of S that can be achieved under the restriction that the dimension of the (classical or quantum) system communicated from Alice to Bob is d, and second, the minimum dimensional (classical or quantum) system required to communicate in order to achieve a certain value of S. Sharing prior classical randomness between Alice and Bob is allowed.

Communication complexity advantage based on quantum contextuality witnesses.—Consider $\{(G,\vec{w}),\{|\psi_i\rangle\langle\psi_i|\}_{i=1}^n,\rho\}$ satisfying Eq. (2) and such that $\rho \in \mathcal{O}(\mathbb{C}^d)$. Since $w_i \geq 0$, without loss of generality, we can take $\max_i w_i = 1$. The task is defined as follows. First, we consider an extended graph $\tilde{G}$ by adding additional vertices to G such that each vertex in $\tilde{G}$ belongs to, at least, one clique of size d. A clique is a set of vertices in which every pair is adjacent. We thereupon assign additional vectors (or rank-one projectors) to those additional vertices, so each vector belongs to at least one basis within the new set of vectors; see Fig. 1. Alice receives $x \in \{0,1,\ldots,n+k\}$ and Bob receives $y \in \{1,\ldots,n+k\}$, where k number of vertices is added. Bob outputs his guess for

$$f(x,y) = \begin{cases} 0, & \text{if } y = x, \\ 1, & \text{if } y \in N_x, \\ 0, & \text{if } y \in \{1,\ldots,n\} \text{ and } x = 0, \end{cases} \tag{4}$$

where N_x is the set of the vertices that are adjacent to (i.e., neighbors of) x in $\tilde{G}$. In other words, Bob needs to distinguish the runs where $y = x$ and $x = 0$ from the runs where $y \in N_x$. Except for these, whenever $y \neq x$ and $y \notin N_x$ or $x = 0$ and $y \in \{n+1,\ldots,n+k\}$, the runs do not contribute to the figure of merit of the communication task. That is, the task for Alice and Bob is to maximize

$$\begin{aligned} S^{(\tilde{G},\vec{w},d)} = \frac{1}{N}\Bigg[& \sum_{x=1}^{n+k} p(z=0|x,y=x) \\ & + \sum_{x=1}^{n+k}\sum_{y\in N_x} p(z=1|x,y) \\ & + \sum_{y=1}^{n} w_y\, p(z=0|x=0,y)\Bigg], \end{aligned} \tag{5}$$

where

$$N = n + k + \sum_{x=1}^{n+k} |N_x| + \sum_{i=1}^{n} w_i, \tag{6}$$

thus $\sum_{x,y} t(x,y) = 1$. Alice and Bob must accomplish this task with the restriction that the dimension of the (classical or quantum) system communicated between them is d. Therefore, the communication task is fully specified by the value of d, the extended graph $\tilde{G}$, and the weights $\vec{w}$. The important point is that there is quantum advantage in this communication task whenever d is "sufficiently small" in the sense that $d \leq \chi(G)$, where $\chi(G)$ is the chromatic number of the graph G [40].

Result 1.—For any $\{(G,\vec{w}), \{|\psi_i\rangle\langle\psi_i|\}_{i=1}^n, \rho\}$ with $\rho \in \mathcal{O}(\mathbb{C}^d)$ such that Eq. (2) holds and $d \leq \chi(G)$, there exists a quantum strategy for the communication complexity task defined by Eq. (5) that provides an advantage over any strategy in which the system communicated between Alice and Bob is classical.

In a general quantum strategy, let $\rho_x \in \mathcal{O}(\mathbb{C}^d)$ denote the quantum state sent by Alice to Bob upon receiving x, and let $\{M_{0|y}, M_{1|y} = \mathbb{1} - M_{0|y}\}_{y=1}^{n+k}$ denote the quantum measurement Bob performs on ρ_x to obtain z, upon receiving input y. Suppose that $\{(G,\vec{w}), \{|\psi_i\rangle\langle\psi_i|\}_{i=1}^n, \rho\}$ is a contextuality witness satisfying Eq. (2). Since, the projectors in $\{|\psi_i\rangle\langle\psi_i|\}_{i=1}^n$ are of rank one, one can always add k rank-one projectors $\{|\psi_i\rangle\langle\psi_i|\}_{i=n+1}^{n+k}$ so that the extended set $\{|\psi_i\rangle\langle\psi_i|\}_{i=1}^{n+k}$ has the relations of orthogonality given by $\tilde{G}$. Given $\{(G,\vec{w}), \{|\psi_i\rangle\langle\psi_i|\}_{i=1}^n, \rho\}$, Alice and Bob choose an extended set and apply the following strategy:

$$\rho_0 = \rho, \quad \rho_x = |\psi_x\rangle\langle\psi_x|, \quad x = 1,\ldots,n+k,$$
$$M_{0|y} = |\psi_y\rangle\langle\psi_y|, \quad y = 1,\ldots,n+k. \tag{7}$$

This way, $p(z=0|x,y=x) = p(z=1|x,y\in N_x) = 1$, so the value of $S^{(\tilde{G},\vec{w},d)}$ in Eq. (5) is

$$\frac{1}{N}\left[n + k + \sum_{x=1}^{n+k} |N_x| + \sum_{i=1}^{n} w_i \mathrm{tr}(\rho|\psi_i\rangle\langle\psi_i|)\right], \tag{8}$$

while communicating a (quantum) system of dimension d between Alice and Bob. In contrast to that, we find the following.

Theorem 1.—Whenever $d \leq \chi(G)$, for any strategy in which the system communicated between Alice and Bob is a classical system of dimension d, the value of $S^{(\tilde{G},\vec{w},d)}$ is upper bounded by

$$S^{(\tilde{G},\vec{w},d)} \leq S_c^{(\tilde{G},\vec{w},d)} = \frac{1}{N}\left[n + k + \sum_{x=1}^{n+k} |N_x| + \alpha(G,\vec{w}) - \delta\right], \tag{9}$$

where δ is the minimum number of "improperly colored" vertices of $\tilde{G}$ when d colors are used to color all the vertices. A vertex is improperly colored if it has at least one neighbor sharing the same color.

For a proof, see Ref. [37], Appendix B. Because of Eq. (2) and the fact that δ is non-negative, the expression in Eq. (8) is strictly larger than $S_c^{(\tilde{G},\vec{w},d)}$.

Let us suppose that $d_{\min}$ is the minimum dimension in which the set of projectors $\{|\psi_i\rangle\langle\psi_i|\}$ and ρ can be realized such that $\{(G,\vec{w}), \{|\psi_i\rangle\langle\psi_i|\}_{i=1}^n, \rho\}$ is a contextuality witness. For any SI contextuality witness, $\chi(G) > d_{\min}$ [41–43]. Therefore, whenever $d = d_{\min}$, there will be at least two adjacent vertices sharing the same color when d colors are used to color the graph, implying $\delta \geq 2$. Moreover, in this case, ρ_0 can be any quantum state in $\mathcal{O}(\mathbb{C}^d)$.

Explicit examples of the quantum advantage for communication complexity tasks based on some quantum SI contextuality sets are presented in [37], Appendix D, together with a proof of their robustness against white noise.

Certifying contextuality witness from communication complexity task.—The quantum communication strategy given by Eq. (7) is based on a contextuality witness. However, a general quantum strategy with advantage consists of a set of states $\{\rho_x\}_{x=0}^{n+k}$ acting on $\mathbb{C}^d$ and a set of measurement $\{M_{0|y}\}_{y=1}^{n+k}$ so that the value of $S^{(\tilde{G},\vec{w},d)}$ is greater than $S_c^{(\tilde{G},\vec{w},d)}$. In general, such a strategy may not be related to contextuality witnesses. Nevertheless, the following theorem allows us to identify whether or not an unknown quantum communication strategy admits a contextuality witness.

Theorem 2.—For the above introduced communication task defined by $S^{(\tilde{G},\vec{w},d)}$, the following condition holds:

$$\forall\, x,y,\ p(0|x,y=x) = p(1|x,y\in N_x) = 1, \tag{10}$$

if and only if $\{\rho_x\}$ is a set of rank-one projectors that has $\tilde{G}$ as graph of orthogonality and $\rho_x = M_{0|x}$.

For a proof, see Ref. [37], Appendix B. Therefore, Theorem 2 presents operational criteria to certify a set of rank-one projectors satisfying orthogonality relations according to a graph. Note that the probabilities in the Eq. (10) condition are the first two terms of $S^{(\tilde{G},\vec{w},d)}$. Consider the particular case of the task, Eq. (5), in which $d = \chi(G)$ and an unknown quantum strategy comprising $\{\rho_x\},\{M_{0|y}\}$ provides greater value than $S_c^{(\tilde{G},\vec{w},d)}$. First, it follows from Eq. (9) that, in this case, $\sum_{y=1}^n w_y \mathrm{tr}(\rho_0 M_{0|y}) > \alpha(G,\vec{w})$ since $\delta = 0$. In addition to that, if the first two terms in $S^{(\tilde{G},\vec{w},d)}$ attain their algebraic values, then Theorem 2 implies $\{(G,\vec{w}), \{M_{0|y}\}_{y=1}^n, \rho_0\}$ must be a contextuality witness.

Increasing advantage in communication complexity.—Here, we will consider only those contextuality witnesses where $\chi(G) > d_{\min}$. In these cases, it suffices to consider a simplified version of the above-described communication

complexity task by taking the first two terms of $S^{(\tilde{G},\vec{w},d)}$. Therefore, the figure of merit will be

$$S^G = \frac{1}{N}\left[\sum_{x=1}^{n} p(z=0|x,y=x) + \sum_{x=1}^{n}\sum_{y\in N_x} p(z=1|x,y)\right], \tag{11}$$

where $N = n + \sum_{x=1}^{n} |N_x|$. Here, the communication problem is solely based on the exclusivity graph G [15], and we do not need to consider additional inputs apart from the set of vertices of G. More importantly, this is an equality problem as Bob guesses whether his input y is equal to x or not [27].

Let $Q(G)$ [or $C(G)$] be the minimum dimension of quantum system (or classical system) that should be communicated to achieve $S^G = 1$. We are now interested in quantum advantages in terms of $C(G)$ and $Q(G)$. A quantum advantage in communication complexity implies $C(G) > Q(G)$, or, equivalently, $\log_2[C(G)] > \log_2[Q(G)]$ conventionally expressed in terms of classical and quantum bits.

Theorem 3.—Given any witness $\{(G,\vec{w}), \{|\psi_i\rangle\langle\psi_i|\}_{i=1}^{n}, \rho\}$ where $|\psi_i\rangle \in \mathbb{C}^{d_{\min}}$,

$$Q(G) \le d_{\min}, \qquad C(G) = \chi(G). \tag{12}$$

Moreover, $Q(G)$ is the minimum dimension d such that there exists a set of projectors $\{\Pi_i\}$ acting on $\mathbb{C}^d$ satisfying the orthogonality relations given by G.

A proof is provided in [37], Appendix B. We can readily check that the quantum strategy, $\rho_x = M_{0|x} = |\psi_i\rangle\langle\psi_i|$, yields $S^G = 1$. Thus, we have an advantage whenever $\chi(G) > d_{\min}$. In order to observe an increasing advantage, we need to consider products of graphs.

Definition 3: Inclusive graph product or co-normal product or disjunctive product or OR product $G \times H$.—The vertex set of the "inclusive graph product" of two graphs G, H is $V(G) \times V(H)$. The edges of $G \times H$ are defined as $(i,j) \sim (i',j')$ if and only if $i \sim j$ or $i' \sim j'$. We denote by G^m the m-times product of the same graph G [44,45].

Theorem 4.—Given a graph G with n vertices, the ratio between classical and quantum communication complexities of S^G based on G^m, that is, $C(G^m)/Q(G^m)$, increases polynomially with m,

$$\frac{C(G^m)}{Q(G^m)} \ge \left(\frac{\chi_f(G)}{d_{\min}}\right)^m, \quad \text{for } m \in \mathbb{N}, \tag{13}$$

where $\chi_f(G)$ is the fractional chromatic number of G [42]. For any graph, $\chi_f(G) \le \chi(G)$.

For a proof, see Ref. [37], Appendix B. Since $\chi_f(G)/d_{\min} > 1$ for any quantum SI contextuality set in dimension $d_{\min}$ [42,43], the right-hand side of Eq. (13) can be arbitrarily large as m increases [46]. It follows from Eq. (13) that the difference between the classical and quantum complexities for the equality task based on G^m is lower bounded by $m \cdot \log_2(\chi_f(G)/d_{\min})$ bits, which increases with m. In Table I, we present some explicit examples of the quantum advantage.

Before proceeding to the next section, we point out an example of SI witness and the respective equality problem where the separation between the classical and quantum communication complexities grows exponentially with the dimension. Consider the set of vectors in $\mathbb{C}^d$ of the form $(1/\sqrt{d})[1,(-1)^{x_1},\ldots,(-1)^{x_{d-1}}]^T$, where $x_i \in \{0,1\}$ such that in every vector the number of x_i taking value 1 is even. Note that there are 2^{d-2} such vectors in $\mathbb{C}^d$, and let us denote this set by $\{|\phi_i\rangle\}_{i=1}^{2^{d-2}}$. The graph, say G_{N_d}, representing the orthogonality relations for this set of vectors was introduced by Newman [50] and has been recently studied in the context of application of contextuality [49]. It turns out for any $d \ge 1128$ and divisible by 4, $\{(G_{N_d},\vec{w}), \{|\phi_i\rangle\langle\phi_i|\}\}$ is SI contextuality witness where $w_i = 1$ for all i (see Appendix C in [37] for the proof). Remarkably, for the equality problem defined by Eq. (11) with respect to G_{N_d}, we have

$$\frac{C(G_{N_d})}{Q(G_{N_d})} \ge \frac{1}{d}\left(\frac{2}{1.99}\right)^d. \tag{14}$$

Thus, the gap between classical and quantum complexities is at least $0.007d - \log_2 d$ bits. The detailed proof of this fact is provided in Appendix C of [37], which follows from the results by Frankl-Rödl [51].

Semi-device-independent quantum key distribution.—Here, we propose a QKD protocol based on quantum advantage in the communication complexity task introduced by $S^{(\tilde{G},\vec{w},d)}$ in Eq. (5) where d is taken to be $d_{\min}$. Unlike fully device-dependent protocols [14,52], our protocol is semi-device-independent [30] involving two black boxes: Alice's preparation device and Bob's measurement device. We only assume that (i) the dimension of the

TABLE I. In order to compare the quantum advantages originated from various SI contextuality witnesses, we have taken the value of m for each set such that 200 qubits is sufficient to accomplish the respective equality problem. With respect to that, the lower bounds on the classical and quantum ratios have been obtained for various SI contextuality witnesses.

SI witness with n	$d_{\min}$	$\chi_f(G)$	$C(G^m)/Q(G^m)$ from Eq. (13) so that $d_{\min}^m \sim 200$ qubits
YO-13 [25]	3	35/11	$\ge 6 \times 10^{13}$
Peres-33 [47]	3	13/4	$\ge 4 \times 10^{13}$
CEG-18 [48]	4	9/2	$\ge 3.4 \times 10^{7}$
Pauli-240 [49]	8	15	$\ge 1.9 \times 10^{18}$
Pauli-4320 [49]	16	60	$\ge 5 \times 10^{28}$

degrees of freedom (of the physical system), in which the information is encoded, is bounded by $d_{\min}$, and (ii) the devices may share classical randomness but that is uncorrelated with the choices of the inputs x, y. The QKD protocol is as follows. After completing a large number of runs, Alice randomly chooses some runs and publicly announces her input x so that Bob can verify that the obtained value of the figure of merit is greater than S_c. Thereby, Bob is ensured that the probabilities produced by his device cannot be simulated by classical systems under the aforementioned assumptions. Bob publicly announces his input y for the remaining runs. Subsequently, Alice notes down $f(x,y)$ according to Eq. (4) as the shared key. Whenever $y \notin \{x, N_x\}$, or, $y \in \{n+1, \ldots, n+k\}$ and $x = 0$, Alice publicly announces that the transmission is unsuccessful.

It is not difficult to show that such QKD protocol is secure against restricted eavesdroppers whenever the contextuality witness satisfies the "monogamy relations" that are proposed in [31]. The monogamy relation between two witnesses of contextuality realized on two separate degrees of freedom of any quantum state ρ implies

$$\sum_{i=1}^{n} w_i \mathrm{tr}[\rho(\Pi_i \otimes \mathbb{1})] + \sum_{i=1}^{n} w_i \mathrm{tr}[\rho(\mathbb{1} \otimes \bar{\Pi}_i)] \leq 2\alpha(G, \vec{w}) \tag{15}$$

for any $\vec{w}$, where $\{\Pi_i\}$, $\{\bar{\Pi}_i\}$ realize the respective exclusivity graph G. Such relation holds for a large class of contextuality witnesses, including the well-known odd-cycle witnesses [31]. The QKD protocol is secure if the mutual information of Alice-Bob is greater than the mutual information of Alice-Eve [30], i.e., $I(A:B) > I(A:E)$, which for individual attacks and binary output implies $S_B > S_E$, taking $S_B(S_E)$ as the value of $S^{(\tilde{G},\vec{w},d)}$ obtained by Bob (Eve). Since Eve also knows the input y, she and Bob are in the same state to guess $f(x,y)$. Because of Theorem 2, when Bob observes that the first two terms in $S^{(\tilde{G},\vec{w},d)}$ attain their maximal values, then $M_{0|y}$ are rank-one projectors realizing $\tilde{G}$. We assume that $M_{0|y}$ for Eve also realizes $\tilde{G}$. Now, even if Eve shares arbitrary quantum correlation with the preparation device of Alice, due to the Eq. (15) monogamy relation, the following holds true:

$$\sum_{y=1}^{n} w_y p_B(0|x=0,y) + \sum_{y=1}^{n} w_y p_E(0|x=0,y) \leq 2\alpha(G, \vec{w}). \tag{16}$$

Taking the best possible scenario for Eve in which she also observes Eq. (10), the above relation implies

$$S_B + S_E \leq 2S_c^{(\tilde{G},\vec{w},d)}. \tag{17}$$

Therefore, whenever Alice-Bob obtains quantum advantage, that is, $S_B > S_c^{(\tilde{G},\vec{w},d)}$, the protocol is secure against such eavesdropping. Subsequently, the key rate can be obtained by $r = I(A:B) - I(A:E)$ (see Table I in [37]).

In addition to the QKD protocol, these communication tasks can also be used to generate quantum randomness in the prepare-and-measure scenario [53–55]. We have discussed this in Appendix D of [37].

Conclusions.—This Letter shows that all forms of quantum contextuality with sufficiently small dimension provide quantum advantage in distributed computation and in various communication protocols without requiring entanglement. In distributed computation, equality problems are essential for implementing large-scale circuits and data verification [27–29] (see Appendix F of [37]). We show the existence of a variant of the equality problem pertaining to every vertex-weighted graph with certain properties providing an advantage over classical communication.

Considering equality problems defined by the graphs of a large class of contextuality witnesses, including all quantum state-independent contextuality witnesses, we show that the communication complexity required to execute such problems in classical theory is larger than that in quantum theory. Moreover, the complexity advantage increases with an increase in the number of inputs, identifying a class of equality problems that can be solved only in quantum communication.

As further applications of quantum contextuality driven communication tasks, we show how such tasks can be used for semi-device-independent QKD, as well as for the purpose of randomness generation. As interesting open problems for further work, we point out the possibility of extending the security proof of the QKD protocol to arbitrary individual eavesdropping strategies and finding optimal communication complexity advantages. It would also be interesting to extend the link between quantum contextuality and quantum advantage in communication complexity tasks involving more than two parties, like, quantum fingerprinting [56].

D. S. acknowledges National Post-Doctoral Fellowship (PDF/2020/001682) for support. A. C. is supported by Project Qdisc (Project No. US-15097, Universidad de Sevilla), with FEDER funds, QuantERA grant SECRET, by MINECO (Project No. PCI2019-111885-2), and MICINN (Project No. PID2020–113738GB-I00). A. S. M. acknowledges support from Project No. DST/ICPS/QuEST/2018/98 of the Department of Science & Technology, Government of India.

[1] J. S. Bell, Rev. Mod. Phys. **38**, 447 (1966).
[2] S. Kochen and E. P. Specker, J. Math. Mech. **17**, 59 (1967).
[3] A. A. Klyachko, M. A. Can, S. Binicioğlu, and A. S. Shumovsky, Phys. Rev. Lett. **101**, 020403 (2008).

[4] A. Cabello, Phys. Rev. Lett. **101**, 210401 (2008).
[5] A. Cabello, S. Severini, and A. Winter, Phys. Rev. Lett. **112**, 040401 (2014).
[6] C. Budroni, A. Cabello, M. Kleinmann, J.-Å. Larsson, and O. Gühne, Rev. Mod. Phys. **94**, 045007 (2022).
[7] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[8] H. Buhrman, R. Cleve, S. Massar, and R. de Wolf, Rev. Mod. Phys. **82**, 665 (2010).
[9] T. S. Cubitt, D. Leung, W. Matthews, and A. Winter, Phys. Rev. Lett. **104**, 230503 (2010).
[10] M. Kleinmann, O. Gühne, J. R. Portillo, J.-Å. Larsson, and A. Cabello, New J. Phys. **13**, 113011 (2011).
[11] M. Howard, J. Wallman, V. Veitch, and J. Emerson, Nature (London) **510**, 351 (2014).
[12] A. Cabello, M. Gu, O. Gühne, and Z.-P. Xu, Phys. Rev. Lett. **120**, 130401 (2018).
[13] A. Grudka, K. Horodecki, M. Horodecki, P. Horodecki, R. Horodecki, P. Joshi, W. Kłobus, and A. Wójcik, Phys. Rev. Lett. **112**, 120401 (2014).
[14] J. Singh, K. Bharti, and Arvind, Phys. Rev. A **95**, 062333 (2017).
[15] D. Saha, P. Horodecki, and M. Pawłowski, New J. Phys. **21**, 093057 (2019).
[16] K. Bharti, M. Ray, A. Varvitsiotis, N. A. Warsi, A. Cabello, and L. C. Kwek, Phys. Rev. Lett. **122**, 250403 (2019).
[17] D. Saha, R. Santos, and R. Augusiak, Quantum **4**, 302 (2020).
[18] P.-E. Emeriau, M. Howard, and S. Mansfield, PRX Quantum **3**, 020307 (2022).
[19] There is other notion of contextuality, preparation contextuality [20], which has found application in oblivious multiplexing and state discrimination tasks [21–23].
[20] R. W. Spekkens, Phys. Rev. A **71**, 052108 (2005).
[21] R. W. Spekkens, D. H. Buzacott, A. J. Keehn, B. Toner, and G. J. Pryde, Phys. Rev. Lett. **102**, 010401 (2009).
[22] S. Ghorai and A. K. Pan, Phys. Rev. A **98**, 032110 (2018).
[23] D. Schmid and R. W. Spekkens, Phys. Rev. X **8**, 011015 (2018).
[24] P. Badziag, I. Bengtsson, A. Cabello, and I. Pitowsky, Phys. Rev. Lett. **103**, 050401 (2009).
[25] S. Yu and C. H. Oh, Phys. Rev. Lett. **108**, 030402 (2012).
[26] M. Kleinmann, C. Budroni, J.-Å. Larsson, O. Gühne, and A. Cabello, Phys. Rev. Lett. **109**, 250402 (2012).
[27] E. Kushilevitz and N. Nisan, *Communication Complexity* (Cambridge University Press, Cambridge, England, 2006).
[28] T. Roughgarden, Found. Trends Theor. Comput. Sci. **11**, 217 (2016).
[29] A. Rao and A. Yehudayoff, *Communication Complexity: And Applications* (Cambridge University Press, Cambridge, England, 2020).
[30] M. Pawłowski and N. Brunner, Phys. Rev. A **84**, 010302(R) (2011).
[31] R. Ramanathan, A. Soeda, P. Kurzyński, and D. Kaszlikowski, Phys. Rev. Lett. **109**, 050404 (2012).
[32] P. Kurzyński, A. Cabello, and D. Kaszlikowski, Phys. Rev. Lett. **112**, 100401 (2014).
[33] D. Saha and R. Ramanathan, Phys. Rev. A **95**, 030104(R) (2017).
[34] J. A. Bondy and U. S. R. Murty, *Graph Theory with Applications* (Macmillan, London, 1976).
[35] A. Cabello, Phys. Rev. A **93**, 032102 (2016).
[36] A. Cabello, Phys. Rev. Lett. **127**, 070401 (2021).
[37] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.130.080802 for proof of all the theorems, explicit examples of the communication tasks based on well-known contextuality witnesses, robustness analysis of the quantum advantage, and details of QKD and randomness protocol.
[38] R. de Wolf, Theor. Comput. Sci. **287**, 337 (2002).
[39] H. Buhrman, R. Cleve, and A. Wigderson, in *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing* (Association for Computing Machinery, New York, 1998), p. 63.
[40] Chromatic number is the smallest number of colors needed to color the vertices of G so that no two adjacent vertices share the same color [34].
[41] A. Cabello, arXiv:1112.5149.
[42] R. Ramanathan and P. Horodecki, Phys. Rev. Lett. **112**, 040404 (2014).
[43] A. Cabello, M. Kleinmann, and C. Budroni, Phys. Rev. Lett. **114**, 250402 (2015).
[44] U. Feige, Combinatorica **17**, 79 (1997).
[45] U. Feige, in *Proceedings of the Twenty-Seventh Annual ACM Symposium on Theory of Computing* (ACM, New York, 1995), p. 635.
[46] Note that $d_{\min}$ is lower bounded by the size of the maximum clique, i.e., the clique of largest size, of G.
[47] A. Peres, J. Phys. A **24**, L175 (1991).
[48] A. Cabello, J. Estebaranz, and G. García-Alcaine, Phys. Lett. A **212**, 183 (1996).
[49] Z.-P. Xu, J. Steinberg, J. Singh, A. J. López-Tarrida, J. R. Portillo, and A. Cabello, Graph-theoretic approach to Bell experiments with low detection efficiency, arXiv:2205.05098.
[50] M. W. Newman, *Independent Sets and Eigenspaces*, Ph.D. thesis (University of Waterloo, 2004).
[51] P. Frankl and V. Rodl, Trans. Am. Math. Soc. **300**, 259 (1987).
[52] C. H. Bennett and G. Brassard, Theor. Comput. Sci. **560**, 7 (2014).
[53] H.-W. Li, M. Pawłowski, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, Phys. Rev. A **85**, 052308 (2012).
[54] T. Lunghi, J. B. Brask, C. C. W. Lim, Q. Lavigne, J. Bowles, A. Martin, H. Zbinden, and N. Brunner, Phys. Rev. Lett. **114**, 150501 (2015).
[55] Y.-G. Han, Z.-Q. Yin, H.-W. Li, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, Phys. Rev. A **93**, 032332 (2016).
[56] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf, Phys. Rev. Lett. **87**, 167902 (2001).