Quantum communication complexity advantage implies violation of a Bell inequality

Harry Buhrman[a,b,c], Łukasz Czekaj[d,e], Andrzej Grudka[f], Michał Horodecki[d,e], Paweł Horodecki[e,g], Marcin Markiewicz[d,e,h], Florian Speelman[a], and Sergii Strelchuk[i,1]

[a]Algorithms and Complexity Unit, Centrum Wiskunde & Informatica, 1098 XG Amsterdam, The Netherlands; [b]Department of Computer Science, University of Amsterdam, 1012 WX Amsterdam, The Netherlands; [c]QuSoft, 1098 XG Amsterdam, The Netherlands; [d]Faculty of Mathematics, Physics and Informatics, Institute of Theoretical Physics and Astrophysics, Gdańsk University, 80-952 Gdańsk, Poland; [e]National Quantum Information Centre of Gdańsk, Gdańsk University, 81-824 Sopot, Poland; [f]Faculty of Physics, Adam Mickiewicz University, 61-614 Poznan, Poland; [g]Faculty of Applied Physics and Mathematics, Gdańsk University of Technology, 80-952 Gdańsk, Poland; [h]Institute of Physics, Jagiellonian University, 30-348 Krakow, Poland; and [i]Department of Applied Mathematics and Theoretical Physics, University of Cambridge, Cambridge CB3 0WA, United Kingdom

Edited by Anton Zeilinger, University of Vienna, Vienna, Austria, and approved January 7, 2016 (received for review April 22, 2015)

We obtain a general connection between a large quantum advantage in communication complexity and Bell nonlocality. We show that given any protocol offering a sufficiently large quantum advantage in communication complexity, there exists a way of obtaining measurement statistics that violate some Bell inequality. Our main tool is port-based teleportation. If the gap between quantum and classical communication complexity can grow arbitrarily large, the ratio of the quantum value to the classical value of the Bell quantity becomes unbounded with the increase in the number of inputs and outputs.

quantum | Bell inequality | port-based teleportation | communication complexity | nonlocality

The key element that distinguishes classical from quantum information theory is quantum correlations. The first attempt to quantify their strength was quantitatively expressed in Bell's theorem (1). They are similar to classical correlations in that one cannot take advantage of them to perform superluminal communication, yet every attempt to explain such correlations from the point of view of classical theory—namely, to find a local hidden variable model—is impossible. For a long time the existence of quantum correlations was merely of interest to philosophically minded physicists and was considered an exotic peculiarity, rather than a useful resource for practical problems in physics or computer science. This has changed dramatically in recent years—it became apparent that quantum correlations can be used as a resource for a number of distributed information processing tasks (2–4), producing surprising results (5, 6).

One area where using quantum correlations has wide-reaching practical implications is communication complexity. A typical instance of a communication complexity problem features two parties, Alice and Bob, who are given binary inputs x and y. They wish to compute the value of $f(x,y)$ by exchanging messages between each other. The minimum amount of communication required to accomplish the task by exchanging classical bits (with bounded probability of success) is called classical communication complexity, denoted as $C(f)$.

There are two ways to account for the communication complexity of computing a function when we want to make use of quantum correlations. In the first one, Alice and Bob share any number of instances of the maximally entangled state $|\Psi^-\rangle_{AB} = (1/\sqrt{2})(|01\rangle - |10\rangle)_{AB}$ beforehand and are allowed to exchange classical bits to solve the problem. Another approach is to have no preshared entanglement, but instead allow Alice and Bob to exchange qubits. The latter type of protocol can always be converted to the former with preshared entanglement and classical communication. We denote the quantum communication complexity of computing the function $f(x,y)$ (with bounded probability of success) by $Q(f)$.

For a large number of problems, the respective quantum communication complexity is much lower compared with its classical counterpart (4, 7). In such cases, we say that there exists a quantum advantage for communication complexity. In other words, one achieves a quantum advantage if the quantum communication complexity of the function is lower than its corresponding classical communication complexity.

One of the most striking example of quantum advantage is the famous Raz problem (5, 8), where quantum communication complexity is exponentially smaller than classical. Another example is the "hidden matching" problem for which the quantum advantage leads to one of the strongest possible violations of the Bell inequality (9). The latter inequality plays an important role in detecting quantum correlations and certifying the genuinely quantum nature of resources at hand. Previously, to obtain an unbounded violation of a particular Bell inequality one resorted to problems with the exponential quantum advantage. Here, we show that one can achieve the same result, using only polynomial quantum advantage.

As a matter of fact, the very first protocols offering quantum advantage were based on a quantum violation of certain Bell inequalities (6). It was even shown that for a very large class of multiparty Bell inequalities, correlations that violate them lead to a quantum advantage (perhaps, for a peculiar function) (10). This indicates that Bell nonlocality often leads to a quantum advantage. However, there are more and more communication protocols that offer a quantum advantage, but, nevertheless, they are not known to violate any Bell inequality.

It has long been suspected (6) that quantum communication complexity and Bell nonlocality are the two sides of the same coin. Although it is possible to convert a Bell nonlocality testing experiment to the communication complexity instance, the reverse has been known only for some particular examples. The question is whether this relationship holds in general, namely, Is quantum communication inherently equivalent to Bell nonlocality when solving communication complexity problems?

Until now, there were only two concrete examples where one could certify quantum correlations in the context of communication complexity by providing a quantum state and a set of measurements

Significance

For many communication complexity problems the quantum strategies, distinguished by using Bell nonlocal correlations, provide exponential advantage over the best possible classical strategies. Conversely, for any Bell nonlocal correlations there exists a communication complexity problem that is solved more efficiently using the former. Despite many efforts, there were only two problems for which one could certify that any strategy that outperforms the classical one must harbor Bell nonlocal correlations. We prove that any large advantage over the best known classical strategy makes use of Bell nonlocal correlations. Thus, we provide the missing link to the fundamental equivalence between Bell nonlocality and quantum advantage.

Author contributions: H.B., Ł.C., A.G., M.H., P.H., M.M., F.S., and S.S. performed research; and S.S. wrote the paper.

The authors declare no conflict of interest.

This article is a PNAS Direct Submission.

[1]To whom correspondence should be addressed. Email: ss870@cam.ac.uk.

This article contains supporting information online at www.pnas.org/lookup/suppl/doi:10.1073/pnas.1507647113/-/DCSupplemental.

PHYSICS

whose statistics violate some Bell inequality. The first case is the "hidden matching" problem and the second one is a theorem, which states that a special subset of protocols that provide quantum advantage also implies the violation of local realism (6). To get the violation of Bell inequalities obtained from the examples above, one had to perform an involved analysis that relied on a problem-specific set of symmetries. Thus, such an approach cannot be generalized to an arbitrary protocol for achieving a quantum advantage in the communication complexity problem.

In this paper, we show that given any (sufficiently large) quantum advantage in communication complexity, there exists a way of obtaining measurement statistics that violate some linear Bell inequality. This completely resolves the question about the equivalence between the quantum communication and Bell nonlocality: Whenever a protocol computes the value of the function $f(x,y)$ better than the best classical protocol, even with a gap that is only quadratic, then there must exist a Bell inequality that is violated.

We provide a universal method that takes a protocol that achieves the quantum advantage in any single- or multiround communication complexity problem and uses it to derive the violation of some linear Bell inequality. This method can be generalized to a setting with more than two parties. Our Bell inequalities lead to a so-called unbounded violation (11): The ratio of the quantum value to the classical value of the Bell quantity can grow arbitrarily large with the increase of the number of inputs and outputs, whenever the ratio of $C(f)$ and $(Q(f))^2$ grows too. In particular, an exponential advantage leads to an exponential ratio.

Our method consists of two parts. In the first part, we use the quantum protocol based on the given communication complexity game to construct a set of quantum measurements on a maximally entangled state The central ingredient of our construction is the recently discovered port-based teleportation (12, 13). In the second part, given a protocol that computes a function f by using $Q(f)$ qubits, and the optimal classical error probability achievable with $(Q(f))^2$ bits, we construct the corresponding linear Bell inequality that is subsequently violated by the above quantum measurements.

For one-way communication complexity problems we develop a much simpler method that is based on the remote state preparation and results in a nonlinear Bell inequality.

Quantum Communication Complexity Protocol

We start by defining a general quantum multiround communication protocol. Two parties, Alice and Bob, receive inputs $x \in X = \{0,1\}^n$ and $y \in Y = \{0,1\}^n$ according to some distribution μ and their goal is to compute the function $f: X \times Y \to \{0,1\}$ by exchanging qubits over multiple rounds. We further use subscripts for the system names to denote the round number. The parties proceed as follows:

i) Alice applies $U_x^{A_0 \to M_1 A_1}$ on her local state ρ_{A_0} and sends ρ_{M_1} to Bob. In general, M_1 may be entangled with A_1, which remains with Alice.

ii) Bob performs $U_y^{M_1 B_0 \to M_2 B_1}$ on the state $\rho_{M_1} \otimes \sigma_{B_0}$. Then he sends back the system M_2 to Alice, keeping B_1.

iii) Parties repeat steps *i* and *ii* for $r-1$ rounds. In the last round, instead of communicating back to Alice, Bob measures the observable o_y and outputs the value of the function f. The observable o_y acts on the system M_{2r-1} and Bob's memory B_{r-1}.

The above protocol may be transformed to the form where a one-qubit system is exchanged between Alice and Bob at any round. To achieve this, we split the Q-qubit message from Alice to Bob (or vice versa) into Q rounds of one-qubit transmission and modify the protocol as follows. We start from the initial state, which has the form

$$|\rho_A^M\rangle |\theta_A^C\rangle |\sigma_B^M\rangle, \quad [1]$$

where $|\rho_A^M\rangle$ and $|\sigma_B^M\rangle$ describe the memory registers that belong to Alice and Bob, respectively. The state $|\theta_A^C\rangle$, initially in state $|\theta\rangle = |0\rangle$ with Alice, is a one-qubit system that is used for message passing from Alice to Bob and vice versa. In each round, Alice applies U_x^i to $\rho \otimes \theta$, and Bob applies U_y^i to $\sigma \otimes \theta$. In the last round, instead of applying a unitary transformation, Bob performs a measurement. One may view unitaries U_x^i and U_y^i as controlled gates acting on the memory with the one-qubit register acting as a control. This implies that for given x, in round i the state of Alice's memory is spanned on at most 2^i orthogonal vectors. This observation will be crucial for the construction of a compressed-memory quantum protocol. Thus, we can transform any given protocol that requires Q qubits of communication into one that makes use of $2Q$ one-qubit exchanges.

From an Arbitrary Protocol to a Compressed-Memory Protocol

One shortcoming of the above protocols is that both players possess a local memory, possibly entangled with the message, which can span an arbitrary number of qubits and therefore could be much too big to properly handle in other parts of our construction. We solve this problem by converting an arbitrary protocol, as described above, to a protocol where we can upper bound the maximum size of the local memory.

The following proposition, which is a consequence of the Yao–Kremer lemma (3, 14), shows that it is possible to compress the parties' local memory each step and that therefore the size of the local memory can be assumed to be at most the total communication. We include the proof in *Supporting Information*, section IV.

Proposition 1. *For any Q-qubit quantum communication protocol (without prior entanglement) there exists a Q-qubit quantum communication protocol for which Alice and Bob can encode their local memory on at most Q qubits each.*

Quantum Measurements from the Quantum Communication Complexity Protocol

We now show how to convert a multiround compressed-memory protocol for computing $f(x,y)$, which gives a quantum advantage to the violation of a linear Bell inequality. There exist two different protocols to achieve this. The first protocol is based on the recently introduced method of port-based teleportation, which we briefly review in the next section. The second method, discussed at the end of this paper, relies on remote state preparation (15). We base our construction on the port-based teleportation because unlike the remote state preparation it is easily extendible to the multiround protocol and also gives rise to a linear Bell inequality.

Port-Based Teleportation

In deterministic port-based teleportation, the two parties share N pairs of maximally entangled qudits $|\Psi^-\rangle_{A_1B_1} \otimes \cdots \otimes |\Psi^-\rangle_{A_NB_N}$, each of which is called a "port." To transmit the state $|\Psi^{\text{in}}\rangle_{A_0}$, the sender performs the square-root teleportation measurement given by a set of positive operator valued measure (POVM) elements $\{\Pi\}_{i=1}^N$ (precisely defined in equation 27 of ref. 13) on all of the systems A_i, $i = 0, \ldots, N$, obtaining the result $z = 1 \ldots N$. Then, he or she communicates z to the receiver who traces out the subsystems $B_1 \ldots B_{z-1} B_{z+1} \ldots B_N$ and remains with the teleported state $|\Psi^{\text{out}}\rangle_{B_z}$ in the subsystem B_z. Teleportation always succeeds and the fidelity of the teleported state with the original is $F(|\Psi^{\text{in}}\rangle_{A_0}, |\Psi^{\text{out}}\rangle_{B_z}) \geq 1 - d^2/N$. The cost of the classical communication from sender to receiver is equal to $c = \log_2 N$. The distinctive feature of this protocol is that unlike with original teleportation, it does not require a correction on the receiver's side.

Constructing Quantum Measurements

Using port-based teleportation we can now construct the relevant quantum measurements. Parties start with the initial state **[1]** and perform the following protocol:

i) Alice applies $U_x^{A_0 \to M_1 A_1}$ on her local state ρ_{A_0}. She obtains the state of size $Q_1 = \log \dim M_1 + \log \dim A_1$, which is teleported to Bob at once, using N_1 ports each of dimension 2^{Q_1}. This consumes N_1 ports. Alice does not communicate the classical teleportation outcomes $\{i_1^A\}$, $|\{i_1^A\}| = N_1$ with $i_1^A \in \{1, \ldots, N_1\}$ to Bob.

ii) Bob applies the local unitary $U_y^{M_1 B_0 \to M_2 B_1}$ to each of the ports (he does not know the value of i_1) and teleports each of the N_1 states one-by-one by applying the teleportation measurement using N_2 ports each of the dimension 2^{Q_2}, where $Q_2 = \log \dim M_2 + \log \dim B_1 + \log \dim A_1$. This consumes $N_1 N_2$ ports. Bob keeps the set of N_2 teleportation outcomes $\{i_{1,1}^B, \ldots, i_{1,N_2}^B\}$, $|\{i_{1,1}^B, \ldots, i_{1,N_2}^B\}| = N_1 N_2$, where for each $j = 1 \ldots N_2$, $i_{1,j}^B \in \{1, \ldots, N_2\}$.

iii) Parties repeat steps *i* and *ii* for $r-1$ rounds.

At the end of the protocol we obtain the set of measurements that map the generic communication protocol into the set of correlations,

$$p\Big(\{i_1^A\}, \{i_{1,1}^B, \ldots, i_{1,N_1}^B\}, \{i_{2,1}^A, \ldots, i_{2,N_1 N_2}^A\}, \ldots, \{i_{r,1}^B, \ldots, i_{r,N_1 N_2 \ldots N_{2r-1}}^B\}, \{o_1, \ldots, o_{N_1 N_2 \ldots N_r}\} | x, y\Big), \qquad [2]$$

where $\{o_j\}$ are the final teleportation measurements in round r on Bob's side. An important feature of this construction is that all of the quantum measurements are performed simultaneously but the classical information exchange happens sequentially. A single round of the protocol is depicted in Fig. 1 and the entire protocol is depicted in Fig. 2.

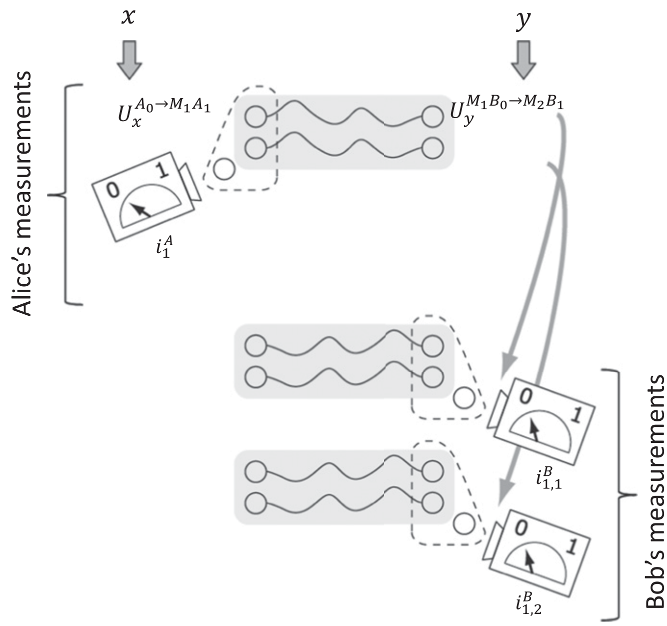

Fig. 1. The structure of a single round of the protocol. Alice applies U_x to her system, which if followed by Bob's unitary U_y. Bob has no information about the outcome of Alice's port-based teleportation, i_1^A, so he teleports each of his qudit subsystems individually, obtaining $i_{1,1}^B$, $i_{1,2}^B$, ….

Simulating the Quantum Protocol

The last part of the puzzle is a method of simulating the compressed-memory quantum protocol, using the above correlations and classical communication.

Lemma 1. *Given a protocol for computing f that uses Q qubits of communication and achieves the success probability* $p_{\rm succ} \ge 1/2 + \epsilon$, $\epsilon > 0$, *one can simulate it using correlations* [**2**] *and* $10Q^2$ *bits of classical communication with the success probability* $p_{\rm succ} \ge 1/2 + (1 - 2^{-Q})^{2Q}\epsilon$.

Proof: Having access to correlations [**2**], Alice and Bob exchange their respective outcomes of the teleportation measurements that amount to $\log_2 N_1 N_2 N_3 \ldots N_{2r-1}$ bits of communication. This finalizes the port-based teleportation and thus simulates the corresponding quantum protocol. After exchange, Bob returns o_L, where L denotes the last index that he received from Alice.

The above protocol is equivalent to $2r$ rounds of port-based teleportation used for the compressed-memory protocol. Because by the compression of *Proposition 1* for every round i the dimension of the teleported state Q_i is at most 2^{2Q+1} (the message is encoded in 1 qubit and the local memories are encoded in Q qubits each), we set $\log_2 N_i = 5Q$ so that the fidelity of teleportation on each step is $F \ge (1 - 2^{-Q})$. Then the protocol has success probability $p_{\rm succ} \ge 1/2 + F^{2r}\epsilon$, where $p_{\rm succ} \ge 1/2 + \epsilon$ is the success probability of the original quantum protocol. Bounding the number of rounds r by the total amount of quantum communication Q, we get $p_{\rm succ} \ge 1/2 + 1/2(1 - 2^{-Q})^{2Q}\epsilon$. Thus, the total amount of classical communication is bounded above by $10Q^2$. □

Construction of a Bell Inequality and Its Violation

Let us sum up the whole construction. First, we start with a quantum multiround protocol to compute f that uses quantum communication and no shared entanglement. This protocol requires Q qubits of communication and achieves $p_{\rm succ} \ge 1/2 + \epsilon$. In this protocol, Alice and Bob may use an arbitrary amount of local quantum memory between rounds. Second, we convert it to the protocol with compressed local quantum memory, where the latter can be encoded in Q qubits. The compressed protocol is then used to obtain correlations in the form [**2**]. These correlations together with classical communication are used to recover the original communication complexity protocol that computes f. This protocol uses $O(Q^2)$ bits of classical communication and achieves success probability $p_{\rm succ} \ge 1/2 + (1 - 2^{-Q})^{2Q}\epsilon$.

Now, if for a function $f(x,y)$ there exists a gap between $C(f)$ and $(Q(f))^2$ with $p_{\rm succ} = 1/2 + \delta$ for the classical communication complexity protocol, and $\delta \ll \epsilon$—then we observe the quantum violation of the Bell inequality of the form

$$\sum_{x,y} \mu(x,y) \sum_{q \in \mathcal{P}} p\big(o_q = f(x,y) | x, y\big) \le \frac{1}{2} + \delta, \qquad [3]$$

where μ is a probability measure on $X \times Y$, the set $\mathcal{P}$ denotes the set of all paths from the root to the leaves of length $2r-1$ of the tree formed by the subsequent outputs of Alice and Bob in the protocol, and $p(o_q = f(x,y)|x,y)$ is the marginal probability that comes from summing over all indexes that do not explicitly appear in the path q (Fig. 3). With the exception of the last level, every node on the ith level has N_i children that correspond to the outcome of the ith round of teleportation. The index of the first node in the path corresponds to the state being on Alice's side and each subsequent index corresponds to the state being either on Alice's or on Bob's side in the alternating manner. The leaves of the tree correspond to the outcomes of Bob's binary observable, which is his guess of the value of the function $f(x,y)$. (Note that in the Bell inequality, only special outputs appear—those given by the paths of length $2r-1$ from the root to the leaves—whereas in general, outputs will be given by all sequences composed of choosing one node from every level.)

The Bell inequality [**3**] is the central quantity of this paper. The left-hand side of the inequality constitutes the maximal success probability of guessing the value of f that can be achieved with the correlations of the form [**2**]. If this success probability turns out to be greater than the maximal success probability attained by the best classical protocol (the right-hand side of the inequality), this implies that correlations [**3**] reveal Bell nonlocality.

Large Violation of a Bell Inequality from Communication Complexity

We now show how to combine the above ingredients to get the main result: Whenever $C(f) \gg (Q(f))^2$, we obtain an unbounded

PHYSICS

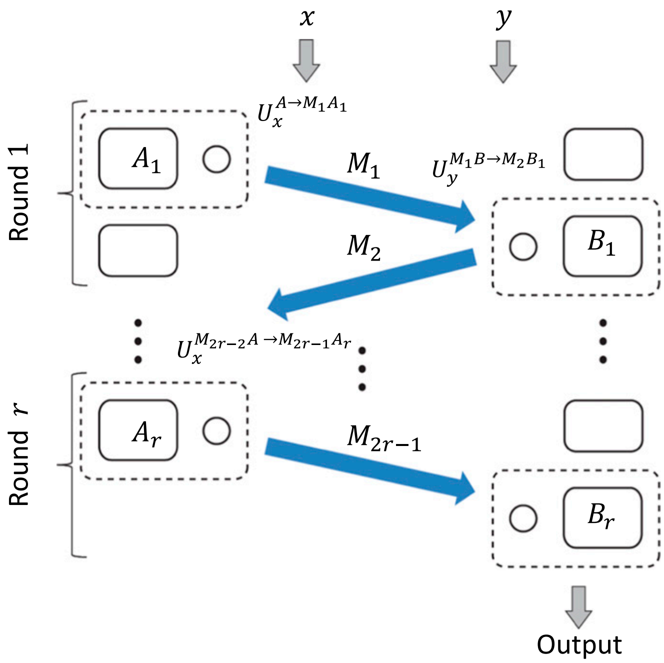

Fig. 2. Constructing quantum measurements. A and B denote Alice's and Bob's local subsystems, respectively. Each measurement M_i, $i=1,\ldots,r_{2r-1}$ represents the square-root measurement in the port-based teleportation (12).

violation of the Bell inequality—the ratio of the quantum to the classical value of our Bell inequality grows arbitrarily when we increase the number of inputs and outputs (6, 9, 11, 16–18).

To state and proof the main theorem we summarize the above results in the following sequence of steps:

i) Given a quantum protocol with advantage that uses Q bits of communication and achieves $p_{\text{succ}}=1/2+\epsilon$, we convert it (using *Proposition 1*) to the memoryless protocol that uses $10Q^2$ bits of communication and achieves the same success probability.

ii) From the memoryless protocol using measurements and quantum state we obtain the set of quantum correlations R_q.

iii) Using R_q and $10Q^2$ bits of classical communication, we obtain a new protocol $\overline{P}$ that achieves

$$p_{\text{succ}}\geq\frac{1}{2}+\left(1-2^{-Q}\right)^{2Q}\epsilon.$$

Recall that all of the above measurements are done simultaneously, but the exchange of the corresponding classical information happens sequentially.

iv) We turn protocol $\overline{P}$ into a Bell inequality. To this end, we consider a general construction of Bell inequality given any function $f(x,y)$ and a protocol P that uses communication and correlations. Namely, denote $f_P(a,b,x,y)$ to be a guess of $f(x,y)$ determined by the protocol for given inputs (x,y) and outputs (a,b). Then, consider the probability of success of guessing the correct value of the function f parameterized by the correlations R,

$$p_{f,P}^{\text{succ}}(R)=\text{Prob}[f_P(a,b,x,y)=f(x,y)]=\sum_{x,y}\mu(x,y)\sum_{a,b}R(ab|xy)\mathbb{I}_{\{f_P(a,b,x,y)=f(x,y)\}},\quad\textbf{[4]}$$

where $\mathbb{I}(\cdot)$ is the indicator function. Our Bell inequality will simply be a shifted value of guessing probability

$$B_{f,P}(R)=p_{f,P}^{\text{succ}}(R)-\frac{1}{2}.\quad\textbf{[5]}$$

v) We consider the behavior of the above Bell inequality on classical correlations R_{cl} as a function of the amount of communication used by $\overline{P}$. To this end we apply *Lemma 3* (proved in *Supporting Information*, section I), which states that given an arbitrary protocol P that uses C_P bits of communication, we have

$$B_{f,P}(R_{\text{cl}})\leq\sqrt{\frac{3C_P}{C(f,2/3)}}.$$

We apply it to our protocol $\overline{P}$.

Our main claim is contained in *Theorem 1*:

Theorem 1. *Suppose two parties can compute a function f, using the protocol P with Q qubits of communication and the success probability* $2/3$*. Then there exist a quantum correlation* R_q *and a Bell inequality* $B_{f,P}$ *such that*

$$\frac{B_{f,P}(R_q)}{B_{f,P}(R_{\text{cl}})}\geq\frac{\sqrt{C(f,2/3)}}{6\sqrt{30Q}}\left(1-2^{-Q}\right)^{2Q},\quad\textbf{[6]}$$

where $C(f,2/3)$ *is the classical communication complexity of f with probability* $2/3$*, and* R_{cl} *stands for arbitrary classical correlation*.

Remark: *Theorem 1* implies that if Q^2 is sufficiently smaller than C (i.e., when we have a sufficiently large quantum advantage in communication complexity), then we obtain violation of a Bell inequality.

Proof: Given the protocol P of computing f with success probability $2/3=1/2+1/6$ (where we set $\epsilon=1/6$) while using Q qubits of communication, we consider protocol $\overline{P}$ from item *iii*, which uses $10Q^2$ bits of communication with the same probability of success. If applied to correlations R_q of item *ii* and using *Lemma 1* above, it achieves the success probability $1/2+(1-2^{-Q})^{2Q}(1/6)$. Thus, the Bell inequality $B_{f,\overline{P}}$ constructed in item *v* evaluated on R_q gives

$$B_{f,\overline{P}}(R_q)\geq\left(1-2^{-Q}\right)^{2Q}\frac{1}{6}.\quad\textbf{[7]}$$

The next step is to check the value of the same Bell inequality on classical correlations R_{cl}. To this end, we apply item *v* with $P=\overline{P}$, and $C_P=10Q^2$, obtaining that for any classical correlations R_{cl}

$$B_{f,\overline{P}}(R_{\text{cl}})\leq\sqrt{\frac{30Q^2}{C(f,2/3)}}.\quad\textbf{[8]}$$

We put together Eqs. **7** and **8**, obtaining the required bound for the ratio of Bell value on our particular quantum correlation R_q and arbitrary classical correlation R_{cl}:

$$\frac{B_{f,\overline{P}}(R_q)}{B_{f,\overline{P}}(R_{\text{cl}})}\geq\frac{\sqrt{C(f,2/3)}}{6\sqrt{30Q}}\left(1-2^{-Q}\right)^{2Q}.\quad\textbf{[9]}$$

□

For $C(f,2/3)\gg Q$ the right-hand side becomes large, implying large violation of a Bell inequality. The diagrammatic proof of *Theorem 1* is depicted in Fig. 4.

We provide several examples to demonstrate the power of our result.

Examples

Both of the examples are based on an explicit communication complexity problem called "vector in subspace" that was first

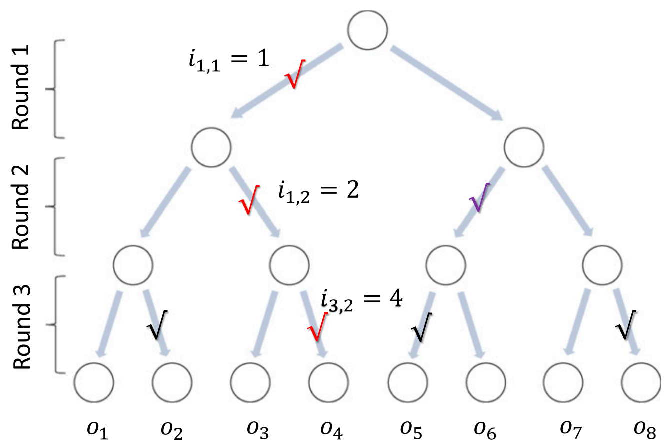

Fig. 3. Exchange of the information after simultaneous teleportations to reveal the path of the teleported system in a three-round protocol. After Alice's teleportation measurement in the first round the state ended up in port 1. Then, Bob teleports each of the two ports from the array that he used in the previous round, obtaining the outcomes 2 and 3 for ports 1 and 2, respectively. Finally, Alice performs a teleportation measurement for each of her four ports, obtaining the outcomes 2,4,5,8 for the ports 1,2,3,4, respectively. *A* defines a path *q* to be a sequence of teleportation outcomes: $q = \{i_{1,1} = 1, i_{2,1} = 2, i_{3,2} = 4\}$. The last node of the path points to the system, whose outcome provides Bob's guess. Recall that the measurements are performed at the same time, and the sequential multiround protocol consists only of the exchange of classical information obtained after teleportation. The latter is required to identify the last node of the path, which is used to make a guess about the value of the function.

introduced in ref. 5. In this problem, Alice and Bob receive the n-dimensional vector v and the description of $n/2$-dimensional subspace H, respectively, with the promise that either $v \in H$ or $v \in H^{\perp}$. The aim of the game is to determine which subspace v belongs to by exchanging messages between the parties. We consider two variants of the problem below.

Vector in Subspace Problem with One-Way Communication. In this protocol, there is only one round of communication from Alice to Bob. Also, the local memory is not used. The deterministic quantum protocol requires $\log n$ qubits of communication (where n is the length of the vector in the problem), whereas the classical communication complexity is $C(f, 2/3) = \Omega(\sqrt[3]{n})$ (8).

Knowing the quantum protocol P explicitly, we obtain a stronger Bell inequality because we do not need to invoke any approximations. Using $5 \log n$ bits of communication and correlations [**2**], we can achieve the quantum success probability of $p_q = 1/2 + 1/2(1 - 2^{-5 \log n})^{10 \log n}$, whereas the classical protocol using the same amount of communication achieves $p_c = 1/2 + \delta$, where $\delta^2 \le 5 \log n / A\sqrt[3]{n}$, for some constant A. Thus, the ratio of quantum to classical values of the Bell inequality given in *Theorem 1* is

$$\frac{B(R_q)}{B(R_{\mathrm{cl}})} = \frac{1/2(1 - 1/n)}{\sqrt{5 \log n / A\sqrt[3]{n}}} = \Omega\left(\frac{\sqrt[6]{n}}{\sqrt{\log n}}\right), \qquad [10]$$

where we use $B \equiv B_{f,P}$ when it does not lead to ambiguity.

Vector in Subspace Problem with Two-Way Communication [Raz Original Problem (5)]. In this protocol, Alice sends Bob a quantum state of size $\log n$ (where n is the length of the vector in the problem) and then receives a state of the same size. As in the previous example, the parties do not use any local memory. There exists a deterministic quantum protocol for this problem. The classical communication complexity is $C(f, 2/3) = \Omega(\sqrt[4]{n}/\log n)$. But using only $10 \log n$ qubits of communication and correlations [**2**], we get $p_q = 1/2 + (1 - 2^{-\log n})^2$. The classical protocol using the same amount of communication achieves $p_c = 1/2 + \delta$, where $\delta^2 \le c(10 \log^2 n / \sqrt[4]{n})$, for some constant A. Thus, the ratio of quantum to classical Bell values is

$$\frac{B(R_q)}{B(R_{\mathrm{cl}})} = \frac{1/2(1 - 1/n)^2}{\sqrt{10\, A \log^2 n / \sqrt[4]{n}}} = \Omega\left(\frac{\sqrt[8]{n}}{\log n}\right). \qquad [11]$$

One-Way Communication Complexity Problems. We now detail the scenario when Alice is allowed to send a single message to Bob to introduce a very different approach to obtain the violation of a Bell inequality. In this case, state preparation protocol on Alice's side followed by the measurement of a quantum state by Bob will suffice. Also, there is no need for the local quantum memory on either side because one does not have to preserve the state of the communication protocol. Therefore, the role of the port-based teleportation is played by the remote state preparation.

One marked difference of this approach is that it consumes a significantly smaller amount of entanglement. Also, in this setting, we obtain the nonlinear Bell inequality that explicitly features the probability of Bob guessing the communication from Alice—something that is not possible using the method that relies on the port-based teleportation.

We first outline the remote state preparation protocol and then construct the relevant Bell inequalities below.

Remote State Preparation. In the remote state preparation, Alice and Bob share a maximally entangled qudit state $|\Phi^+\rangle_{AB} = (1/\sqrt{d})\sum_{i=0}^{d-1} |i\rangle_A |i\rangle_B$. Alice wants to prepare a known quantum state $|\phi\rangle$ on Bob's side by acting only on her share of the qudit, requiring no postprocessing on his side. To achieve this, she performs a measurement with elements $\{|\phi^*\rangle\langle\phi^*|, \mathbb{I} - |\phi^*\rangle\langle\phi^*|\}$, where $|\phi^*\rangle$ is a conjugation of $|\phi\rangle$ in the computational basis, on her part of $|\Phi^+\rangle_{AB}$, followed by the communication of the classical outcome to Bob if she measured $|\phi^*\rangle\langle\phi^*|$ (we denote this outcome as 1). This protocol has a very low probability of success, $1/d$. We discuss the techniques to amplify it in *Supporting Information*, section II.

Correlations. Applying the remote state preparation protocol to our communication complexity problem, we obtain the correlations

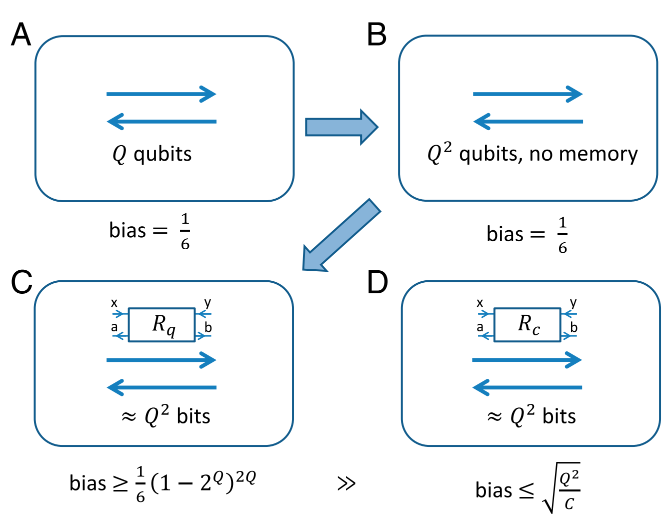

Fig. 4. The scheme of the proof of *Theorem 1*. (*A*) an initial protocol evaluating function *f* with bias 1/6, using *Q* qubits; (*B*) memoryless protocol, with the same bias, using Q^2 qubits; (*C*) protocol $\overline{P}$ using quantum correlations and Q^2 qubits, with bias still about 1/6; (*D*) protocol $\overline{P}$ gives small bias for any classical correlation R_c if Q^2 is sufficiently smaller than $C(f, 2/3)$.

$$p(a,b|x,y)=\mathrm{tr}\left[\left(M_x^a\otimes M_y^b\right)\rho_{AB}\right], \qquad [12]$$

where $\{M_x^a\}$ are the POVM elements from the remote state preparation and $\{M_y^b\}$ describes Bob's measurements on the shared state ρ_{AB}. In the current setup, the number of the binary observables of Alice and Bob is equal to the number of inputs x and y. The correlations [**12**] are obtained by acting on a single instance of the entangled state whereas the multiround approach uses in the order of 2^Q states. Merging m instances together, we obtain the set of correlations

$$p(\{i\},\{o_1,\ldots,o_N\}|x,y), \qquad [13]$$

where $i\in I$, $I=\{1,\ldots,m\}$ denotes the case when the remote state preparation succeeds and $\{o_i\}$ are the respective outputs. Thus, our Bell inequality may be written in the form [**3**]:

$$\sum_{x,y}\mu(x,y)\sum_{i\in I}p(i,o_i=f(x,y)|x,y)\le\frac{1}{2}+\delta. \qquad [14]$$

Nonlinear Bell Inequality. Here we derive a Bell inequality for the case where the parties have the option to abort at any stage of the protocol. Our inequality turns out to be nonlinear and will depend only on two parameters, p_A and p_B, defined as follows:

- p_A—probability that Alice succeeded, i.e., her outcome is 1 (averaged over all observables by the measure μ):

$$p_A=\sum_{x,y}\mu(x,y)p(a=1|x,y). \qquad [15]$$

This probability turns out to be equal to Bob successfully "guessing" the communication from Alice in the absence of communication from the latter.

- p_B—conditional probability that Bob's outcome is equal to value of the function, given that Alice succeeded:

$$p_B=\sum_{x,y}\mu(x,y)p(b=f(x,y)|x,y,a=1). \qquad [16]$$

Using roughly $m\approx 1/p_A$ instances of the state ρ_{AB}, Alice obtains one successful outcome $a=1$ on average. Then, Alice communicates to Bob this successful instance.

To obtain the inequality, we show how Alice and Bob may guess the correct value of the function. In this setup, as in the previous case, Alice uses $m\approx 1/p_A$ instances of the state ρ_{AB}. Then Alice communicates to Bob the first instance where the outcome appeared, using $\log m\approx -\log p_A$ bits. Finally, Bob looks at the outcome for the successful instance and with probability p_B obtains the value of the function f.

If Alice and Bob share a state that admits a local-realistic description, then the used communication cannot be smaller than the value $C(p_B,n)$, because it is the optimal value attainable by classical means. Thus, for any local-realistic state, we must necessarily have

$$\log\frac{1}{p_A}\gtrsim C(p_B,n). \qquad [17]$$

See *Supporting Information*, section III for further details.

Discussion

Examples show that our protocol produces large violations that are a bit weaker than the best known ones such as $n/\log^2 n$ (16) or $\sqrt{n}/\log n$ (9). This seems to be the price for its universality. However, it is an interesting open question, whether one can find a communication complexity protocol, such that the obtained Bell inequality would admit more dramatic violation than what is currently achievable. Another challenge is to decrease the amount of entanglement used to violate our Bell inequalities, which in our construction is exponential in the quantum communication complexity of the given problem. Similarly, the output size grows exponentially, which gives rise to the question of whether there exists a more efficient method of exhibiting the Bell nonlocality of quantum communication complexity schemes. The last two challenges could be addressed by devising a more efficient teleportation protocol or improving one of the existing ones (19). Finally, our method does not cover the protocols with initial entanglement. This is quite paradoxical, because protocols that use initial entanglement should be Bell nonlocal even more explicitly. It is therefore desirable to search for a method of demonstrating the Bell nonlocality of such protocols.

ACKNOWLEDGMENTS. Part of this work was done at the National Quantum Information Centre of Gdańsk as well as during the Program on Mathematical Challenges in Quantum Information, Isaac Newton Institute for Mathematical Sciences, 2013. This work is supported by European Commission (EC) IP QESSENCE, European Research Council (ERC) AdG QOLAPS, European Union (EU) project RAQUEL, Grant NCN Maestro (DEC- 2011/02/A/ST2/00305), the EU project SIQS, and MNiSW Grant IdP2011 000361. H.B. is partially funded through the Netherlands Organisation for Scientific Research Gravitation Grant Networks. S.S. acknowledges the support of Sidney Sussex College.

1. Bell JS (1964) On the Einstein-Podolsky-Rosen paradox. *Physics* 1(3):195–200.
2. Yao A-C (1979) Some complexity questions related to distributed computing. *Proceedings of 11th Annual ACM Symposium on the Theory of Computing*, eds Fischer MJ, Demillo RA, Lynch NA, Burkhard WA, Aho AV (ACM Press, New York), pp 209–213.
3. Yao A-C (1993) Quantum circuit complexity. *Proceedings of 34th IEEE Symposium on Foundations of Computer Science* (IEEE Computer Society, Palo Alto, CA), pp 352–360.
4. Cleve R, Buhrman H (1997) Substituting quantum entanglement for communication. *Phys Rev A* 56(2):1201.
5. Raz R (1999) Exponential separation of quantum and classical communication. *Proceedings of 31st Annual ACM Symposium on the Theory of Computing*, eds Vitter JS, Larmore L, Leighton T (ACM, New York), pp 358–367.
6. Buhrman H, Cleve R, Massar S, de Wolf R (2010) Nonlocality and communication complexity. *Rev Mod Phys* 82(1):665.
7. Buhrman H, Cleve R, van Dam W (2001) Quantum entanglement and communication complexity. *SIAM J Comput* 30:1829–1841.
8. Regev O, Klartag B (2011) Quantum one-way communication can be exponentially stronger than classical communication. *Proceedings of 43rd Annual ACM Symposium on Theory of Computing*, ed Vadhan S (ACM, New York), Vol 31, pp 31–40.
9. Buhrman H, Scarpa G, de Wolf R (2010) Better non-local games from hidden matching. *arXiv*:1007.2359.
10. Brukner C, Zukowski M, Pan J-W, Zeilinger A (2004) Bell's inequalities and quantum communication complexity. *Phys Rev Lett* 92(12):127901.
11. Junge M, et al. (2010) Unbounded violations of bipartite Bell inequalities via operator space theory. *Commun Math Phys* 300(3):715–739.
12. Ishizaka S, Hiroshima T (2008) Asymptotic teleportation scheme as a universal programmable quantum processor. *Phys Rev Lett* 101(24):240501.
13. Ishizaka S, Hiroshima T (2009) Quantum teleportation scheme by selecting one of multiple output ports. *Phys Rev A* 79(4):042306.
14. Kremer I (1995) Quantum communication. Master's thesis (Hebrew University, Jerusalem).
15. Bennett C (2005) Remote preparation of quantum states. *IEEE Trans Inf Theory* 51(1):56–74.
16. Buhrman H, Regev O, Scarpa G, de Wolf R (2011) Near-optimal and explicit Bell inequality violations. *IEEE Conference on Computational Complexity* (IEEE Computer Society, Washington, DC), Vol 157, pp 157–166.
17. Palazuelos C (2012) On the largest Bell violation attainable by a quantum state. *arXiv*:1206.3695.
18. Junge M, Palazuelos C (2011) Large violation of Bell inequalities with low entanglement. *Commun Math Phys* 306:695.
19. Pirandola S, Eisert J, Weedbrook C, Furusawa A, Braunstein S (2015) Advances in quantum teleportation. *arXiv*:1505.07831.
20. Kushilevitz E, Nisan N (2006) *Communication Complexity* (Cambridge Univ Press, Cambridge, UK).
21. de Wolf R (2001) Quantum computing and communication complexity. PhD thesis (University of Amsterdam, Amsterdam).
22. Buhrman H, de Wolf R (2001) Communication complexity lower bounds by polynomials. *16th Annual IEEE Conference on Computational Complexity*, 10.1109/CCC.2001.933879.