Bell's Inequalities and Quantum Communication Complexity

Časlav Brukner,[1] Marek Żukowski,[2] Jian-Wei Pan,[1] and Anton Zeilinger[1,3]

[1]*Institut für Experimentalphysik, Universität Wien, Boltzmanngasse 5, A-1090 Wien, Austria*
[2]*Institute Fizyki Teoretycznej i Astrofizyki Uniwersytet Gdański, PL-80-952 Gdańsk, Poland*
[3]*Institut für Quantenoptik und Quanteninformation, Österreichische Akademie der Wissenschaften, Boltzmanngasse 3, A-1090 Wien, Austria*

(Received 21 October 2002; revised manuscript received 8 December 2003; published 22 March 2004)

We prove that for every Bell's inequality, including those which are not yet known, there always exists a communication complexity problem, for which a protocol assisted by states which violate the inequality is more efficient than any classical protocol. Violation of Bell's inequalities is the *necessary* and *sufficient* condition for quantum protocol to beat the classical ones.

DOI: 10.1103/PhysRevLett.92.127901 PACS numbers: 03.67.Hk, 03.65.Ud, 03.67.Mn, 42.50.Ar

Entanglement is the essential feature which distinguishes the quantum from the classical [1]. On one hand, entangled states violate Bell inequalities, and thus rule out local realistic explanation of quantum mechanics [2]. On the other hand, they enable one to perform certain communication and computation tasks with efficiency not achievable by the laws of classical physics [3].

Communication complexity studies the amount of information that participants of a distributed system need to exchange in order to perform a certain task [4]. Consider two separated parties, Alice and Bob. She receives a data input x and he an input y. They do not know the data of the partner. The goal is for both of them to determine the value of a certain function $f(x, y)$. Before they start the protocol, they are allowed to share *classically correlated random strings* or any other local data, which may improve the success of the protocol. The obvious method to achieve the goal is that Alice communicates x to Bob, he computes the function $f(x, y)$, and communicates its value back to Alice. It is the topic of communication complexity to address questions such as: Could there be more communication efficient solutions for some functions? What are these functions?

This abstract problem has practical relevance for optimization of distributed computation and computer networks. In very large circuit integrated chips, for example, one wants to minimize energy use by decreasing the number of electric signals required between the different components during a distributed computation. For a survey of applications, see Ref. [5].

Generally, one can distinguish two types of communication complexity problems (CCPs), related to the following two questions: (i) What is the minimal amount of communication required for the parties all to determine the value of the function with certainty? (ii) What is the highest possible probability for the parties to arrive at the correct value of the function if only a restricted amount of communication is allowed? Here we consider the second class of problems. In this case, the correct value of the function does not have to be obtained with certainty; an error is allowed. The parties try to compute the function correctly with as high probability as possible. An execution is considered successful if the value given by all parties is correct.

From the perspective of quantum information the question is: Are there communication complexity tasks such that the parties can increase the success rate of solving the problem if they share prior entanglement, rather than classically correlated random strings [6–10]? Cleve and Buhrman [6] showed that entanglement can indeed be used to save on classical communication. In Ref. [7] is presented a two-party CCP that can be solved with a higher probability of success than classically if prior shared entanglement is available. The quantum protocol is based on the violation of Clauser-Horne-Shimony-Holt (CHSH) [11] inequality by the maximally entangled state. Similarly, the quantum protocols of multiparty problems of Refs. [7,8,12] were based on the Greenberger-Horne-Zeilinger (GHZ) [13] argument against local realism.

The question is which general states can lead to higher than classical probability of success. Here we will show that the necessary and sufficient condition for the quantum protocols of Refs. [6–8,12] to have a higher success rate than any classical protocol is that the state violates a Bell inequality. This is based on the observation that the quantum protocol can be seen as a modified test of Bell's inequality. The questions arise: Is this a general feature of all Bell's inequalities? Can one paraphrase every Bell's inequality in the context of CCPs?

The answers we give are positive: For every Bell's inequality, including those which are not known yet, there always exists a CCP, for which the protocol assisted by states which violate the inequality is more efficient than any classical protocol. As an explicit example, we will use the complete set of 2^{2^n} of n-qubit Bell's inequalities for correlation functions [14,15]. This includes the specific multiparty problems of Ref. [6–8,12] as special cases.

One might object that the CCPs considered here are (artificially) adapted to Bell's inequality. This is true but unimportant for two reasons: (i) Typical functions in the problems are related to such as sine and cosine which are

by no means artificial. (ii) From the quantum information perspective, we are interested only in CCPs for which quantum solution can have an advantage over the classical one. We show that, within the class considered, apart from the problems which are adapted to Bell's inequalities, there are no other such problems.

The two-party CCP of Ref. [7] is as follows. Alice receives a two-bit string $z_1 = (y_1, x_1)$ and Bob a two-bit string $z_2 = (y_2, x_2)$, where $y_1, y_2 \in \{-1, 1\}$ and $x_1, x_2 \in \{0, 1\}$. Their common goal is to compute the function (a reformulation of the original function of Ref. [7]),

$$f(z_1, z_2) = y_1 y_2 (-1)^{x_1 x_2}, \tag{1}$$

with as high a probability as possible, while exchanging altogether only two bits of information. All input strings are distributed with equal probability.

We will show that the quantum solution of this problem will have a higher success rate than the classical one if and only if one uses entangled states that violate the CHSH inequality.

We first present a class of classical protocols (which we prove to be optimal in the appendix). Alice calculates locally any function $a(x_1, \lambda_A)$ and Bob calculates locally any function $b(x_2, \lambda_B)$. Here λ_A and λ_B are any other parameters on which their functions a and b may depend. They, e.g., may include random strings of numbers, shared by Alice and Bob before they start the protocol. Alice sends $e_A = a y_1$ to Bob and Bob sends $e_B = b y_2$ to Alice. Upon the receipt of e_A and e_B, they both give $e_A e_B$ for the value of the function f.

Before showing the maximal probability of success in this protocol, we introduce its quantum competitor. Suppose Alice and Bob share a pair of entangled qubits. If Alice receives $x_1 = 0$, she will measure a two-valued observable A_0 on her qubit. For $x_1 = 1$, she will measure a different observable A_1. Bob follows the same protocol. If he receives $x_2 = 0$, he will measure observable B_0 on his qubit. For $x_2 = 1$, he will measure a different observable B_1. We ascribe to the two outcomes of the measurements the values ± 1. The value obtained by Alice in the given measurement will be denoted by a, whereas the one of Bob's by b (a and b play the similar role as in the classical protocol). Alice sends bit $e_A = y_1 a$ to Bob, and Bob sends bit $e_B = y_2 b$ to Alice. Finally, they both put $e_A e_B$ for the value of the function.

In both the classical and the quantum protocols, the task is to maximize the probability P for the product ab to be equal to $(-1)^{x_1 x_2}$. In the quantum case, this probability is given by

$$P = \tfrac{1}{4}[P_{A_0B_0}(ab = 1) + P_{A_0B_1}(ab = 1) + P_{A_1B_0}(ab = 1) + P_{A_1B_1}(ab = -1)], \tag{2}$$

where, e.g., $P_{A_0,B_0}(ab = 1)$ is the probability that the product ab is equal to one if Alice measures A_0 and Bob measures B_0. Recall that all four possible input combinations occur with the same probability 1/4.

It is crucial to notice that the classical protocols introduced above can be considered as local realistic models of the quantum protocol (λ are local hidden variables). Thus, the success probability P_C in the classical case is also given by Eq. (2). However, there exists a local realistic bound for P_C. Indeed $4P \leq 3$ is a version of the CHSH inequality [11]. Thus, P_C is bounded by 0.75. The quantum protocol will have higher success rate P_Q than the classical one P_C if, and only if, the two-qubit state violates the CHSH inequality. With the use of a maximally entangled state, one has $P_Q \approx 0.85$ [7].

Therefore, Bell's theorem provides an efficient solution of CCP of Ref. [7]. We now generalize this to an arbitrary number of parties and to various functions.

Consider n separated parties and any Bell inequality for correlation functions

$$\sum_{x_1,\ldots,x_n=0}^{1} g(x_1, \ldots, x_n) E(x_1, \ldots, x_n) \leq B(n). \tag{3}$$

Here g is a real function, $B(n)$ is a bound imposed by local realism, and $E(x_1, \ldots, x_n)$ denotes the correlation function $E(O^1_{x_1}, \ldots, O^n_{x_n})$, for measurements on n particles. The party i can measure one of the two dichotomic observables O^i_0 and O^i_1, each of spectrum ± 1.

Denote the outcome of the measurement obtained by party i by a_i. The correlation function is given by $E(x_1, \ldots, x_n) = P_{x_1,\ldots,x_n}(\prod_i a_i = 1) - P_{x_1,\ldots,x_n}(\prod_i a_i = -1)$, where $P_{x_1,\ldots,x_n}(\prod_i a_i = \pm 1)$ is the probability that the product of local measurement results $\prod_i a_i = \pm 1$ if the parties measure observables $O^1_{x_1}, \ldots, O^n_{x_n}$. It can be expressed as

$$E(x_1, \ldots, x_n) = S[g]\left[2P_{x_1,\ldots,x_n}\left(\prod_i a_i = S[g]\right) - 1\right], \tag{4}$$

where we introduce the sign function $S[g] = g/|g| = \pm 1$ of the function g. Using Eq. (4), one can easily show that the general Bell inequality (3) can be rewritten as

$$\sum_{x_1,\ldots,x_n} Q(x_1, \ldots, x_n) P_{x_1,\ldots,x_n}\left(\prod_i a_i = S[g]\right) \leq \frac{1}{2} + \frac{B(n)}{2\sum |g|}, \tag{5}$$

where Q is a probability distribution defined by

$$Q(x_1, \ldots, x_n) = \frac{|g(x_1, \ldots, x_n)|}{\sum_{x_1,\ldots,x_n=0}^{1} |g(x_1, \ldots, x_n)|}. \tag{6}$$

As we will see below, the left-hand side of inequality (5) will be equal to the probability of success in a class of CCPs adapted to the Bell inequality, whereas the right-hand side of inequality (5) will define its classical limit.

The class of our CCPs is as follows: (i) There are n parties. The ith party receives a two-bit input string

(x_i, y_i). (For convenience the values of the bits are encoded as follows: $x_i = 0$ or 1, and $y_i = -1$ or 1). (ii) The values of y_i are distributed randomly, whereas those of x_i in accordance with a probability distribution $Q(x_1, \ldots, x_n)$. Thus, the inputs $x_1, \ldots, x_n$ can in general be (classically) correlated. (iii) After receiving the input strings, each party is allowed to broadcast only *one bit* of information (denoted as e_i). It may reveal, e.g., a part of the received string, or some locally produced result of computation or measurement. (iv) Finally, each party attempts to give a value for the function $f(x_1, \ldots, x_n, y_1, \ldots, y_n) = \pm 1$, given by

$$f = y_1 y_2 \cdots y_n S[g(x_1, x_2, \ldots, x_n)]. \tag{7}$$

The execution of the protocol is successful when *all* parties arrive at the correct value of f. Their joint task is to maximize the probability of success. Various problems considered in Refs. [6–9,12] are particular cases from our class of problems with specific numbers n of parties and function g.

The optimal class of classical protocols (see appendix for the proof of optimality) is a generalization of the one discussed previously for the two-party problem. The party i calculates locally any function $a_i(x_i, \lambda_i)$, where λ_i $(i = 1, \ldots, n)$ again is a random string of variables shared among the parties before they start the protocol. Next, she/he broadcasts $e_i = a_i y_i$. After the broadcast, all parties put as the value of f the number $\prod_i e_i = \prod_i y_i a_i$, which is equal to the actual value of function f in a certain fraction of cases (see below).

Let us introduce a quantum competitor to the class of classical protocols considered above. The parties share n entangled qubits. Each of them can perform measurements of a two-valued observable on the local qubit. The quantum protocol reads (Fig. 1): If party i receives $x_i = 0$, she will measure observable O_0^i on her qubit. For $x_i = 1$ she measures a different observable O_1^i. The value obtained by party i is denoted again by a_i. The party

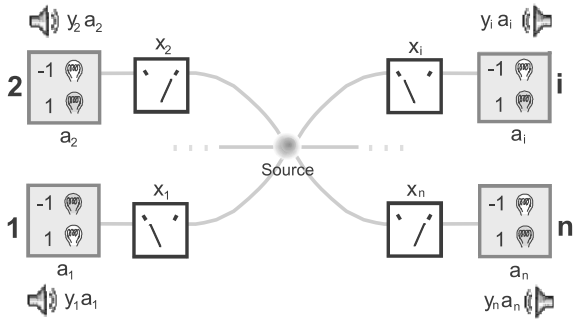

FIG. 1. Multiparty quantum communication complexity protocol based on Bell's experiment with n qubits. Party i receives a two-bit input string (x_i, y_i). Depending on the value of x_i, party i chooses to measure one of the two dichotomic observables O_0^i or O_1^i. The measurement result obtained by party i is $a_i = \pm 1$. Each party broadcasts $e_i = y_i a_i$.

broadcasts $e_i = a_i y_i$. Finally, all parties put as the value of f the number $\prod_i e_i = \prod_i y_i a_i$.

The probability of success in both the classical and the quantum protocols is equal to the probability P for the product $\prod_i a_i$ to be equal to $S[g]$. Thus, in both cases it can be expressed by the left-hand side of inequality (5), i.e., $P = \sum_{x_1,\ldots,x_n} Q(x_1, \ldots, x_n) P_{x_1,\ldots,x_n}(\prod_i a_i = S[g])$.

The classical protocols are again equivalent to local realistic models of the quantum protocol because the λ can be considered as local hidden variables. The probability of success in classical protocols is bounded by the inequality (5). In the quantum protocol, however, this limit can be exceeded. This will be the case if, and only if, the n-qubit state violates Bell's inequality.

Let us show some examples. The set of 2^{2^n} Bell's inequalities of the form (3) was obtained in Refs. [14,15]. There the class of functions g is given by $g(x_1, \ldots, x_n) = \sum_{s_1,\ldots,s_n=-1}^{1} S(s_1, \ldots, s_n) s_1^{x_1} \cdots s_n^{x_n}$, where $S(s_1, \ldots, s_n) = \pm 1$ is a sign function and the bound $B(n) = 2^n$. There are 2^{2^n} different sign functions and, thus, 2^{2^n} different functions g. Below, we give two explicit functions g from this class. We give only the final results, as they follow from the general proof given above.

Consider $S_{\text{odd}} = \sqrt{2}\cos[(s_1 + \cdots + s_n)\frac{\pi}{4}]$ for n odd and $S_{\text{even}} = \cos[(s_1 + \cdots + s_n)\frac{\pi}{4}]$ for n even. This implies $g_{\text{odd}} = \sqrt{2^{n+1}}\cos[\frac{\pi}{2}(x_1 + \cdots + x_n)]$ for n odd, whereas for n even one has $g_{\text{even}} = \sqrt{2^n}\cos[\frac{\pi}{2}(x_1 + \cdots + x_n)]$. The probability distribution $Q(x_1, \ldots, x_n)$ is such that only inputs x_i which satisfy the condition that $x_1 + \cdots + x_n$ is even are distributed (with equal probability). This type of problem was first considered in Refs. [7,8]. The quantum protocol rests on the violation of the Mermin inequality [16,17]. The maximal probability of success in the classical protocol is $P_C^{\max} = \frac{1}{2}(1 + 1/\sqrt{2^{n-1}})$ for n odd, and $P_C^{\max} = \frac{1}{2}(1 + 1/\sqrt{2^{n-2}})$ for n even. In the quantum case, with the use of n qubits in a GHZ state, the task can be performed with certainty, i.e., $P_Q^{\max} = 1$. This contrasts both classical cases, where in the limit $n \to \infty$ one has $P_C^{\max} \to 0.5$, just as for a random choice.

Next, suppose that the number n of parties is even and consider $S'_{\text{even}} = \sqrt{2}\cos[\frac{\pi}{4} + (s_1 + \cdots + s_n)\frac{\pi}{4}]$. This implies $g'_{\text{even}} = \sqrt{2^{n+1}}\cos[\frac{\pi}{2}(x_1 + \cdots + x_n) + \frac{\pi}{4}]$. The quantum protocol is now based on the violation of the Ardehali inequality [18,17]. The maximal probability of success in a classical protocol is $P_C^{\max} = \frac{1}{2}(1 + 1/\sqrt{2^n})$, whereas in the quantum protocol with the use of the GHZ state this probability reads $P_Q^{\max} = \frac{1}{2}(1 + 1/\sqrt{2})$. Thus, in this case one does not have certainty. Nevertheless, because Bell's inequality defined by g'_{even} is violated by the GHZ states by a higher factor than the one defined by g_{even}, the quantum protocol is more resistant to noise admixture to the GHZ states.

One can generalize our results to Bell's inequalities with higher-dimensional systems and more measurement

settings. If the inputs x_i have m possible values, then the quantum protocol should be adapted such that each party has a choice to measure between m measurement settings. Similarly, if the inputs y_i have d possible values and function $S[g]$ is replaced with one which has d possible values, then the quantum protocol should be based on the violation of Bell's inequalities for d-dimensional quantum systems [19]. Recently, one such protocol using entangled qutrits was proposed [20].

One can extend the notion of contradiction with local realism to include also the cases of violation of Bell's inequalities only after local operations and classical communication (LOCC) [21]. However, the states which violate Bell's inequalities only after LOCC cannot give any advantage over classical protocols in the class of CCPs considered here. Simply, LOCC transformation requires more communication than is permitted by the problems. However, if one extends the class of the problems by allowing more communication, such states could give an advantage.

M. Ż. is supported by the Professorial Subsidy of the Foundation for Polish Science (FNP). The work is supported by the Austrian FWF Project No. F1506, and by the European Commission, Contract No. IST-2001-38864 RAMBOQ, and is a part of the Austrian-Polish Program "Quantum Communication and Quantum Information."

Appendix.—Proof that the class of classical protocols considered in the main text is the optimal one.

For convenience, redefine the bit values x_i as $\tilde{x}_i = (-1)^{x_1} = \pm 1$. In general, the bit $e_i = \pm 1$, broadcast by the party i, is a function of *both* local inputs $\tilde{x}_i$ and y_i and has the general form

$$e(\tilde{x}_i, y_i) = a_i(\tilde{x}_i) + b_i(\tilde{x}_i)y_i, \tag{8}$$

where $|a_i(\tilde{x}_i)| + |b_i(\tilde{x}_i)| = 1$, and $|a_i(\tilde{x}_i)|, |b_i(\tilde{x}_i)| = 0$ or 1.

One can introduce the "answer" function, A, that Alice (say, partner 1) can use to give her best choice for the value of f. As the only data that she has are x_1, y_1, and $e_2, \ldots, e_n$, function A must be of the form $A(\tilde{x}_1, y_1, e_2(\tilde{x}_2, y_2), \ldots, e_n(\tilde{x}_n, y_n))$. Furthermore, as A is a function of $n+1$ bits, it can be decomposed as follows

$$A(\tilde{x}_1, y_1, e_2, \ldots, e_n) = \sum_{j_0,\ldots,j_n=0,1} A_{j_0\cdots j_n} \tilde{x}_1^{j_0} y_1^{j_1} \prod_{i=2}^{n} e_i^{j_i}, \tag{9}$$

where the expansion coefficients are given by

$$A_{j_0\cdots j_n} = \frac{1}{2^{n+1}} \sum_{\tilde{x}_1, y_1, e_2, \ldots, e_n = \pm 1} A(\tilde{x}_1, \ldots, e_n) \tilde{x}_1^{j_0} y_1^{j_1} \prod_{i=2}^{n} e_i^{j_i}. \tag{10}$$

Since the allowed values for A are ± 1, one has $|A_{j_0\cdots j_n}| \leq 1$.

As a measure of fidelity of function A with respect to f, we introduce their "weighted" scalar product

$$(f, A) \equiv \sum_{\tilde{x}_1, y_1, \ldots, \tilde{x}_n, y_n = \pm 1} \frac{1}{2^n} Q(\tilde{x}_1, \ldots, \tilde{x}_1) f(\tilde{x}_1, \ldots, y_n) A(\tilde{x}_1, \ldots, e_n), \tag{11}$$

where $1/2^n Q(\tilde{x}_1, \ldots, \tilde{x}_n)$ is the probability of the given sequence of inputs. The probability that Alice gives the correct value of f is given by $P = \frac{1}{2}[1 + (f, A)]$. Inserting the values of e_i as given by Eq. (8) into A and using definition (7) for f, one obtains

$$\frac{1}{\sum |g|} \sum_{\tilde{x}_1, \ldots, \tilde{x}_n \pm 1} g(\tilde{x}_1, \ldots, \tilde{x}_n)(A_{01\cdots 1} + A_{11\cdots 1}\tilde{x}_1) \prod_{i=2}^{n} b_i(x_i) \tag{12}$$

for (f, A). Using Eq. (10), one can easily show that $|A_{01\cdots 1} + A_{11\cdots 1}\tilde{x}_1| \leq 1$. Thus, due to Bell's inequality (3), the maximal possible value of (f, A) is given by $B(n)/\sum |g|$. Finally, since the classical protocol in the main text reaches this value for (f, A), it is optimal. QED

[1] E. Schrödinger, Naturwissenschaften **23**, 807 (1935); **23**, 823 (1935); **23**, 844 (1935).
[2] J. S. Bell, Physics (Long Island City, N.Y.) **1**, 195 (1964).
[3] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).
[4] A. C.-C. Yao, in *Proceedings of the 11th Annual ACM Symposium on Theory of Computing* (STOC 1978) (ACM Press, New York, 1979), pp. 209–213.
[5] E. Kushilevitz and N. Nisan, *Communication Complexity* (Cambridge University Press, Cambridge, England, 1997).
[6] R. Cleve and H. Buhrman, Phys. Rev. A **56**, 1201 (1997).
[7] H. Buhrman, R. Cleve, and W. van Dam, quant-ph/9705033.
[8] H. Buhrman *et al.*, Phys. Rev. A **60**, 2737 (1999).
[9] G. Brassard, quant-ph/0101005.
[10] L. K. Grover, quant-ph/9704012.
[11] J. Clauser *et al.*, Phys. Rev. Lett. **23**, 880 (1969).
[12] E. F. Galvao, quant-ph/0009014.
[13] D. M. Greenberger *et al.*, Am. J. Phys. **58**, 1131 (1990).
[14] R. F. Werner and M. M. Wolf, Phys. Rev. A **64**, 032112 (2001).
[15] M. Żukowski and Č. Brukner, Phys. Rev. Lett. **88**, 210401 (2002).
[16] N. D. Mermin, Phys. Rev. Lett. **65**, 1838 (1990).
[17] A. V. Belinskii and D. N. Klyshko, Phys. Usp. **36**, 653 (1993).
[18] M. Ardehali, Phys. Rev. A **46**, 5375 (1992).
[19] D. Kaszlikowski *et al.*, Phys. Rev. Lett. **85**, 4418 (2000); D. Collins *et al.*, Phys. Rev. Lett. **88**, 040404 (2002).
[20] Č. Brukner, M. Żukowski, and A. Zeilinger, Phys. Rev. Lett. **89**, 197901 (2002).
[21] S. Popescu, Phys. Rev. Lett. **74**, 2619 (1995).