Quantum Communication Complexity Protocols Based on Higher-Dimensional Entangled Systems

Časlav Brukner
Institut für Experimentalphysik, Universität Wien, Boltzmanngasse 5,
A–1090 Wien, Austria, email: caslav.brukner@univie.ac.at

Tomasz Paterek
Instytut Fizyki Teoretycznej i Astrofizyki, Uniwersytet Gdański,
PL-80-952 Gdańsk, Poland, email: pater@univ.gda.pl

Marek Żukowski
Instytut Fizyki Teoretycznej i Astrofizyki, Uniwersytet Gdański,
PL-80-952 Gdańsk, Poland, email: zukowski@ap.univie.ac.at

We introduce new communication complexity problems whose quantum solution exploits entanglement between higher-dimensional systems. We show that the quantum solution is more efficient than the broad class of classical ones. The difference between the efficiencies for the quantum and classical protocols grows with the dimensionality of the entangled systems.

I. INTRODUCTION

To date only very few tasks in quantum communication and quantum computation exploit higher-dimensional systems. One such example is quantum-key distribution based on higher alphabets which was shown to be more secure than the one based on qubits.[1] It is therefore highly desirable to find new tasks which either require higher-dimensional entanglement to breach the classical limits, or for which the separation between efficiency of quantum and classical solution increases with the dimensionality of the entangled systems.

Communication complexity studies the amount of communication that the participants of a communicating system need to exchange in order to perform a task [2]. Typically there are two separated parties, conventionally called Alice and Bob, who receive some data of which they only know their own data and not the data of the partner. For example, Alice receives an input x and Bob receives y. Their common goal is to determine the value of some given function $f(x, y)$ exchanging as little communication as possible. This situation is known as a "communication complexity problem" (see Ref. [3] for a survey of applications).

We consider a specific type of communication complexity problems (CCPs) in which one asks what is the highest possible probability for the parties to arrive at the correct value of the function, under the condition of *restricted* communication. The parties try to compute the function correctly with maximal probability. An execution is considered successful, if the value given by all parties is correct. Classically, the parties are allowed to share random strings or any other local data which might improve the success rate of the protocol. In 1997 Cleve and Burhman showed that there are CCPs for which the parties can increase the success rate, if they share prior entangled quantum systems, rather than classically correlated random strings [4].

There is a strong link between violation of local realism (i.e. violation of Bell's inequalities) and CCPs [5]. In Ref. [6] a two-party problem was found whose quantum solution was based on the violation of the Clauser-Horne-Shimony-Holt inequality [7]. Similarly the quantum solutions of specific multi-party problems were based on a Greenberger-Horne-Zeilinger argument against local realism [6, 8–10]. Finally, it was shown that one can link a CCP with every Bell inequality for qubits [11]. However, if the inequalities involve higher dimensional objects, new possibilities emerge.

Here we give quantum communication complexity protocols based on higher-dimensional entangled systems. For a wide class of classical protocols we find *an increase in the separation between the efficiency of the quantum and classical strategies, which grows with the dimensionality of the entangled systems*. We show that the quantum protocol is more efficient than the classical ones if and only if the protocol participants can share a state that violates the CGLMP inequalities for higher-dimensional systems [12]. The results form a generalization of those of Ref. [13] to arbitrarily high-dimensional systems. Despite the fact that the CCPs considered here may seem to be artificial, we think that it points a new link between Bell's theorem and CCPs.

II. QUANTUM COMMUNICATION COMPLEXITY PROBLEMS WITH QUDITS

Let us now define the two-party communication complexity problem which will be our case of study. This problem is a generalization of the one presented in Ref. [13]. A certain number of questions, about values of some d-valued

functions, is posed to the parties. The parties are restricted both in communication as well as in broadcasting their answers. Specifically, the parties must give single answer to $2[d/2]$ questions ($[x]$ stands for the integer part of the number x), basing on the local inputs which they obtained, known only locally, and the value of a dit (a generalization of a bit, to a unit of information which can have d values) broadcast by the partner. The integer d describes the number of possible answers to each question. Further, the parties are not allowed to differ in their answers. That is, they must produce two identical answers each time.

Formally the $2[d/2]$ questions will be formulated as a problem of computation of $[d/2]$ functions f_k^+ ($k = 1, ..., [d/2]$) and $[d/2]$ functions f_k^- ($k = 1, ..., [d/2]$). The parties are allowed to give only one answer to the question about the values of all $2[d/2]$ functions and their goal is to give the correct value of $[d/2]$ functions f_k^+, with the highest possible probability, and *at the same time*, the correct value of $[d/2]$ functions f_k^- with the lowest possible probability. Before putting the value to all these functions, the parties can broadcast only one dit of information. The questions are not treated equally. The importance of questions changes with the weight $1 - \frac{2k}{d-1}$.

We now introduce the two-party task in detail and give all the functions explicitly: Alice receives a data string $\alpha = (a_{bit}, a_{dit})$ and Bob a string $\beta = (b_{bit}, b_{dit})$. Alice's string is a combination of a bit $a_{bit} \in \{0, 1\}$ and a dit $a_{dit} \in \{1, \gamma, \gamma^2, \ldots, \gamma^{d-1}\}$ where $\gamma = e^{i(2\pi/d)}$. We use this specific notation for the values of dits in order to simplify the formulas for the functions. Similarly Bob's string is a combination of a bit $b_{bit} \in \{0, 1\}$ and a dit $b_{dit} \in \{1, \gamma, \gamma^2, \ldots, \gamma^{d-1}\}$. All possible input strings are distributed randomly and with equal probability. Before they broadcast their answers, Alice and Bob are allowed to exchange two dits of information. Alice and Bob each broadcast her/his answer in the form of one dit. The two answers must be identical. That is, each party broadcast the same one dit. The task of Alice and Bob is to maximize (having in mind the weight of the questions) all differences between the probabilities $P(f_k^+)$, of giving the correct value for the functions

$$f_k^+ = a_{dit} b_{dit} \gamma^{a_{bit} b_{bit} + k(-1)^{a_{bit} + b_{bit}}}, \quad k = 0, \ldots, [d/2] - 1, \tag{1}$$

and $P(f_k^-)$, of giving the correct value for the functions

$$f_k^- = a_{dit} b_{dit} \gamma^{a_{bit} b_{bit} + (k+1)(-1)^{a_{bit} + b_{bit} + 1}}, \quad k = 0, \ldots, [d/2] - 1. \tag{2}$$

That is, they aim at the maximal value of

$$\Delta = \sum_{k=0}^{[d/2]-1} \left(1 - \frac{2k}{d-1}\right) \left(P(f_k^+) - P(f_k^-)\right). \tag{3}$$

We will show that, if two parties use a class of classical protocols (optimality of which will be shown elsewhere), the difference Δ introduced above is at most 0.5, whereas if they use two entangled qudits this difference can be larger. Furthermore the difference increases with d.

III. QUANTUM VERSUS CLASSICAL PROTOCOL

Note that the first factor $a_{dit} b_{dit}$ in the full functions $f_k^{\pm}$ results in completely random values if only one of the independent inputs a_{dit} or b_{dit} is random. This is not the case for the last factors with inputs a_{bit} and b_{bit}. Thus, intuition suggests that good classical protocol for the two parties may be that Alice "spends" her dit by sending a_{dit} and Bob by sending b_{dit} and that they put for the part of f's dependent on the bits the value most often appearing in the third column and, at the same time, least often appearing in the fourth column of the Table 1. Moreover, because of the weight function they should give preference to the values connected with functions for $k = 0$. The second factor of f_0^+ is equal to 1 in three out of four cases, whereas f_0^- is 1 in one of four cases. Thus if each of them broadcasts the value $a_{dit} b_{dit}$ as her/his answer, $\Delta = 1(0.75 - 0.25) = 0.5$.

Let us now present the optimal class of classical protocols which can be followed by Alice and Bob, and which contains the above intuitive example as a special case: Alice calculates locally any function $a(a_{bit}, \lambda_A)$ and Bob calculates locally any function $b(b_{bit}, \lambda_B)$. Here λ_A and λ_B are any other parameters on which their functions a and b may depend. They may include random strings of numbers shared by Alice and Bob before the protocol started. Alice sends to Bob $e_A = a_{dit} a$ and receives from him $e_B = b_{dit} b$. Upon receipt of e_A and e_B, they both broadcast $e_A e_B$ as their answers (which always agree). Note, that our intuitive protocol is reproduced by $a = 1$ and $b = 1$ for all inputs.

Before showing what is the maximal Δ achievable for such a wide class of classical protocols, we shall introduce its quantum competitor. Let Alice and Bob share a pair of entangled qudits and suitable measuring device (see, e.g. Ref. [14]). This is their quantum protocol: If Alice receives $a_{bit} = 0$, she will measure her qudit with the apparatus which

TABLE I: A set of possible input values for a_{bit} and b_{bit} and the corresponding values of the exponents of $f_k^{\pm}$.

a_{bit}	b_{bit}	$a_{bit}b_{bit} + k(-1)^{a_{bit}+b_{bit}}$	$a_{bit}b_{bit} + (k+1)(-1)^{a_{bit}+b_{bit}+1}$
0	0	k	$-(k+1)$
0	1	$-k$	$k+1$
1	0	$-k$	$k+1$
1	1	$k+1$	$-k$

is set to measure a d-valued observable A_0. Otherwise, i.e., for $a_{bit} = 1$, she sets her device to measure a different d-valued observable A_1. Bob follows the same protocol. If he receives $b_{bit} = 1$, he measures the d-valued observable B_1 on his qudit. For $b_{bit} = 0$ he measures a different d-valued observable B_0. We ascribe to the outcomes of the measurements the d values $1, \gamma, \gamma^2, \ldots, \gamma^{d-1}$. The actual value obtained by Alice in the given measurement will be denoted again by a, whereas the one of Bob's, also again, by b. Alice sends dit $e_A = a_{dit}a$ to Bob, and Bob sends dit $e_B = b_{dit}b$ to Alice. They both broadcast $e_A e_B$ as their answers.

The task in both protocols is to maximize Δ defined by (3). The probability $P(f_k^+)$ is the probability for the product ab (of the local measurement results in the quantum case, and the local functions in the classical case) to be equal to the part of the functions f_k^+ which depends only on a a_{bit} and b_{bit}:

$$P(f_k^+) = \frac{1}{4}\Big[P_{01}(ab = \gamma^{-k}) + P_{11}(ab = \gamma^{k+1})$$
$$+ P_{10}(ab = \gamma^{-k}) + P_{00}(ab = \gamma^{k})\Big], \tag{4}$$

where e.g. $P_{01}(ab = \gamma^{-k})$ is the probability that $ab = \gamma^{-k}$ if she receives $a_{bit} = 0$, and he $b_{bit} = 1$. In the quantum case the probabilities on right hand side of Eq. (4) are probabilities for certain products of measurement results, whereas in the classical case they are probabilities for the products of locally computed functions, where the λ_A's and λ_B's are distributed according to probability distribution $\rho(\lambda_A, \lambda_B)$ (note that this distribution cannot depend upon the strings received by Alice and Bob after the initialization of the protocol). Recall that all four possible combinations for a_{bit} and b_{bit} occur with the same probability $\frac{1}{4}$. Similarly, the probability $P(f_k^-)$ is given by

$$P(f_k^-) = \frac{1}{4}\Big[P_{01}(ab = \gamma^{k+1}) + P_{11}(ab = \gamma^{-k})$$
$$+ P_{10}(ab = \gamma^{k+1}) + P_{00}(ab = \gamma^{-(k+1)})\Big]. \tag{5}$$

Finally, one notices that the success measure in the task is given by

$$\Delta = \frac{1}{4}I_d, \tag{6}$$

where I_d is just left hand side of CGLMP inequality [12]. The equivalence of I_d and Collins *et al.* inequalities may not be obvious at the first glance because in Ref. [12] authors ascribe to local measurement results integers $0, 1, \ldots, d-1$ and use modulo d calculus; however, the difference between that description and the one used here is just in the notation. Collins *et al.* showed that $I_d \leq 2$ for all local realistic theories.

If one looks back at the family of classical protocols introduced above, one sees that they are equivalent to a local realistic model of the quantum protocol (λ's are local hidden variables, and a_{bit}, b_{bit} are local variables which define the measurements). This implies that within the full class of classical protocols considered here $\Delta \leq 0.5$.

Thus, the necessary and sufficient condition for the state of two qudits to improve the success in the communication complexity task over any classical protocol of the discussed class is that the state violates the Bell inequality for two qudits.

It was shown in Ref. [15] that nonmaximally (asymmetric) entangled states of two qudits can violate the CGLMP inequalities stronger than the maximally entangled one. Maximal violations for some d and corresponding probabilities for success in the CCP are gathered in the Table 2.

Therefore, in a classical protocol, even with shared random variables, more than two dits of information exchange are necessary to complete the task successfully with $\Delta > 0.5$, whereas with quantum entanglement two dits can be sufficient for the task with the same Δ. Note that the discrepancy between the measure of success in the classical and the quantum protocol grows with d.

TABLE II: Maximal violation of CGLMP inequalities and corresponding measures for success in the CCP. The Δ_Q denotes the quantum success measure and Δ_C the classical one. The values of maximal violations are taken from the work of Acin *et al.*.

d	Maximal violation	Δ_Q	$\Delta_Q - \Delta_C$
3	2.9149	0.7287	0.2287
4	2.9727	0.7432	0.2432
5	3.0157	0.7539	0.2539
6	3.0497	0.7624	0.2624
7	3.0776	0.7694	0.2694
8	3.1013	0.7753	0.2753

We would like to stress that asking all $2[d/2]$ questions is not necessary to prove the advantage of the quantum protocol. As showed in Ref. [13] even one question f_0^+ is sufficient for an advantage of quantum strategy over the classical ones, but asking all questions maximizes the advantage.

IV. CONCLUDING REMARKS

One can generalize the scheme to more than two parties. Our results suggest that Bell's inequalities might have a significance beyond that of a non-optimal witness of non-separability. In view of the fact that to date only very few quantum information procedures use higher-dimensional systems as resources, the development of quantum communication complexity protocols exploiting the entanglement between such systems might open a new avenue of research.

[1] N. J. Cerf *et al.*, Phys. Rev. Lett. 88, 127902 (2002); D. Bruß *et al.*, *ibid*, 127901.
[2] A. C.-C. Yao, in *Proceedings of the 11th Annual ACM Symposium on Theory of Computing*, 209-213 (1979).
[3] E. Kushilevitz and N. Nisan, *Communication Complexity* (Cambridge University Press, 1997).
[4] R. Cleve and H. Buhrman, Phys. Rev. A **56**, 1201 (1997).
[5] J. S. Bell, Physics (Long Island City, N.Y.) **1**, 195 (1964).
[6] H. Buhrman, R. Cleve and W. van Dam, e-print quant-ph/9705033.
[7] J. Clauser *et al.*, Phys. Rev. Lett. **23**, 880-884 (1969).
[8] H. Buhrman, *et al.*, Phys. Rev A **60**, 2737 (1999).
[9] E. F. Galvao, e-print quant-ph/0009014.
[10] D. M. Greenberger *et al.*, Am. J. Phys. **58**, 1131 (1990).
[11] Č. Brukner, M. Żukowski, J. Pan, A. Zeilinger, arXiv: quant-ph/0210114.
[12] D. Collins, N. Gisin, N. Linden, S. Massar, and S. Popescu, Phys. Rev. Lett. **88**, 040404 (2002).
[13] Č. Brukner, M. Żukowski, and A. Zeilinger, Phys. Rev. Lett. **89**, 197901 (2002).
[14] M. Żukowski, A. Zeilinger, and M. A. Horne, Phys. Rev. A **55**, 2564 (1997).
[15] A. Acin, T. Durt, N. Gisin, and J. I. Latorre, Phys. Rev. A **65**, 052325 (2002).