Quantum communication complexity advantage implies violation of the Bell inequality

H. Buhrman, L. Czekaj, A. Grudka, M. Horodecki,
P. Horodecki, M. Markiewicz, F. Speelman, S. Strelchuk *

Abstract

We obtain a general connection between a quantum advantage in communication complexity and non-locality. We show that given any protocol offering a (sufficiently large) quantum advantage in communication complexity, there exists a way of obtaining measurement statistics which violates 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 with the increase in the number of inputs and outputs becomes unbounded.

The key element which distinguishes classical from quantum information theory is quantum correlations. Their strength and the mysterious nature was first recognized in the EPR paradox [1] and then quantitatively expressed in Bell's theorem [2]. 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 [3, 4, 5] producing surprising results [6, 7].

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 inputs $x \in X = \{0,1\}^n$ and $y \in Y = \{0,1\}^n$ respectively, distributed according to some apriori distribution μ. They wish to compute the value of $f : X \times Y \to \{0,1\}$ 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, two parties, Alice and Bob, share a maximally entangled state $|\Psi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)_{AB}$ beforehand and are allowed to exchange classical bits in order to solve the problem. Another approach is to have no pre-shared entanglement, but instead allow Alice and Bob to exchange qubits. The latter protocol can always be converted to the former with pre-shared entanglement and classical communication. We denote quantum communication complexity of computing the function $f(x,y)$ (with bounded probability of success) as $Q(f)$.

*H. Buhrman and F. Speelman are with Centrum Wiskunde & Informatica (CWI), A. Grudka is with Adam Mickiewicz University, M. Horodecki, M. Markiewicz and L. Czekaj are with Gdańsk University, P. Horodecki is with Gdańsk University of Technology, S. Strelchuk is with the University of Cambridge.

For a large number of problems, the respective quantum communication complexity is much lower compared to its classical counterpart [5, 8].

In such cases, we say that there exists a *quantum advantage for communication complexity.* In other words, one achieves 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 [6, 9] 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 [10]. The latter inequality plays an important role in detecting quantum correlations and certifying the genuinely quantum nature of resources at hand.

As a matter of fact, the very first protocols offering quantum advantage were based on a quantum violation of certain Bell inequalities [7]. It was even shown that for a very large class of multiparty Bell inequalities, correlations which violate them lead to a quantum advantage (perhaps, for a peculiar function) [11]. This indicates that non-locality often leads to a quantum advantage. However, there are more and more communication protocols which offer a quantum advantage, but, nevertheless, they are not known to violate any Bell inequality. We ask the opposite question:

Q: *Does quantum advantage in communication complexity inherently rely on the non-local nature of correlations?*

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 whose statistics violate some Bell inequality. The first case is the "hidden matching" problem and the second one – a theorem, which states that a special subset of protocols that provide quantum advantage also imply the violation of local realism [7]. To get the violation of Bell inequalities obtained from the examples above, one had to perform an involved analysis which 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.

Our main result is that for *any* given protocol which operates without prior entanglement, and offers a (sufficiently large) quantum advantage in communication complexity, there exists a way of obtaining measurement statistics which violate some *linear* Bell inequality. Thus, whenever we find such a protocol which computes the value of function $f(x, y)$ and achieves $Q(f) < C(f)$, then it must harbor some non-local quantum correlations.

We provide a universal method which takes a protocol that achieves the quantum advantage in any single- or multi-round 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 then two parties. Our Bell inequalities lead to the so-called unbounded violation, (see [12]): 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 $C(f) > (Q(f))^4$. In particular, the exponential advantage leads to the exponential ratio.

Examples show that our protocol produces large violation which is a bit weaker than the best known one: $\frac{n}{\log^2 n}$ [16]. 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 be in some respect better than existing large Bell violations. 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, so there is a question, whether there exists a more efficient method of exhibiting the non-locality of quantum communication complexity schemes. Finally, our method does not cover the protocols with initial entanglement. This is quite paradoxical, because protocols that use initial entanglement should be non-local even more explicitly. It is therefore desirable to search for a method of demonstrating the non-locality of such protocols.

Construction.
Our method consists of two parts. In the first part, given the protocol which computes function f by using $Q(f)$ qubits, and the optimal classical error probability achievable with $(Q(f))^4$ bits, we construct the corresponding linear Bell inequality. In the second part, we use the quantum protocol to construct a set of quantum measurements on maximally entangled state which leads to the violation of the Bell inequality above. The central ingredient of our construction is the recently-discovered port-based teleportation [13, 14].

Proof ingredients.
Firstly, we start with quantum multi-round protocol to compute f which uses quantum communication and no shared entanglement. This protocol requires Q qubits of communication and achieves $p_{succ} \geq 1/2 + \epsilon$. In this protocol, Alice and Bob may use local quantum memory between rounds. Second, we construct the protocol without local quantum memory which increases the cost of communication to $O(Q^2)$. This is achieved using the consequence of Yao's Compression Lemma [4, 15]:

Lemma 1. *For any Q-qubit quantum communication protocol (without prior entanglement) there exists an $Q^2 + 2Q$-qubit quantum communication protocol such that Alice and Bob do not need any local quantum memory that persists between the rounds.*

The memoryless protocol is then used to obtain correlations $\mathcal{P}$ which together with classical communication are used to recover the original communication complexity protocol which computes f. The last part of the puzzle is a method of simulating the memoryless quantum protocol using the above correlations and classical communication:

Lemma 2. *Given the memoryless protocol for computing f which uses Q qubits of communication and achieves the success probability $p_{succ} \geq 1/2 + \epsilon$, $\epsilon > 0$, one can simulate it using correlations $\mathcal{P}$ and $O(Q^2)$ bits of classical communication with the success probability $p_{succ} \geq 1/2 + (1 - 2^{-Q})^{2Q}\epsilon$.*

Now, if for a function $f(x, y)$ there exists a gap between $C(f) > Q^4(f)$ with $p_{succ} = 1/2 + \delta$ for the classical communication complexity protocol, and $\delta \ll \epsilon$ – then we observe the quantum violation of the Bell inequality of the form:

$$\sum_{x,y} \mu(x, y) \sum_{(i_1,\ldots,i_{2r-1}) \in I} p(o_{i_{2r-1}} = f(x, y)|x, y) \leq 1/2 + \delta, \tag{1}$$

where μ is a probability measure on $X \times Y$, the set I 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. For all levels but the last one, every node on i-th level has N_i children which correspond to the outcome of the i-th round of teleportation. The leaves of the tree correspond to the outcomes of Bob's binary observable, which is his guess of the value of the function $f(x, y)$.

References

[1] A. Einstein, B Podolsky, N. Rosen, Phys. Rev. 47, 777 (1935).

[2] J. S. Bell, Physics 1, 195 (1964).

[3] A. C. Yao, Proc. of 11th STOC 209 (1979)

[4] A. C. Yao. In Proceedings of 34th IEEE FOCS, 352 (1993).

[5] R. Cleve, H. Buhrman, Phys. Rev. A **56**, 1201 (1997), arXiv:9704026

[6] R. Raz. In Proc. of 31st Annual ACM Symposium on the Theory of Computing, 358 (1999).

[7] H. Buhrman, R. Cleve, S. Massar, R. de Wolf; Rev. Mod. Phys. **82**, 665698 (2010), arXiv:0907.3584

[8] H. Buhrman, R. Cleve, W. van Dam SIAM J.Comput. 30 (2001) 1829-1841, arXiv:9705033

[9] O. Regev, B. Klartag, Proc. of STOC '11 the 43rd annual ACM symposium on Theory of computing, 31 (2011), arXiv:1009.3640.

[10] H. Buhrman, G. Scarpa, R. de Wolf, arXiv:1007.2359

[11] C. Brukner, M. Zukowski, J.-W. Pan, A. Zeilinger, Phys. Rev. Lett. **92**, 127901 (2004), arXiv:0210114

[12] M. Junge, C. Palazuelos, D. Perez-Garcia, I. Villanueva, M.M. Wolf, Comm. Math. Phys. **300**, 715 (2010), arXiv:0910.4228

[13] S. Ishizaka, T. Hiroshima, Asymptotic teleportation scheme as a universal programmable quantum processor. Physical Review Letters, 101(24):240501 (2008)

[14] S. Ishizaka, T. Hiroshima, Quantum teleportation scheme by selecting one of multiple output ports, Phys. Rev. A 79, 042306 (2009)

[15] I. Kremer. Quantum Communication. Master's thesis, 1995

[16] H. Buhrman, O. Regev, G. Scarpa, R. de Wolf, lations, IEEE Conference on Computational Complexity, 157 (2011), arXiv:1012.5043

[17] C. Palazuelos, arXiv:1206.3695