Universal scheme for violation of local realism from quantum advantage in one-way communication complexity

L. Czekaj,1 A. Grudka,2 M. Horodecki,1 P. Horodecki,3 and M. Markiewicz1

1Faculty of Mathematics, Physics and Informatics, Gdańsk University, 80-952 Gdańsk, Poland
2Faculty of Physics, Adam Mickiewicz University, Umultowska 85, 61-614 Poznań, Poland
3Faculty of Applied Physics and Mathematics, Gdańsk University of Technology, 80-952 Gdańsk, Poland

We consider relations between communication complexity problems and detecting correlations (violating local realism) with no local hidden variable model. We show first universal equivalence between characteristics of protocols used in that type of problems and non-signaling correlations. We construct non linear bipartite Bell type inequalities and strong nonlocality test with binary observables by providing general method of Bell inequalities construction and showing that existence of gap between quantum and classical complexity leads to violation of these inequalities. We obtain, first to our knowledge, explicit Bell inequality with binary observables and exponential violation.

PACS numbers:

Key element which distinguishes classical and quantum world are quantum correlations. The strength of these correlations was first realized in EPR paradox [1] and then quantitatively expressed in Bell theorem [2]. Although non-signaling, they cannot be reduced to local hidden variable model. This property leads to another approach to understanding quantum correlations, where they are taken as a resource which abridges "hardness" of certain information processing tasks [3–5]. Reduction of communication cost of solving certain distributed computational problems by use of quantum correlations is the result on this ground which emphasizes non-local character of quantum correlations [3–6].

For a long time violation of local realism (i.e. existence of correlations that cannot be described by local hidden variable model) was of interest of philosophically oriented physicists, and was considered as a kind of exotic peculiarity, that does not affect our life. Quantum information era has completely reversed this picture: local realism and its quantum mechanical violation has become a practical resource. One area, where quantum mechanical violation has practical implications is communication complexity. An everyday task is to compute some function of distributed arguments. For example, "doodle" utility allows to schedule appointment for distant parties. Now the question is: how much information needs to be exchanged to find the time slot which will be suitable for all parties?

The amount of bits needed to exchange in order to solve some common problem is called communication complexity. Restricting to two parties (Alice and Bob), we consider a function $f(x, y)$, such that Alice has $x$ and Bob has $y$. We assume some apriori distribution over $x, y$, and ask about communication complexity, i.e. the number of bits needed to exchange in order to compute the function by e.g. Bob. It turns out that if Alice and Bob share an entangled state they may need to exchange much less bits, than when they share classical correlations (aka shared randomness) [8–10]. Intuitively this means, that the statistics of outcomes of measurement performed on such state must violate local realism. Indeed, if it were possible to describe the statistics in a local realistic way, this would mean that instead of having such entangled state, we might have used a local realistic model, which is nothing more than classical shared randomness. Therefore, the number of bits could not have been smaller than needed in classical case. Putting it in a different way: if the results of measurement exist prior to the measurement, equally well, the experiment could be simulated by writing those preexisting values on a piece of paper, and then simply reading them out.

This intuition is confirmed by many examples: first protocols of quantum advantage were based on known earlier examples of violation of local realism, manifested by violation of Bell inequalities [3]. Moreover it was shown that all Bell inequalities of certain type lead to a quantum advantage (for a perhaps peculiar function [11]).

Instead of sharing entanglement, Alice and Bob might be allowed to transmit qbits. For this scheme the quantum advantage (i.e. that one needs to send considerable less amount of qubits than bits) is also manifested for some functions. Such a scheme can always be converted to the scheme, where the parties send bits, and share entangled state. Most profound is here the famous Raz protocol [3, 10], where the quantum advantage over classical communication complexity is exponential. Another prominent example is so called "hidden matching", which served to obtain superstrong violation of Bell inequality [11].

However, despite the clear intuition, there is no universal protocol of the following sort: given quantum advantage in communication complexity, provide a violation of some Bell inequality. The mentioned example of Bell inequality obtained from "hidden matching" is based on some special symmetries. Also a general theorem, which says that quantum advantage implies violation of local realism, requires some very particular symmetries of the quantum protocol [6].
In this paper, we are going to describe a universal method, which given any quantum advantage (with one-way communication) allows to construct a relevant Bell inequality. The Bell inequality is nonlinear (cf. entropic Bell inequalities [12]), i.e. it says that some nonlinear function of joint probabilities of the measurements performed on a state, must be in some way bounded, if the statistics can be explained by local realistic theories. More precisely, we exhibit two constructions for given function $f(x, y)$:

(i) classical bound on minimum communication required to compute $f \rightarrow$ Bell inequality,

(ii) quantum protocol using qbits to compute $f \rightarrow$ quantum measurements on maximally entangled state.

The implication (i) is obtained using techniques analogous to the ones in the proof of Theorem 11 in [13], where upper bound for quantum communication complexity in case of inefficient detectors [14] is proposed. By a slight modification of the proof of Theorem 11 we derive a Bell inequality instead of upper bound. The proof of implication (ii) involves, in particular remote state preparation protocol [15].

The basic feature of the above two constructions is that: Whenever there is a quantum advantage, i.e. a quantum protocol requires less qbits than the classical bound, then the statistics of the constructed measurements violate the derived Bell inequality.

The constructions are summarized on FIG. 1.

We apply the constructions to obtain the strongest nonlocality test using binary observables. Namely, if we consider random noise, then admixing just $p = \sqrt{\log n}/\sqrt{n}$ of maximally entangled bipartite state causes violation. Here $n$ denotes size of each party subsystem expressed in qbits. To our knowledge, this is the first exponential violation of bipartite Bell inequality with binary observables. Presented Bell-type inequalities are less sensitive in detection of local realism violation than well known "hidden matching" Bell inequality [6, 11] ($p \gtrsim \log n/\sqrt{n}$).Khot and Vishnoi game [16, 17] ($p \gtrsim \log^2 n/n$) or even earliest examples of bipartite Bell inequalities with large violation [18, 19], however the others utilize observables with $n$ outputs. Reduction of number of observable outputs is important from experimental point of view.

It is well known that maximal quantum violation of Bell inequalities with binary observables as well as their resistance to any type of noise is bounded by Grothendieck constant, so that there is no room for unbounded violations [20]. This might seem to contradict our result. However here we discuss only robustness under admixing a particular type of classical state, i.e. isotropic noise. This kind of robustness is important from practical point of view, since isotropic noise appears usually in experimental realisations.

We will now briefly describe the constructions of the Bell inequality and quantum measurements and provide examples illustrating how they work. Some notions from communication complexity are described in more detail in Appendix A. Good introduction to the topic gives [3].

**Bell inequality from classical bounds on communication complexity.** Suppose we know the following classical communication complexity result: to obtain probability of success $p_S$ of computing a function $f(x, y)$ by Alice and Bob, where $(x, y)$ are a priori distributed according to probability distribution $\mu(x, y)$, Alice needs to send $C(p_S, n)$ bits, where $n$ is the size of the problem (e.g. if $x, y \in A$, then $n = \log |A|$).

We will then obtain Bell inequality, which says that arbitrary statistics that are explainable by local realism have to obey some constraints. Our inequality will be nonlinear. It will be derived for the following setup: Alice (Bob) has as many binary observables as there are inputs $x (y)$. The inequality will depend only on two parameters:

- $p_A$ - probability that Alice’s outcome is 1 (averaged with measure $\mu$ over all observables)

\[
p_A = \sum_{x, y} \mu(x, y)p(\alpha = 1|x, y).
\]
instance, she will obtain outcome of the state. Alice is almost sure, that at least for one \( C \) for some fixed probability of success, usually classical (local) distributions.

which is an analogue of the Theorem 11 in [13] for our Bell inequality (3). As the state we will take a classical observable \( B \) for protocols with one-way communication: indeed, Alice needs \( \log d \) bits to inform Bob, at which pair she succeeded to obtain outcome 1. In such case, she prepared remotely \( \psi_x \) at Bob’s side. Therefore, we obtain \( p_B = \frac{2}{3} \). If we plug in these values to the inequality \( 3 \) we obtain:

\[
Q \geq C
\]

Thus, whenever for a given problem there is a quantum advantage in communication complexity, i.e. \( Q \) is smaller than \( C \), the statistics violates local realism expressed by Bell inequality \( 3 \). Since in most cases the complexities \( Q \) and \( C \) are found up to a constant factor, we can say, that the inequality is violated whenever \( Q \) is smaller than \( C \) multiplied by some constant. We see, that the violation is precisely of order of a gap between classical and quantum communication complexity (in case of e.g. exponential separation we obtain a large violation).

Quantum measurements on bipartite state from quantum protocol. Suppose, now that there is a quantum protocol, which requires a smaller number of qubits \( Q(\frac{2}{3}, n) \) (denoted later by \( Q \)) than the number \( C(\frac{2}{3}, n) \) of bits needed by optimal classical protocol (denoted later by \( C \)). We will now find measurements on a quantum bipartite state, whose statistics will violate our Bell inequality \( 3 \). As the state we will take a maximally entangled state of two systems, each consisting of \( Q \) qubits.

Arbitrary quantum protocol works as follows: Alice prepares state \( \psi_x \), sends it to Bob, who measures binary observable \( B_y \). Since \( \psi_x \) is known, it is natural to use remote state preparation \( 13 \) instead of quantum state transmission for non-locality test. Now, our measurements on bipartite state will be the following: Bob will measure the same observable, i.e. \( B_y \), while Alice will measure simply \( |\psi_x^\ast\rangle\langle\psi_y^\ast| \) (i.e. up to complex conjugate \( * \) it is the projector onto the state, she would prepare in the communication complexity protocol). To see, whether Bell inequality is violated, we need to find the values of \( p_A \) and \( p_B \) of our proposed measurement. Clearly, \( p_B = \frac{2}{3} \), since if Alice obtained outcome 1 (i.e. she measured \( |\psi_x^\ast\rangle\langle\psi_y^\ast| \)), this means that she prepared \( \psi_x \) on Bob’s side, which is as if the state was sent to Bob i.e. as if the quantum protocol were implemented. In such a case, Bob guesses function with probability \( \frac{2}{3} \) (as we assumed about the quantum protocol). Moreover, \( p_A = 1/d \) where \( d \) is dimension of Alice’s Hilbert space, but this is equal to \( 2^Q \), since \( Q \) is the number of qbits of subsystem. The scheme of the construction is presented on FIG. 2b).

Quantum violation. Let us now argue, that the quantum statistics obtained from the above construction will violate our Bell inequality. To this end, note that the obtained statistics allows to compute function \( f \) with probability \( \frac{2}{3} \) with small amount of communication: indeed, Alice needs \( \log d \) bits to inform Bob, at which pair she succeeded to obtain outcome 1. In such case, she prepared remotely \( \psi_x \) at Bob’s side. Therefore, we obtain \( p_B = \frac{2}{3} \). If we plug in these values to the inequality \( 3 \) we obtain:

\[
\log \frac{1}{p_A} \geq C(p_B, n), \tag{3}
\]

which is an analogue of the Theorem 11 in [13] for classical (local) distributions.

This is Bell’s inequality obtained from known communication complexity bounds, which is obeyed by statistics obtained from all states that admit local realistic description.

We should mention here, that a typical result from communication complexity is optimal number of bits for some fixed probability of success, usually \( p = 2/3 \), while the above inequality requires to know \( C(p_A, n) \) for all \( p_A \). However by a standard pumping argument (see Appendix B), one finds that \( C(\frac{2}{3} + \epsilon, n) \geq \frac{1}{4} C(\frac{2}{3}, n) \) for \( p_A = \frac{2}{3} \). Plugging it into \( 3 \) we obtain the following Bell inequality, that uses \( C(\frac{2}{3}, n) \):

\[
\log \frac{1}{p_A} \geq \frac{1}{3} \left( p_B - \frac{1}{2} \right)^2 C\left( \frac{2}{3}, n \right). \tag{4}
\]

Quantum measurements on bipartite state from quantum protocol. Suppose, now that there is a quantum protocol, which requires a smaller number of qbits \( Q(\frac{2}{3}, n) \) (denoted later by \( Q \)) than the number \( C(\frac{2}{3}, n) \) of bits needed by optimal classical protocol (denoted later by \( C \)). We will now find measurements on a quantum bipartite state, whose statistics will violate our Bell inequality \( 3 \). As the state we will take a maximally entangled state of two systems, each consisting of \( Q \) qbits.

Arbitrary quantum protocol works as follows: Alice prepares state \( \psi_x \), sends it to Bob, who measures binary observable \( B_y \). Since \( \psi_x \) is known, it is natural to use remote state preparation \( 13 \) instead of quantum state transmission for non-locality test. Now, our measurements on bipartite state will be the following: Bob will measure the same observable, i.e. \( B_y \), while Alice will measure simply \( |\psi_x^\ast\rangle\langle\psi_y^\ast| \) (i.e. up to complex conjugate \( * \) it is the projector onto the state, she would prepare in the communication complexity protocol). To see, whether Bell inequality is violated, we need to find the values of \( p_A \) and \( p_B \) of our proposed measurement. Clearly, \( p_B = \frac{2}{3} \), since if Alice obtained outcome 1 (i.e. she measured \( |\psi_x^\ast\rangle\langle\psi_y^\ast| \)), this means that she prepared \( \psi_x \) on Bob’s side, which is as if the state was sent to Bob i.e. as if the quantum protocol were implemented. In such a case, Bob guesses function with probability \( \frac{2}{3} \) (as we assumed about the quantum protocol). Moreover, \( p_A = 1/d \) where \( d \) is dimension of Alice’s Hilbert space, but this is equal to \( 2^Q \), since \( Q \) is the number of qbits of subsystem. The scheme of the construction is presented on FIG. 2b).

Quantum violation. Let us now argue, that the quantum statistics obtained from the above construction will violate our Bell inequality. To this end, note that the obtained statistics allows to compute function \( f \) with probability \( \frac{2}{3} \) with small amount of communication: indeed, Alice needs \( \log d \) bits to inform Bob, at which pair she succeeded to obtain outcome 1. In such case, she prepared remotely \( \psi_x \) at Bob’s side. Therefore, we obtain \( p_B = \frac{2}{3} \). If we plug in these values to the inequality \( 3 \) we obtain:

\[
Q \geq C \tag{5}
\]

Thus, whenever for a given problem there is a quantum advantage in communication complexity, i.e. \( Q \) is smaller than \( C \), the statistics violates local realism expressed by Bell inequality \( 3 \). Since in most cases the complexities \( Q \) and \( C \) are found up to a constant factor, we can say, that the inequality is violated whenever \( Q \) is smaller than \( C \) multiplied by some constant. We see, that the violation is precisely of order of a gap between classical and quantum communication complexity (in case of e.g. exponential separation we obtain a large violation).

Results in rigorous form, and implications. Now we formulate a rigorous version of the Bell inequality \( 3 \), which directly involves the size of the inputs of a protocol. An analogous version of inequality \( 4 \) is given in Appendix C.

Theorem 1 Let \( C_\mu(f, n, p_A^S) \) be a communication complexity of function \( f \) for protocols with one-way classical communication, success probability \( p_A^S \) and inputs of size \( n \) randomized according to probabilistic measure \( \mu \). All correlations parameterized by \( p_A \) and \( p_B \) (cf. 11 and 2) with local hidden variable model fulfill:

\[
[\log 1/p_A + \log \log 1/\delta] + 1 \geq C_\mu(f, n, (1-\delta)p_B+\delta/2), \tag{6}
\]

where \( \delta \) is free parameter which may be optimized to achieve the largest set of detectable quantum correlations.
For definitions and rigorous proof see Appendix C. The consequence of (6) are the following inequalities for fixed error quantum protocol:

$$Q_\mu(f,n,2/3) \geq \frac{1}{432} C_\mu(f,n,2/3) - 2$$

(7)

and for error-free quantum protocol:

$$Q_\mu(f,n,1) \geq C_\mu(f,n,2/3) - 2,$$

(8)

which are more formal analogues of (5). Here $C_\mu(f,n,2/3)$ is defined as in Thm. 1 and $Q_\mu(f,n,p_S)$ is communication complexity of quantum protocol.

**Theorem 2** If there exists a quantum protocol with advantage in the communication complexity over classical one, i.e. violating the inequality (7) or (8), then quantum correlations which violate Bell inequality (3) might be obtained by construction (ii).

Conditions (7) and (8) might be stated in more general form (for discussion and derivation see Appendix C).

To give some intuition, we present in FIG. 3 $C_\mu(f,n,p_B)$ and minimal log $1/p_A$ attainable by classical correlations for vector in subspace problem (the problem is described in the further part of the paper). Exact formulae used to obtain FIG. 3 are described in Appendix D.

Below we discuss our method by means of several examples. They are well known results on quantum advantage, where asymptotic bounds are known, for large size of the problem.

![FIG. 2: Schemes of the constructions provided in the paper: a) classical communication protocol utilizing correlations $p(a,b|x,y)$; b) measurements on maximally entangled state derived from the quantum communication protocol that give correlations $p(a,b|x,y)$: the label “$\psi_a$” means that Alice successfully prepared state $\psi_a$ on Bob’s site while “$\psi^+_a$” means that she failed; detailed description is provided in text.](image)

![FIG. 3: Quantum violation detected by Bell-type inequality constructed for vector in subspace problem for some fixed problem size $n$. Values of $C_\mu(f,n,p_B)$ (solid line, cf. (3) and Appendix B) and $\log 1/p_A$ (boundary of the shaded area, cf. (9)) presented on the Y axis in the same scale. Here we can distinguish three regions: (i) the region below $\log 1/p_A$ curve (shaded area) situates quantum correlations which are detected by our Bell-type inequality; (ii) the area between $\log 1/p_A$ and $C_\mu(f,n,p_B)$ refers to protocols which outperform classical one but do not lead to correlations violating Bell inequality; (iii) above $C_\mu(f,n,p_B)$ is regime of classical protocols. For large problem size $n$, region (ii) becomes relatively small.](image)

The first example we discuss in this paper concerns vector in subspace problem (VSP). Here Alice receives $n$-dimensional vector $v$ and Bob $n/2$-dimensional space $H$. There is promise that $v \in H$ or $v \in H^\perp$. Bob has to decide which one is true. The problem has real inputs, however it might be discretized in an easy way. Exponential separation for one-way quantum and classical protocols was shown in [10]. Classical communication complexity for that problem obeys

$$C_\mu(2/3,n) \geq c\sqrt{n}$$

(9)

for $n$ large enough and some fixed constant $c$, while there is deterministic quantum protocol which requires only $\log n$ qubits of communication. We consider fixed problem size $n$ for which Alice’s Hilbert space has dimension $n$. This leads to probability $p_A = 1/n$ (cf. (11)). Deterministic quantum protocol means that $p_B = 1$. Since communication cost of protocol increase with its success probability $p_S$, taking $\delta$ such that $(1 - \delta) > 2/3$ we get quantum violation of Bell inequality (8), i.e.

$$\log n + \log \log 1/\delta < c\sqrt{n},$$

(10)

for large $n$.

We will illustrate how Bell inequality constructed from VSP performs in high dimensional spaces on the example of isotropic state $\psi_{iso} = p\Phi^+ + (1-p)I/n^2$. Simple calculations (see Appendix E) show that Bell inequality is violated if for small $\delta$ and sufficiently...
large $n$ we have
\[
\log n + \log \log 1/\delta < \frac{1}{3} \left( 1 - \delta \right)^{P/2} c' \sqrt{n}.
\] (11)

Therefore nonlocality is detected for $p$ decreasing slower than $\sqrt{\log n}/\sqrt{n}$ with $n$.

In a similar manner we obtain quantum violation of Bell inequality (13) for functional formulation of hidden matching problem ($\alpha$PHM) introduced in [21]. For input size $n$ large enough we get:
\[
c' \log(n)/\alpha + \log \log 1/\delta < \frac{1}{3} \left( \frac{1 - \delta}{6} \right)^2 c'' \sqrt{n}/\alpha.
\] (12)

We put constants $c'$ and $c''$ since quantum and classical communication complexities are known up to the multiplicative constant. Here nonlocality is detected for isotropic state when $p$ decrease slower that $\sqrt{\log n}/\sqrt{n}$.

While our method works for standard communication complexity problems, where the amount of communication is a function of size of the problem which can grow, we can also apply it to some extent to problems with constant size. We illustrate it in Appendix F by means of a problem based on so called random access code, which is the problem of effective encoding of 2 bits into one bit (qbit). For isotropic states, this inequality has the same detection power as original CHSH inequality. For more details see Appendix F.

Authors would like to thank Bo’az Klartag, Marius Junge, Carlos Palazuelos and Marcin Pawlowski for discussion. This work was supported by ERC grant QOLAPS (29148) and project QUASAR. MM is supported by International PhD Project: “Physics of future quantum basen information technologies” grant MPD/2009-3/4 and by the NCN grant No. 2012/05/E/ST2/02352. Part of this work was done in National Quantum Information Center of Gdansk.

I. APPENDIX

A. General introduction

At the beginning of the appendix we describe in more detail various communication scenarios which appear in the context of communication complexity. We define success probability and communication complexity. Then we provide pumping argument, rigorous derivation of Bell inequality and we analyze classical protocols for RAC problem.

Protocol is a set of rules that determine how Alice and Bob communicate and how they compute their outputs according to given inputs. It is kind of recipe how to accomplish distributed computational task.

Instead of calculation of function $f$ as it took place in the paper, Alice and Bob might be asked to calculate relation. It means that for certain input pair, more than one output is acceptable result. Message passing in the protocol might be one-way from Alice to Bob or iterative - protocol might be split into rounds where Alice sends message to Bob or Bob sends message to Alice. Depending on the message type, communication is classical or quantum. Further distinctions relate to additional resources available for players. There might be no additional resources, private randomness, shared randomness, shared entanglement and such exotic resource as shared PR-boxes. It is known that some resources may drastically change complexity of the problem, e.g. shared randomness may reduce communication exponentially by the cost of success probability, shared PR-boxes make any problem trivial since any problem might be solved with 1 bit of communication. Some resources might be interchanged, e.g. shared entanglement and classical communication might be replaced by quantum communication, shared randomness might be replaced by private randomness with additional small amount of communication. Protocols with randomness $r$ might be decomposed into probabilistic mixture of deterministic ones while protocols with shared entanglement do not have such decomposition.

Protocol $\Pi$ succeeds if it is able to accomplish the task $\Pi(x,y) = f(x,y)$ (similarly for relations), where $\Pi(x,y)$ denotes protocol outcome. The measure of that event is success probability $p_S$ which is defined as worst case success probability $p_S^W = \min_{x,y} p_r(\Pi(x,y) = f(x,y))$ or weighted success probability $p_S^W = \sum_{x,y} \mu(x,y) p_r(\Pi(x,y) = f(x,y))$ according to some probabilistic measure $\mu$ on the input space. Protocol which calculates function $f$ for a given problem of size $n$ and success probability $p_S$ requires $k$ bits (qbits) of communication. Communication complexity for fixed $f, p_S, n$ is the minimum of $k$ over protocols from appropriate class.

We will denote communication complexity of classical protocols with classical shared resources and worst case success probability as $R$ (randomized protocols), with classical shared resources and success probability weighted according to $\mu$ as $C_\mu$ (distributional protocols) and communication complexity of protocols with quantum communication as $Q$ (quantum protocols). The following relation holds: $C_\mu \leq R$.

$C_\mu$ is bounded by communication complexity of distributional deterministic protocol. To see this, let us express randomized protocol as a convex combination of deterministic protocols. For fixed $f, p_S, n, \mu$ and
amount of communication we have:

\[ p_S \leq \sum_{x,y} \mu(x, y)p(\Pi(x, y) = f(x, y)) \]  

(13)

\[ = \sum_{x,y} \mu(x, y) \left( \sum_r p_r(\Pi_r(x, y) = f(x, y)) \right) \]  

(14)

\[ = \sum_r p_r \left( \sum_{x,y} \mu(x, y)\mathbb{I}(\Pi_r(x, y) = f(x, y)) \right) \]  

(15)

\[ \leq \max_r \left( \sum_{x,y} \mu(x, y)\mathbb{I}(\Pi_r(x, y) = f(x, y)) \right) \]  

(16)

The last step is valid since deterministic protocol with higher success probability may be always taken. This result means that shared randomness does not help in distributional problems, however it is necessary to use pumping argument. It also means that we do not need to know \( C_{\mu} \) but communication complexity of distributional deterministic protocol is enough for our purpose.

Now we put in more formal form the statement provided at the beginning of the paper, that quantum correlations which lead to communication advantage have to violate local realism. Let \( c_{\mu}(\Pi) \) be communication required by protocol \( \Pi \) which calculates function \( f \) in setup parametrized by \( \mu, p^*_S, n \), then:

\[ c_{\mu}(\Pi) \geq C_{\mu}. \]  

(17)

Since the amount of communication increases with \( p^*_S \), communication complexity provides maximal value \( p^*_S \) of success probability among protocols with fixed amount of communication \( C_{\mu} \). This leads to another inequality

\[ p^*_S(\Pi) \leq \frac{\epsilon^2}{C_{\mu}} \]  

(18)

which is complementary to \([17] \).

### B. Pumping argument

We move to the pumping argument, which is based on well known techniques of increasing the success probability by repetition of randomized protocol \([22]\), and prove the following bound for communication required in randomized algorithm:

\[ C(p_S) \geq \frac{1}{3} \left( p_S - \frac{1}{2} \right)^2 C \left( \frac{2}{3} \right) \]  

(19)

where \( C(p_S) \) stands for communication complexity of arbitrary (quantum or classical) randomized protocol and \( c \) is a constant. The bound is valid for \( \frac{1}{2} < p_S < \frac{2}{3} \).

We use pumping argument to show that smaller \( C(p_S) \) enables to construct protocol which uses less communication than \( C(\frac{2}{3}) \) to achieve \( p_S = \frac{2}{3} \) and hence leads to contradiction.

Let the protocol \( \Pi \) uses \( C(\frac{1}{2} + \epsilon) \) bits of communication to achieve \( p_S = \frac{1}{2} + \epsilon \). Let us consider protocol \( \Pi' \)

in which Alice and Bob repeat \( l \) times protocol \( \Pi \) and then Bob returns as an answer the most often output of \( \Pi \). Since we are restricted to Boolean functions, the success probability \( p'_S \) of \( \Pi' \) is equal to the probability that protocol \( \Pi \) gives correct answer no less than \( \lceil l/2 \rceil + 1 \) times. By the Chernoff bound we get:

\[ p'_S \geq 1 - \exp \left( -\frac{1}{2} l \epsilon^2 \right). \]  

(20)

Since we require that \( p'_S \geq \frac{2}{3} \) we get that

\[ l \geq \frac{3}{\epsilon^2}. \]  

(21)

From communication complexity bound, for \( p_S = \frac{2}{3} \), protocol \( \Pi' \) requires at least \( C(\frac{2}{3}) \) bits of communication. On the other hand, protocol \( \Pi' \) repeats \( l \) times protocol \( \Pi \) and uses \( l C(\frac{1}{2} + \epsilon) \) bits of communication. Putting this together, we have:

\[ l C \left( \frac{1}{2} + \epsilon \right) \geq C \left( \frac{2}{3} \right). \]  

(22)

Using relation \([21] \) we get finally:

\[ C \left( \frac{1}{2} + \epsilon \right) \geq \frac{\epsilon^2}{3} C \left( \frac{2}{3} \right). \]  

(23)

For \( \frac{1}{2} + \epsilon = \frac{2}{3} \) our estimation leads to communication complexity bound \( 1/108 \) \( C(\frac{2}{3}) \) which is much below true value. This discrepancy comes from nonoptimality of pumping protocol.

### C. Rigorous derivation of Bell inequality and Bell inequality violation

Here we show rigorous derivation of Bell inequality:

\[ \left[ \log 1/p_A + \log \log 1/\delta \right]+1 \geq C_{\mu}(f, n, (1-\delta)p_A + \delta/2). \]  

(24)

We do this by explicit construction of one-way protocol with classical communication and shared resources from given correlations. We restrict our considerations to the family of correlations \( p(a, b|x, y) \) with \( x, y \in \{0, 1\}^n \), \( a, b \in \{0, 1\} \). \( a = 1 \) is interpreted as an acceptance signal. In that case we will expect that \( b = f(x, y) \). We do not lose generality since we might always take negation of \( a, b, x, y \) which is local operation. As described before, for our purposes it is enough to look only at parameters \( p_A \) and \( p_B \) of the correlations:

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

(25)

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

(26)

We show that correlation \( p(a, b|x, y) \) characterised by \( n, p_A \) and \( p_B \) leads to protocol \( \Pi_P \) solving problem
of size $n$ using $[\log 1/p_A + \log \log \delta] + 1$ bits of communication and achieving $p_S^Q = (1 - \delta)p_B + \delta/2$ for weight $\mu(x, y)$.

Protocol $\Pi_B$ works as follows. Let Alice and Bob share $[k/p_A]$ instances of correlations. They use their inputs $x, y$ to select proper measurements. Alice sends to Bob index $i$ of first correlation where she gets $a = 1$. Bob takes the result $b$ for the correlation $i$ and returns it as an output of protocol $\Pi_B$. In case when none of boxes returned $a = 1$, the message ABORT is sent to Bob and he returns a random bit.

Protocol requires $[\log k/p_A]$ bits of communication to encode index of the box and 1 extra bit to encode the message ABORT. Probability that Alice gets $a = 1$ for at least one instance is $1 - (1 - p_A)^{k/p_A} \geq 1 - 2^{-k}$. In that case Bob returns proper value with probability $p_B$. If Bob obtains message ABORT, he returns proper value with probability $1/2$. Putting $\delta = 2^{-k}$ we get overall success probability $p_S^Q = (1 - \delta)p_B + \delta/2$ with communication of $[\log 1/p_A + \log \log 1/\delta] + 1$ bits.

By (17), for all boxes with local hidden variable model we get:

$$[\log 1/p_A + \log 1/\delta] + 1 \geq C_{\mu}(f, n, (1 - \delta)p_B + \delta/2).$$

(27)

In case when communication complexity is given only for fixed $p_S = \frac{2}{3}$, by the pumping argument and the fact that $C_{\mu}(\frac{2}{3}, n) \leq C_{\mu}(p_S, n)$ for $p_S \geq \frac{2}{3}$ we obtain

$$[\log 1/p_A + \log \log 1/\delta] + 1 \geq \frac{1}{3}((1 - \delta)p_B + \delta/2 - \frac{1}{3})^2 C_{\mu}(\frac{2}{3}, n)$$

if $(1 - \delta)p_B + \delta/2 \leq \frac{2}{3}$,

$$C_{\mu}(\frac{2}{3}, n)$$

if $(1 - \delta)p_B + \delta/2 > \frac{2}{3}$.

Using the fact, that correlations obtained from quantum protocol with communication complexity $Q$ and success probability $p_S$ are characterized by $p_A = 2^{-Q}$ and $p_B = p_S$ and putting that into (24), we may rewrite Thm. 1 in the following form:

**Proposition 1** Let $C_{\mu}(f, n, p_S^Q)$ be defined as in Thm. 1. If correlations obtained by construction (ii) from quantum protocol with success probability $p_S$ and communication complexity $Q$ do not violate local realism in terms of Bell inequality (13), then communication complexity of the protocol obeys:

$$Q(f, n, p_S^Q) \geq \max_\delta (C_{\mu}(f, n, (1 - \delta)p_S + \delta/2) - \log \log 1/\delta - 2).$$

(29)

Inequality (29) is rigorous version of inequality (28). Inequality (13) is immediate consequence of the above proposition obtained for $\delta = 1/2$ from the pumping argument (see Appendix B). To obtain inequality (29) it is enough to take $\delta = 2/3$ and $p_S = 1$.

To state quantum violation of Bell inequality, it is enough to know only asymptotic results like domination of $C_{\mu}(f, n, p_S^Q)$ over $Q_{\mu}(f, n, p_S^Q)$ for some fixed $p_S^Q \geq p_S^C$ (we say that function $g(n)$ dominates $h(n)$ if for any constant $k$ there exists $n_0$ such that for any $n > n_0$ there is $k g(n) \geq h(n)$). Then by definition we get that for $n$ large enough (20) is violated.

**D. Explicit Bell inequality for VSP problem**

Bound for classical communication complexity in FIG. 3 is obtained from bounded error communication complexity and the pumping argument and it has form

$$C_{\mu}(\nu) = \left\{ \begin{array}{ll} \frac{1}{3}(p - 1/2)^2 \sqrt{n} & \text{if } p \leq \frac{2}{3} \\ \sqrt{n} & \text{if } p > \frac{2}{3} \end{array} \right. (30)$$

Here we omitted scaling constant since it may be putted under the $\sqrt{n}$ term which is equivalent to scaling of the problem size $n$. $\log 1/p_A$ is obtained by numerical optimisation of the following expression:

$$\log 1/p_A = \max_\delta C_{\mu}(\nu) \delta ((1 - \delta)p_B + \delta/2, n) + \log_2 \log 1/\delta$$

(31)

for $n = 10^4$.

**E. VSP Bell inequality violation for isotropic states**

Let us consider quantum measurement on bipartite state for quantum VSP protocol in the context of isotropic state $\psi_{\text{iso}} = p\Phi^+ + (1 - p)\mathbf{1}/n^3$. Since there is deterministic quantum protocol which solves the problem using $\log n$ qubits of communication, we have that $p_B = 1$ for correlations obtained for $\Phi^+$ state. On the other hand, if completely mixed state is shared Bob’s output is random and $p_B = \frac{1}{2}$. For both cases $p_A = 1/n$. It means that for isotropic state, despite the fact that $p_B$ is nonlinear function of state, it is probabilistic combination of $p_B$ for those two cases and we have $p_B = \frac{p}{2} + \frac{1}{2}$. Putting $\epsilon = (1 - \delta)(\frac{p}{2} + \frac{1}{2}) + \frac{p}{2} - \frac{1}{2}$ into (26), we obtain Bell inequality for VSP in the small $p_S$ regime and for $n$ large enough:

$$\log n + \log \log 1/\delta \geq \frac{1}{3}((1 - \delta)p)^2 \sqrt{n}. (32)$$

This inequality leads to relation:

$$\frac{\sqrt{3}(1 - \delta)}{2}\sqrt{\log n + \log \log 1/\delta} / \sqrt{n} \geq p. (33)$$

Now, if $p$ decrease slower than $\sqrt{\log n} / \sqrt{n}$ then for any constant $c > 0$ there exists $n_0$ such that for $n \geq n_0$ holds:

$$c \sqrt{\log n} / \sqrt{n} < p, (34)$$

which contradicts (33). It shows that for $n$ large enough, violation of local realism may be shown for isotropic states $\psi_{\text{iso}}$ for $p \geq \sqrt{\log n} / \sqrt{n}$. 

F. Random access code as an communication complexity problem

The setup is the following: Alice obtains 2-bit string \( x_0x_1 \) as an input, and Bob has to return value of the bit selected by his input \( y \). Alice is allowed to communicate only single bit (qbit) to Bob. Below we present RAC 2 → 1 problem in the form of matrix whose entries are outputs for given \( x \) and \( y \):

\[
\begin{array}{c|cccc}
 y \backslash x_1 x_0 & 00 & 01 & 10 & 11 \\
 0 & 0 & 1 & 0 & 1 \\
 1 & 1 & 0 & 1 & 1 \\
\end{array}
\]  

(35)

Deterministic protocol with 1-bit communication splits input values into two sets: \( S_0 \) and \( S_1 \). Alice sends to Bob message \( m \) according to the index of the set to which her input belongs. All messages \( m \) and inputs \( y \) generate family of non-intersect rectangles \( \{ R_{m,y} \} \) which cover problem matrix. Since protocol is deterministic, Bob returns single value for the rectangle. Hence for all \( (x,y) \in R_{m,y} \) the output is the same. It is easy to calculate that for uniform input distribution \( \mu(x,y) = \frac{1}{8} \), for any split \( S_0, S_1 \), we have \( p_S \leq 0.75 \).

Since the problem is defined for fixed and small size, we cannot use our general construction and Bell inequality [8]. Instead we will use weighted success probability \( p_S \) for inputs distributed according to \( \mu \) to discriminate between quantum and classical correlations. Let \( \Pi \) be a protocol with fixed amount of communication and classical shared resources. Its success probability \( p_S(\Pi) \) obeys Bell inequality in the form:

\[ p_S(\Pi) \leq \hat{p}_S, \]  

(36)

where \( \hat{p}_S \) is maximum over all such protocols.

For uniform distribution of input strings, classical protocol gives correct answer with probability \( p_S = 0.75 \) while for quantum protocol worst case success probability is \( p_S = \cos^2(\pi/8) = (2 + \sqrt{2})/4 \) [23]. It means that there is separation between classical and quantum protocols.

In quantum protocol \( \Pi_Q \), Alice sends one of four one-qubit states \( |\psi_{x_0x_1}\rangle \) which have Bloch sphere representation \( \frac{1}{\sqrt{2}}(-1)^{x_0}(-1)^{x_1}, 0 \). Bob measures according to projectors \( E_y \) having representation \( (-1)^{y}(1-y, y) \). In our construction of \( p(a, b|x, y) \) Alice (Bob) measures \( E_{x_0=x_1}^a = |\psi_{x_0x_1}\rangle\langle\psi_{x_0x_1}| \), \( E_{x_0=x_1}^a = 1 - E_{x_0=x_1}^a = (E_y^b) \) one the shared singlet state \( \Phi^+ \). The correlations have the following conditional probability distribution:

\[ p(a, b|x, y) = \text{tr} \left[ (E_{x_0=x_1}^a \otimes E_y^b)\Phi^+ \right]. \]  

(37)

Protocol \( \Pi_{RAC} \) works as follows. Alice and Bob share singlet state. Alice measures observable \( x_0x_1 \) and sends the result \( a \) to Bob. Bob measures observable \( y \) but he returns result \( b \) modulo message from Alice (i.e. \( a \oplus b \)).

Weighted success probability with uniform input distribution leads to the following Bell inequality (cf. inequality [36]):

\[ \sum_{a,x,y} \frac{1}{8} p(a, b = x_y \oplus a|x, y) \leq 0.75. \]  

(38)

The correlations [37] violate inequality [35] giving \( p_S = \cos^2(\pi/8) > 0.75 \).

We compare inequality [38] with CHSH inequality in ability to detect violation of local realism for the Werner states. Putting \( \Psi_W = p\Phi^++(1-p)/4 \) in place of \( \Phi^+ \) in [37] we get that both tests detect violation of local realism for \( p > 1/\sqrt{2} \). It is worth to mention that local hidden variable model construction is known for \( p_c = 2/3 \) [24].

---

[1] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. 47, 777 (1935)
[2] J. S. Bell, Physics, 1, 195 (1965)
[3] R. Cleve, H. Buhrman, Phys. Rev. A 56, 1201 (1997), arXiv:9704026
[4] A. C. Yao, Proc. of 11th STOC 209 (1979)
[5] A. C. Yao. In Proceedings of 34th IEEE FOCS, 352 (1993).
[6] H. Buhrman, R. Cleve, S. Massar, R. de Wolf; Rev. Mod. Phys. 82, 665698 (2010), arXiv:0907.2583
[7] R. Raz. In Proc. of 31st Annual ACM Symposium on the Theory of Computing, 358 (1999)
[8] H. Buhrman, R. Cleve, W. van Dam SIAM J Comput. 30 (2000) 1829-1841, arXiv:9705033
[9] C. Brukner, M. Zukowski, J.-W. Pan, A. Zeilinger, Phys. Rev. Lett. 92, 127901 (2004), arXiv:0210114
[10] O. Regev, B. Klartag, Proc. of STOC '11 the 43rd annual ACM symposium on Theory of computing, 31 (2011), arXiv:1009.3640
[11] H. Buhrman, G. Scarpa, R. de Wolf, arXiv:1007.2350
[12] S. L. Braunstein, C. M. Caves, Phys. Rev. Lett. 61, 662 (1988) ; N. J. Cerf and C. Adami, Phys. Rev. A. 55, 3371 (1997), arXiv:9608047
[13] S. Laplante, V. Lerays, J. Roland Lecture Notes in Computer Science, 7391, 617 (2012), arXiv:1203.4155
[14] S. Massar, Phys. Rev. A. 65, 032121 (2002), arXiv:0109008
[15] C. H. Bennett, P. Hayden, D. W. Leung, P. W. Shor, A. Winter, IEEE Trans. Inform. Theory, 51,56 (2005), arXiv:0307100
[16] H. Buhrman, O. Regev, G. Scarpa, R. de Wolf, I. Santha, IEEE Conference on Computational Complexity, 157 (2011), arXiv:1012.5043
[17] C. Palazuelos, arXiv:1206.3695
[18] M. Junge, C. Palazuelos, D. Perez-Garcia, I. Villanueva, M.M. Wolf, Comm. Math. Phys. 300, 715 (2010), arXiv:0910.4228
[19] M. Junge, C. Palazuelos, Comm. Math. Phys. 306,
[20] M. Junge, C. Palazuelos, D. Perez-Garcia, I. Villanueva, M.M. Wolf, Phys. Rev. Lett. 104 170405 (2010), arXiv:0910.4228

[21] D. Gavinsky, J. Kempe, I. Kerenidis, R. Raz, R. de Wolf, Proc. 39th STOC, 516 (2007), arXiv:0611209

[22] E. Kushilevitz, N. Nisan, Communication Complexity, Cambridge University Press 2006

[23] A. Ambainis, A. Nayak, A. Ta-Shma, U. Vazirani, Journal of the ACM, 49, 496 (2002), arXiv:9804043

[24] A. Acin, N. Gisin, B. Toner, Phys. Rev. A 73, 062105 (2006), arXiv:0606138